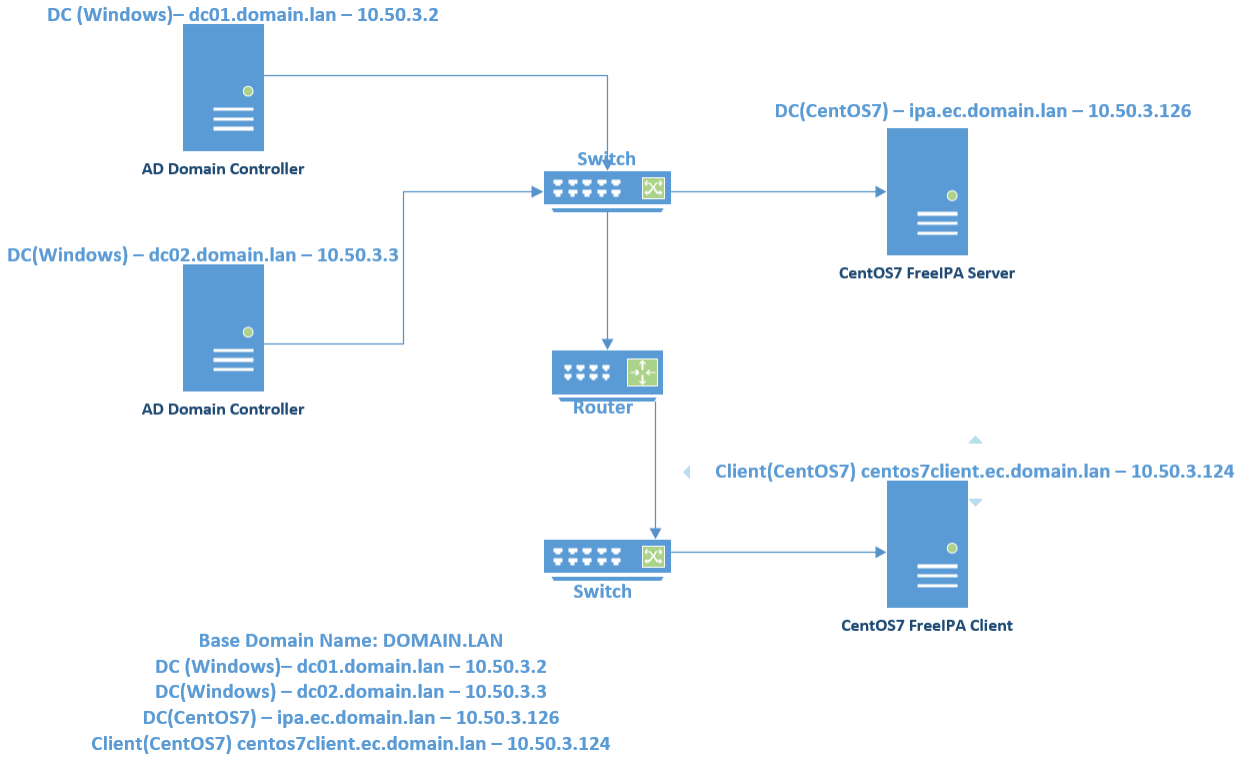
Integration FreeIPA in CentOS7 to Microsoft Active Directory

Our purpose is configure and integrate CentOS7 with Microsoft Active Directory as domain controller.

We use the following machines:
DC (Windows)– dc01.domain.lan – **10.50.3.2**
DC(Windows) – dc02.domain.lan – **10.50.3.3**
DC(CentOS7) – ipa.ec.domain.lan – **10.50.3.126**
Client(CentOS7) centos7client.ec.domain.lan – **10.50.3.124**

Our Base DN is **DOMAIN.LAN**. Both of Active Directory Domain Controllers works on Windows server 2012 R2.

The network topology will be as following:

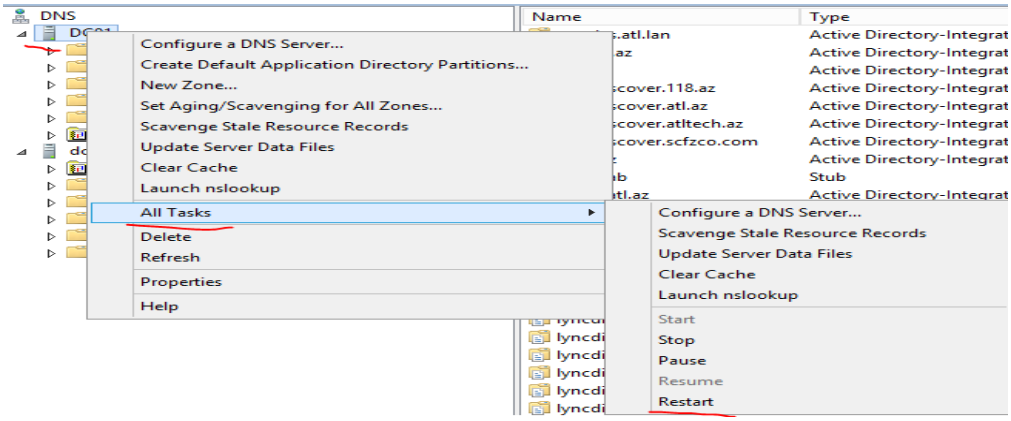


First of all go to the Active Directory Domain Controller and open PowerShell to write the DNS records as following:
PS C:\Users\Administrator> **dnscmd 127.0.0.1 /RecordAdd domain.lan ipa.ec A 10.50.3.126**
Add A Record for ipa.ec.domain.lan at domain.lan
Command completed successfully.

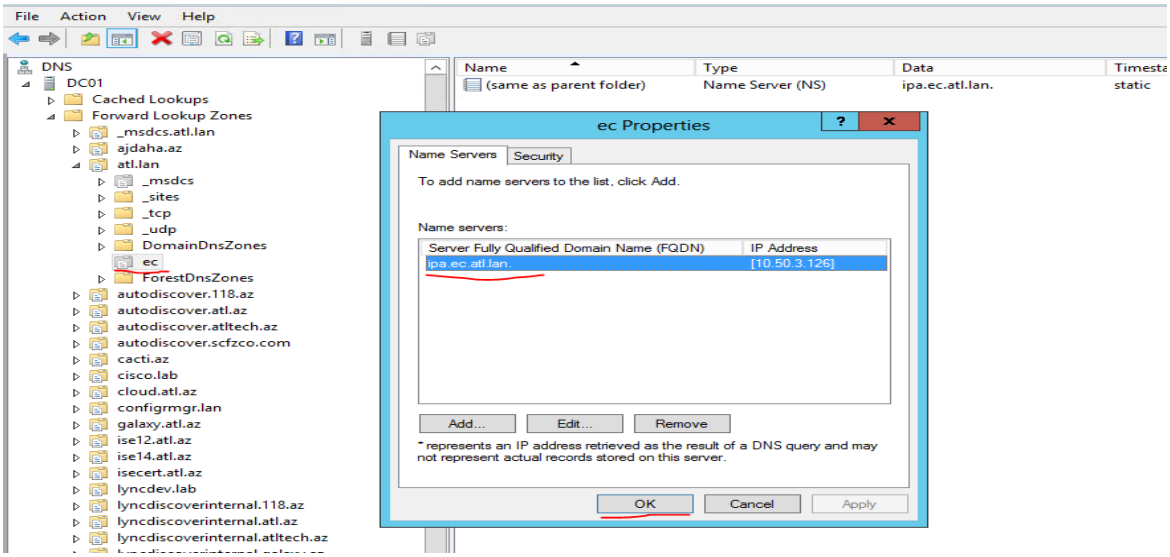
PS C:\Users\Administrator> **dnscmd 127.0.0.1 /RecordAdd domain.lan ec NS ipa.ec.domain.lan**

```
Add NS Record for ec.domain.lan at domain.lan
Command completed successfully.

PS C:\Users\Administrator> dnscmd 127.0.0.1 /ClearCache
127.0.0.1 completed successfully.
Command completed successfully.
```

After adding new **A** and **NS** records we must restart DNS service for each AD to quickly apply changes:



The result of the changes must be as following:



Note: Hostname for FreeIPA server(10.50.3.126) must be configured as **ipa.ec.domain.lan** and for FreeIPA client(10.50.3.124) must be configured as **centos7client**.

Note: Disable **SELinux** and **firewalld** for both(FreeIPA server and client) Machines.

Disable Selinux and firewall for FreeIPA server:

```
[root@ipa ~]# sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
```

```
[root@ipa ~]# systemctl stop firewalld; systemctl disable firewalld; reboot
rm '/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service'
rm '/etc/systemd/system/basic.target.wants/firewalld.service'
```

/etc/hosts file for FreeIPA(10.50.3.126) server will be as following:

```
[root@ipa ~]# echo "10.50.3.126 ipa.ec.domain.lan ipa" >> /etc/hosts
```

Install needed packages:

```
[root@ipa ~]# yum -y install vim net-tools bind-utils
```

Install packages for FreeIPA server:

```
[root@ipa ~]# yum -y install ipa-server-trust-ad bind bind-dyndb-ldap ipa-server-dns
```

Install and configure FreeIPA server with the following credentials(Result must be as following):

```
[root@ipa ~]# ipa-server-install --realm=EC.DOMAIN.LAN --domain=ec.domain.lan --ds-password='A123456789a' --admin-password='A123456789a' --mkhomedir --ssh-trust-dns --setup-dns --unattended --forwarder=10.50.3.2 --no-host-dns
Checking DNS domain ec.domain.lan, please wait ...

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 DNS (bind)

Warning: skipping DNS resolution of host ipa.ec.domain.lan
Checking DNS domain ec.domain.lan., please wait ...
Checking DNS forwarders, please wait ...
DNS server 10.50.3.2: answer to query '. SOA' is missing DNSSEC signatures (no RRSIG data)
Please fix forwarder configuration to enable DNSSEC support.
(For BIND 9 add directive "dnssec-enable yes;" to "options {}")
WARNING: DNSSEC validation will be disabled

The IPA Master Server will be configured with:
Hostname:       ipa.ec.domain.lan
IP address(es): 10.50.3.126
Domain name:    ec.domain.lan
Realm name:     EC.DOMAIN.LAN

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       10.50.3.2
Forward policy:   only
Reverse zone(s):  No reverse zone


Configuring NTP daemon (ntpd)
  [1/4]: stopping ntpd
  [2/4]: writing configuration
  [3/4]: configuring ntpd to start on boot
  [4/4]: starting ntpd
Done configuring NTP daemon (ntpd).
Configuring directory server (dirsrv). Estimated time: 1 minute
  [1/47]: creating directory server user
  [2/47]: creating directory server instance
  [3/47]: updating configuration in dse.ldif
  [4/47]: restarting directory server
  [5/47]: adding default schema
  [6/47]: enabling memberof plugin
  [7/47]: enabling winsync plugin
  [8/47]: configuring replication version plugin
  [9/47]: enabling IPA enrollment plugin
  [10/47]: enabling ldapi
  [11/47]: configuring uniqueness plugin
  [12/47]: configuring uuid plugin
  [13/47]: configuring modrdn plugin
  [14/47]: configuring DNS plugin
  [15/47]: enabling entryUSN plugin
```

```
  [16/47]: configuring lockout plugin
  [17/47]: configuring topology plugin
  [18/47]: creating indices
  [19/47]: enabling referential integrity plugin
  [20/47]: configuring certmap.conf
  [21/47]: configure autobind for root
  [22/47]: configure new location for managed entries
  [23/47]: configure dirsrv ccache
  [24/47]: enabling SASL mapping fallback
  [25/47]: restarting directory server
  [26/47]: adding sasl mappings to the directory
  [27/47]: adding default layout
  [28/47]: adding delegation layout
  [29/47]: creating container for managed entries
  [30/47]: configuring user private groups
  [31/47]: configuring netgroups from hostgroups
  [32/47]: creating default Sudo bind user
  [33/47]: creating default Auto Member layout
  [34/47]: adding range check plugin
  [35/47]: creating default HBAC rule allow_all
  [36/47]: adding sasl mappings to the directory
  [37/47]: adding entries for topology management
  [38/47]: initializing group membership
  [39/47]: adding master entry
  [40/47]: initializing domain level
  [41/47]: configuring Posix uid/gid generation
  [42/47]: adding replication acis
  [43/47]: enabling compatibility plugin
  [44/47]: activating sidgen plugin
  [45/47]: activating extdom plugin
  [46/47]: tuning directory server
  [47/47]: configuring directory to start on boot
Done configuring directory server (dirsrv).
Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes 30 seconds
  [1/31]: creating certificate server user
  [2/31]: configuring certificate server instance
  [3/31]: stopping certificate server instance to update CS.cfg
  [4/31]: backing up CS.cfg
  [5/31]: disabling nonces
  [6/31]: set up CRL publishing
  [7/31]: enable PKIX certificate path discovery and validation
  [8/31]: starting certificate server instance
  [9/31]: creating RA agent certificate database
  [10/31]: importing CA chain to RA certificate database
  [11/31]: fixing RA database permissions
  [12/31]: setting up signing cert profile
  [13/31]: setting audit signing renewal to 2 years
  [14/31]: restarting certificate server
  [15/31]: requesting RA certificate from CA
  [16/31]: issuing RA agent certificate
  [17/31]: adding RA agent as a trusted user
  [18/31]: authorizing RA to modify profiles
  [19/31]: authorizing RA to manage lightweight CAs
  [20/31]: Ensure lightweight CAs container exists
  [21/31]: configure certmonger for renewals
  [22/31]: configure certificate renewals
  [23/31]: configure RA certificate renewal
  [24/31]: configure Server-Cert certificate renewal
  [25/31]: Configure HTTP to proxy connections
  [26/31]: restarting certificate server
  [27/31]: migrating certificate profiles to LDAP
  [28/31]: importing IPA certificate profiles
  [29/31]: adding default CA ACL
  [30/31]: adding 'ipa' CA entry
  [31/31]: updating IPA configuration
Done configuring certificate server (pki-tomcatd).
Configuring directory server (dirsrv). Estimated time: 10 seconds
  [1/3]: configuring ssl for ds instance
  [2/3]: restarting directory server
  [3/3]: adding CA certificate entry
Done configuring directory server (dirsrv).
Configuring Kerberos KDC (krb5kdc). Estimated time: 30 seconds
  [1/9]: adding kerberos container to the directory
  [2/9]: configuring KDC
  [3/9]: initialize kerberos container
WARNING: Your system is running out of entropy, you may experience long delays
  [4/9]: adding default ACIs
  [5/9]: creating a keytab for the directory
  [6/9]: creating a keytab for the machine
  [7/9]: adding the password extension to the directory
  [8/9]: starting the KDC
  [9/9]: configuring KDC to start on boot
Done configuring Kerberos KDC (krb5kdc).
Configuring kadmin
  [1/2]: starting kadmin
  [2/2]: configuring kadmin to start on boot
Done configuring kadmin.
Configuring ipa_memcached
```

```
  [1/2]: starting ipa_memcached
  [2/2]: configuring ipa_memcached to start on boot
Done configuring ipa_memcached.
Configuring ipa-otpd
  [1/2]: starting ipa-otpd
  [2/2]: configuring ipa-otpd to start on boot
Done configuring ipa-otpd.
Configuring ipa-custodia
  [1/5]: Generating ipa-custodia config file
  [2/5]: Making sure custodia container exists
  [3/5]: Generating ipa-custodia keys
  [4/5]: starting ipa-custodia
  [5/5]: configuring ipa-custodia to start on boot
Done configuring ipa-custodia.
Configuring the web interface (httpd). Estimated time: 1 minute
  [1/21]: setting mod_nss port to 443
  [2/21]: setting mod_nss cipher suite
  [3/21]: setting mod_nss protocol list to TLSv1.0 - TLSv1.2
  [4/21]: setting mod_nss password file
  [5/21]: enabling mod_nss renegotiate
  [6/21]: adding URL rewriting rules
  [7/21]: configuring httpd
  [8/21]: configure certmonger for renewals
  [9/21]: setting up httpd keytab
  [10/21]: setting up ssl
  [11/21]: importing CA certificates from LDAP
  [12/21]: setting up browser autoconfig
  [13/21]: publish CA cert
  [14/21]: clean up any existing httpd ccache
  [15/21]: configuring SELinux for httpd
  [16/21]: create KDC proxy user
  [17/21]: create KDC proxy config
  [18/21]: enable KDC proxy
  [19/21]: restarting httpd
  [20/21]: configuring httpd to start on boot
  [21/21]: enabling oddjobd
Done configuring the web interface (httpd).
Applying LDAP updates
Upgrading IPA:
  [1/9]: stopping directory server
  [2/9]: saving configuration
  [3/9]: disabling listeners
  [4/9]: enabling DS global lock
  [5/9]: starting directory server
  [6/9]: upgrading server
  [7/9]: stopping directory server
  [8/9]: restoring configuration
  [9/9]: starting directory server
Done.
Restarting the directory server
Restarting the KDC
Configuring DNS (named)
  [1/11]: generating rndc key file
WARNING: Your system is running out of entropy, you may experience long delays
  [2/11]: adding DNS container
  [3/11]: setting up our zone
  [4/11]: setting up our own record
  [5/11]: setting up records for other masters
  [6/11]: adding NS record to the zones
  [7/11]: setting up kerberos principal
  [8/11]: setting up named.conf
  [9/11]: setting up server configuration
  [10/11]: configuring named to start on boot
  [11/11]: changing resolv.conf to point to ourselves
Done configuring DNS (named).
Configuring DNS key synchronization service (ipa-dnskeysyncd)
  [1/7]: checking status
  [2/7]: setting up bind-dyndb-ldap working directory
  [3/7]: setting up kerberos principal
  [4/7]: setting up SoftHSM
  [5/7]: adding DNSSEC containers
  [6/7]: creating replica keys
  [7/7]: configuring ipa-dnskeysyncd to start on boot
Done configuring DNS key synchronization service (ipa-dnskeysyncd).
Restarting ipa-dnskeysyncd
Restarting named
Updating DNS system records
Restarting the web server
Configuring client side components
Using existing certificate '/etc/ipa/ca.crt'.
Client hostname: ipa.ec.domain.lan
Realm: EC.DOMAIN.LAN
DNS Domain: ec.domain.lan
IPA Server: ipa.ec.domain.lan
BaseDN: dc=ec,dc=atl,dc=lan

Skipping synchronizing time with NTP server.
New SSSD config will be created
```

```
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
trying https://ipa.ec.domain.lan/ipa/json
Forwarding 'schema' to json server 'https://ipa.ec.domain.lan/ipa/json'
trying https://ipa.ec.domain.lan/ipa/session/json
Forwarding 'ping' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
Forwarding 'ca_is_enabled' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Forwarding 'host_mod' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring ec.domain.lan as NIS domain.
Client configuration complete.

==============================================================================
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 certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
```

After installation of the FreeIPA server to the 10.50.3.126 server change the **/etc/resolv.conf** file as following:

```
[root@ipa ~]# cat /etc/resolv.conf
search domain.lan ec.domain.lan
nameserver 10.50.3.2
nameserver 10.50.3.3
```

Or restart network service:

```
[root@ipa ~]# systemctl restart network
```

Configure IPA server for cross-realm trusts:

```
[root@ipa ~]# ipa-adtrust-install --admin-password='A123456789a' --netbios-name=EC --add-sids --unattended
The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will setup components needed to establish trust to AD domains for
the IPA Server.

This includes:
  * Configure Samba
  * Add trust related objects to IPA LDAP server

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

WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your existing samba configuration.


Configuring CIFS
  [1/22]: stopping smbd
  [2/22]: creating samba domain object
  [3/22]: creating samba config registry
  [4/22]: writing samba config file
  [5/22]: adding cifs Kerberos principal
  [6/22]: adding cifs and host Kerberos principals to the adtrust agents group
  [7/22]: check for cifs services defined on other replicas
  [8/22]: adding cifs principal to S4U2Proxy targets
  [9/22]: adding admin(group) SIDs
  [10/22]: adding RID bases
  [11/22]: updating Kerberos config
```

```
'dns_lookup_kdc' already set to 'true', nothing to do.
  [12/22]: activating CLDAP plugin
  [13/22]: activating sidgen task
  [14/22]: configuring smbd to start on boot
  [15/22]: adding special DNS service records
  [16/22]: restarting Directory Server to take MS PAC and LDAP plugins changes into account
  [17/22]: adding fallback group
  [18/22]: adding Default Trust View
  [19/22]: setting SELinux booleans
  [20/22]: starting CIFS services
  [21/22]: adding SIDs to existing users and groups
This step may take considerable amount of time, please wait..
  [22/22]: restarting smbd
Done configuring CIFS.

==============================================================================
Setup complete

You must make sure these network ports are open:
        TCP Ports:
          * 135: epmap
          * 138: netbios-dgm
          * 139: netbios-ssn
          * 445: microsoft-ds
          * 1024..1300: epmap listener range
        UDP Ports:
          * 138: netbios-dgm
          * 139: netbios-ssn
          * 389: (C)LDAP
          * 445: microsoft-ds

See the ipa-adtrust-install(1) man page for more details

==============================================================================
```

Establish and verify cross-realm trust - Add trust with AD domain(We do this in FreeIPA server):

```
[root@ipa ~]# ipa trust-add --type=ad domain.lan
Active Directory domain administrator: atladm
Active Directory domain administrator's password: write_pass_here
-----------------------------------------------
Added Active Directory trust for realm "domain.lan"
-----------------------------------------------
  Realm name: domain.lan
  Domain NetBIOS name: ATL
  Domain Security Identifier: S-1-5-21-2852957904-459492390-1610673386
  Trust direction: Trusting forest
  Trust type: Active Directory domain
  Trust status: Established and verified
```

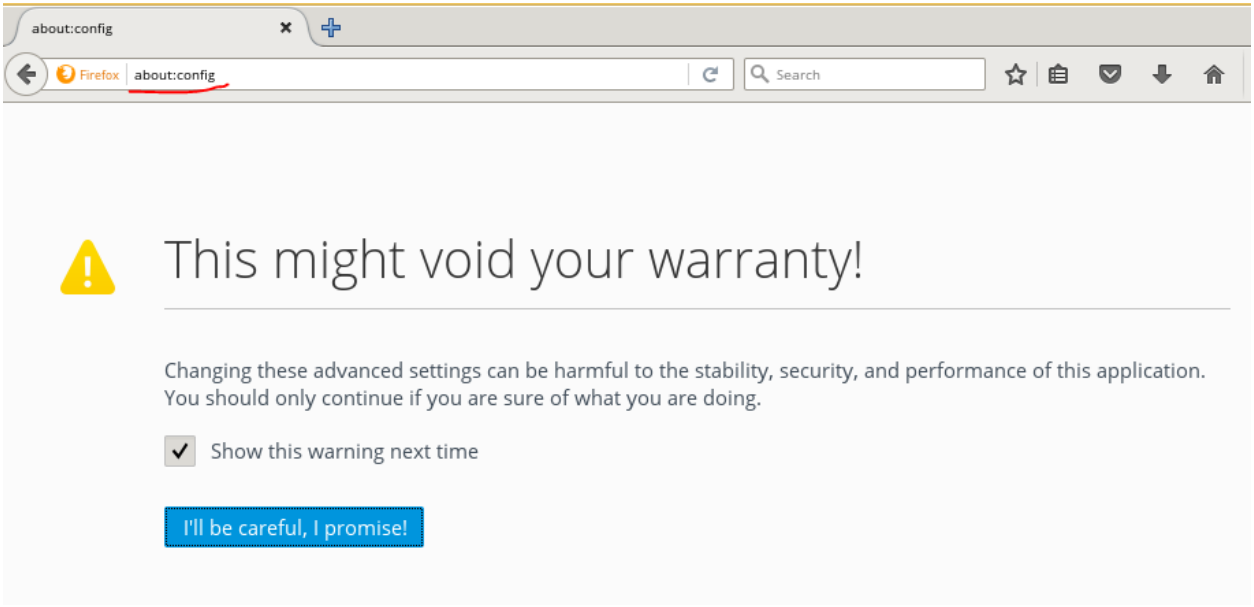
Check trusted domain:

```
[root@ipa ~]# ipa trustdomain-find domain.lan
  Domain name: domain.lan
  Domain NetBIOS name: ATL
  Domain Security Identifier: S-1-5-21-2852957904-459492390-1610673386
  Domain enabled: True
----------------------------
Number of entries returned 1
----------------------------
```

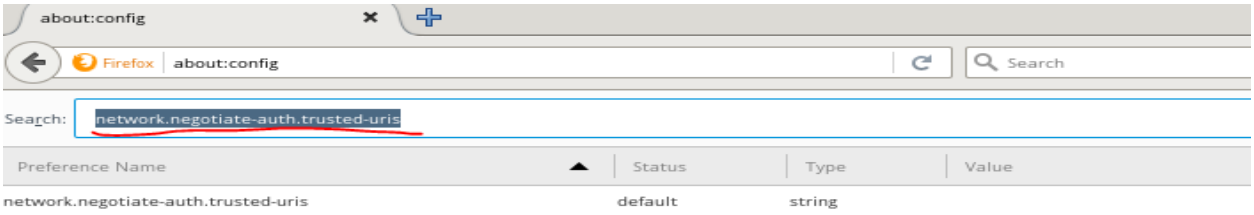
Install X packages and firefos browser to FreeIPA server(**10.50.3.126**). We will use X for use browser in server:

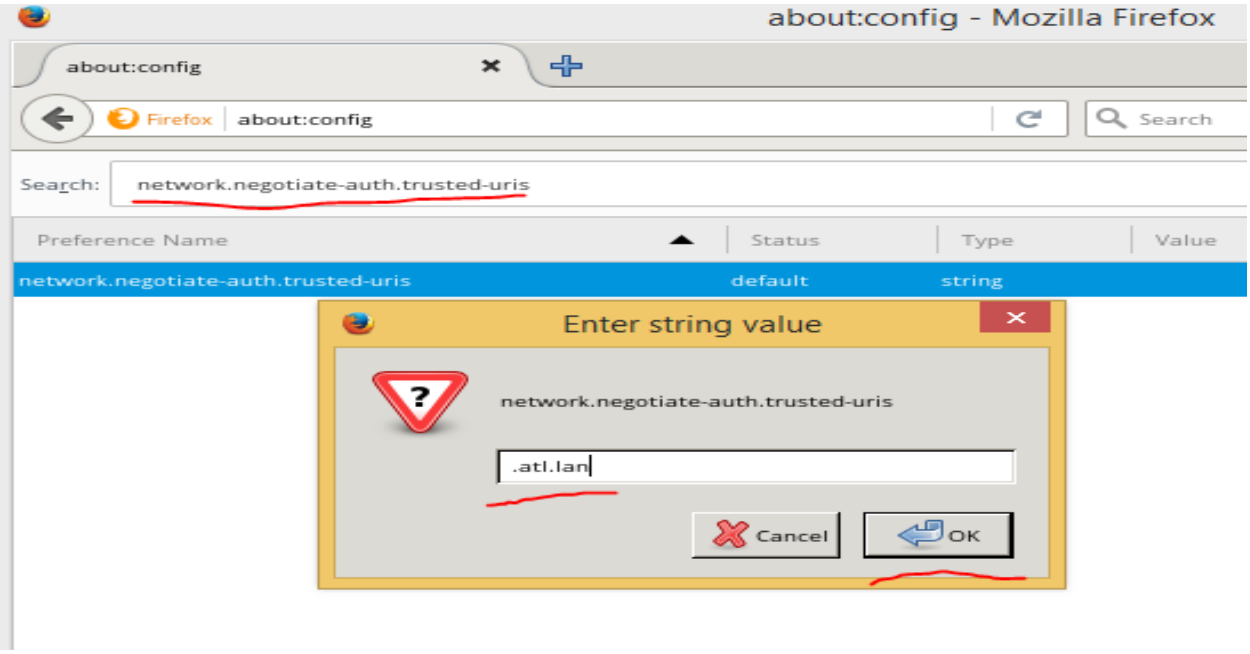
```
[root@ipa ~]# yum -y install xorg-x11-apps xorg-x11-utils xorg-x11-xinit
xorg-x11-xauth xorg-x11-server-Xorg xorg-x11-font*
[root@ipa ~]# yum install -y firefox
```

Login to FreeIPA (10.50.3.126) server with X11 forward again and open Firefox browser. In url tab write **about:config** and press **I'll be careful, I promise!** button:

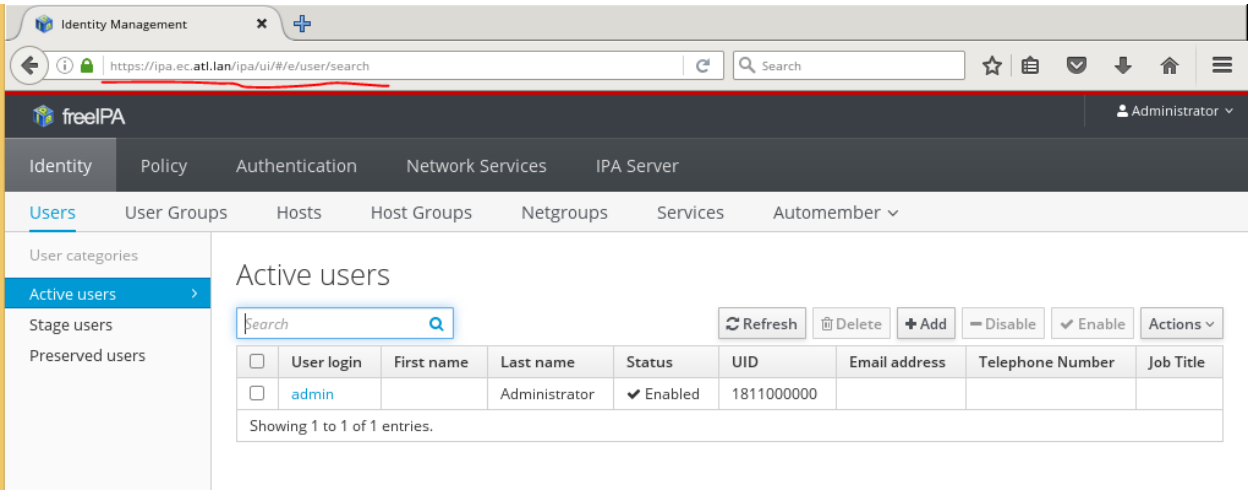


In opened search page write **network.negotiate-auth.trusted-uris** and then bouble click to opened page and write BASE DN (**.domain.lan**)of our AD Domain controller and press to **OK** button:

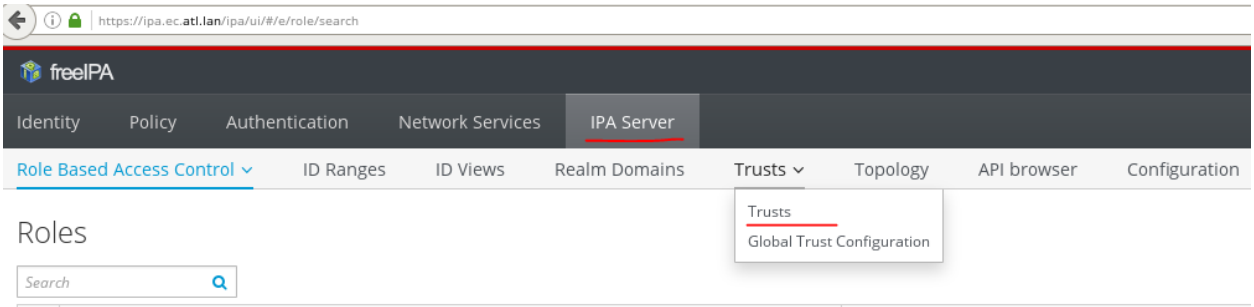




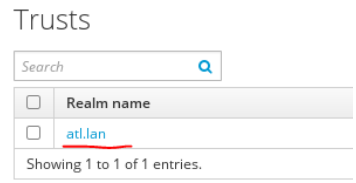
After that login to FreeIPA server management interface(**https://ipa.ec.domain.lan**):

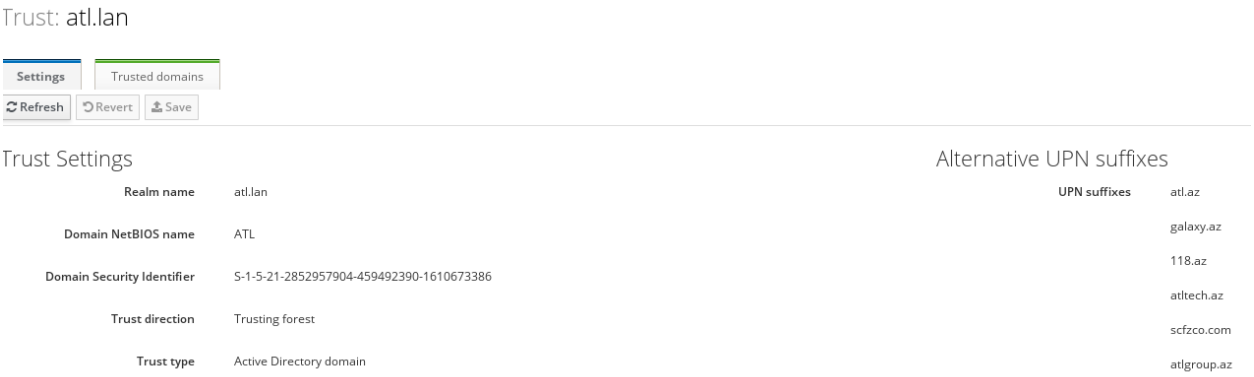


Go to the **IPA server** -> **Trusts** -> **Trusts** to check domain:

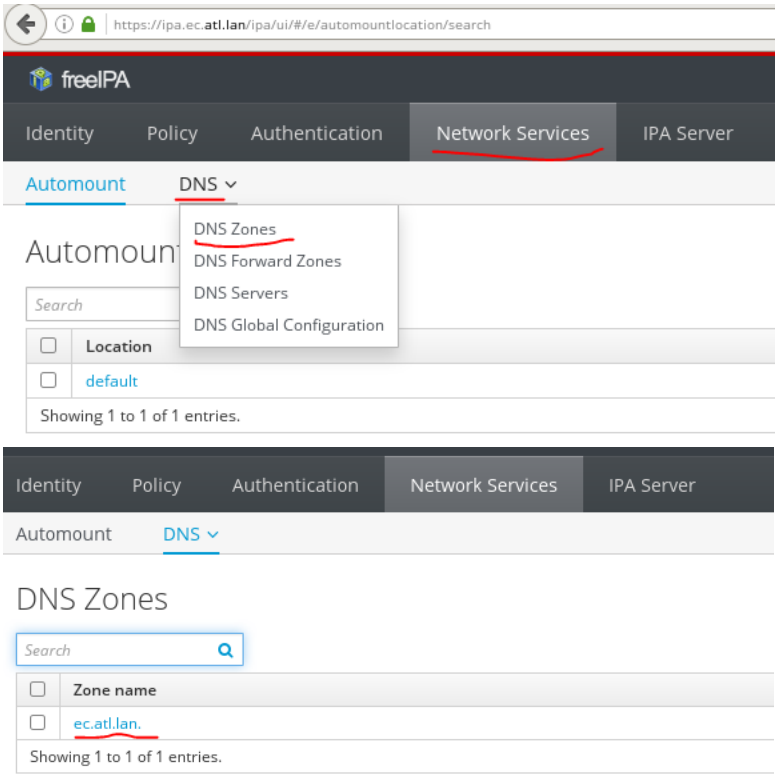


Click to domain and check trusts:

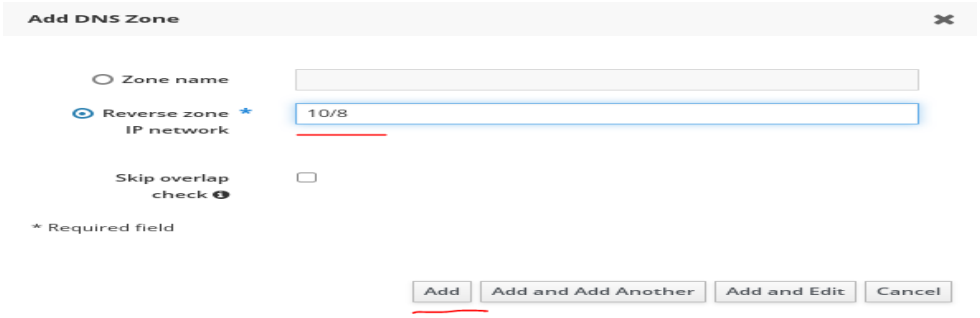




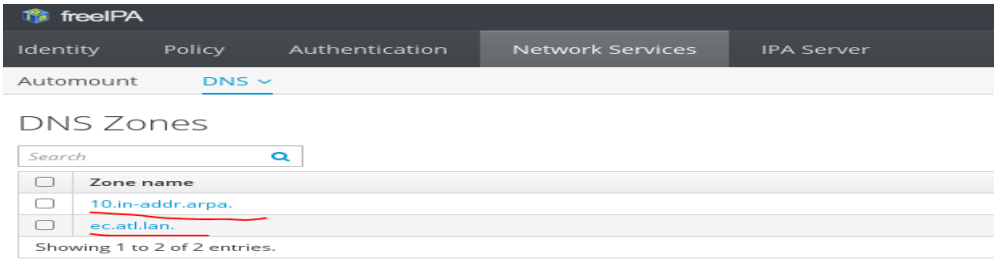
Then go to the Network Services -> DNS -> DNS Zones and click to the domain name to check records:



Again go to the **Network Services** -> **DNS** -> **DNS Zones** and the press to **Add** button and then select **Reverse zone IP network**, write there **10/8** and press to **Add** button.



Result must be as following:



List of records:

DNS Resource Records: ec.atl.lan.

DNS Resource Records | Settings

Search

Record name	Record Type	Data
@	NS	ipa.ec.atl.lan.
_kerberos	TXT	"EC.ATL.LAN"
_kerberos-master._tcp	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos-master._udp	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._tcp	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._tcp.dc._msdcs	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._udp	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._udp.Default-First-Site-Name._sites.dc._msdcs	SRV	0 100 88 ipa.ec.atl.lan.
_kerberos._udp.dc._msdcs	SRV	0 100 88 ipa.ec.atl.lan.
_kpasswd._tcp	SRV	0 100 464 ipa.ec.atl.lan.
_kpasswd._udp	SRV	0 100 464 ipa.ec.atl.lan.
_ldap._tcp	SRV	0 100 389 ipa.ec.atl.lan.
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs	SRV	0 100 389 ipa.ec.atl.lan.
_ldap._tcp.dc._msdcs	SRV	0 100 389 ipa.ec.atl.lan.
_ntp._udp	SRV	0 100 123 ipa.ec.atl.lan.
ipa	A	10.50.3.126
	SSHFP	3 2 30D9F759026B4826D8E4FCC31751F71299A5E78562F373787C4B2B11 F2EAE75F
	SSHFP	1 2 C5C63350249E5653703C40097334F298EC3124AF921EDAA8AB3B8F95 229AB5FD
	SSHFP	3 1 94C375DA008111455960B1ADFA2980E1402BD80F
	SSHFP	4 2 886BD6E0CE8188DCEF76174A61ABCEE3C2BE45E739EB93F5E944F6CC EE233F1A
	SSHFP	1 1 5CD34568D6DFE4B5AD6DF74DFA111D11E33A2C8A
	SSHFP	4 1 D01E784EC0C412376841BF411DD982D2AF3CE2EE
ipa-ca	A	10.50.3.126

Showing 1 to 18 of 18 entries.

Change default shell to /bin/bash for all users:

```
[root@ipa ~]# ipa config-mod --defaultshell=/bin/bash
  Maximum username length: 32
  Home directory base: /home
  Default shell: /bin/bash
```

```
  Default users group: ipausers
  Default e-mail domain: ec.domain.lan
  Search time limit: 2
  Search size limit: 100
  User search fields: uid,givenname,sn,telephonenumber,ou,title
  Group search fields: cn,description
  Enable migration mode: FALSE
  Certificate Subject base: O=EC.DOMAIN.LAN
  Password Expiration Notification (days): 4
  Password plugin features: AllowNThash
  SELinux user map order: guest_u:s0$xguest_u:s0$user_u:s0$staff_u:s0-
s0:c0.c1023$unconfined_u:s0-s0:c0.c1023
  Default SELinux user: unconfined_u:s0-s0:c0.c1023
  Default PAC types: nfs:NONE, MS-PAC
  IPA masters: ipa.ec.domain.lan
  IPA CA servers: ipa.ec.domain.lan
  IPA NTP servers: ipa.ec.domain.lan
  IPA CA renewal master: ipa.ec.domain.lan
```

To change default shell in the client machine, go to client machine and in the **/etc/sssd/sssd.conf** file change under **[nss]** section **override_shell** variable to the **/bin/bash** like as following:

```
[nss]
override_shell = /bin/bash
```

Add new CentOS7 client machine to server:

```
[root@ipa ~]# ipa host-add centos7client.ec.domain.lan --
password='A123456789a' --ip-address=10.50.3.124 --os="CentOS 7" --
platform="VMware" --location="ATL datacenter" --locality="Narimanov" --
desc="Test CentOS7 server"
---------------------------------------
Added host "centos7client.ec.domain.lan"
---------------------------------------
  Host name: centos7client.ec.domain.lan
  Description: Test CentOS7 server
  Locality: Narimanov
  Location: ATL datacenter
  Platform: VMware
  Operating system: CentOS 7
  Password: True
  Keytab: False
  Managed by: centos7client.ec.domain.lan
```

Now we must to go to the CentOS7 FreeIPA client(10.50.3.124) machine

DNS servers for our CentOS7 client machine must be as following in the **/etc/resolv.conf** file:

```
[root@centos7client ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ipa.ec.domain.lan
nameserver 10.50.3.126
nameserver 10.50.3.2
nameserver 10.50.3.3
```

Disable Selinux, add IP to **/etc/hosts** file, update and install needed packages and disable firewalld:

```
[root@centos7client ~]# sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
[root@centos7client ~]# echo "10.50.3.124 centos7client.ec.domain.lan centos7client" >> /etc/hosts
[root@centos7client ~]# yum update -y && yum -y install vim net-tools bind-utils
[root@centos7client ~]# systemctl stop firewalld; systemctl disable firewalld; reboot
```

Install IPA client package to the CentOS7 client machine:

```
[root@centos7client ~]# yum -y install ipa-client
```

Connect to FreeIPA server(Password we created before for this machine):

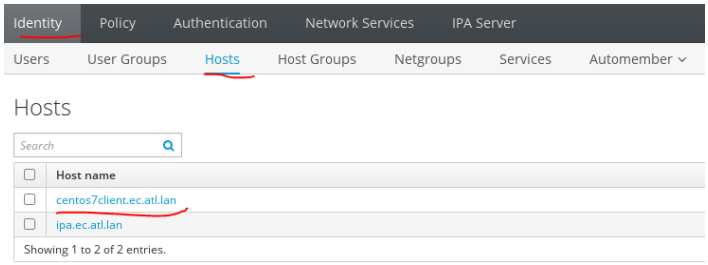
```
[root@centos7client ~]# ipa-client-install -w 'A123456789a' --mkhomedir
Discovery was successful!
Client hostname: centos7client.ec.domain.lan
Realm: EC.DOMAIN.LAN
DNS Domain: ec.domain.lan
IPA Server: ipa.ec.domain.lan
BaseDN: dc=ec,dc=atl,dc=lan

Continue to configure the system with these values? [no]: yes
Synchronizing time with KDC...
Attempting to sync time using ntpd.  Will timeout after 15 seconds
Do you want to download the CA cert from http://ipa.ec.domain.lan/ipa/config/ca.crt ?
(this is INSECURE) [no]: yes
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=EC.DOMAIN.LAN
    Issuer:      CN=Certificate Authority,O=EC.DOMAIN.LAN
    Valid From:  Tue Dec 27 10:21:46 2016 UTC
    Valid Until: Sat Dec 27 10:21:46 2036 UTC

Enrolled in IPA realm EC.DOMAIN.LAN
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm EC.DOMAIN.LAN
trying https://ipa.ec.domain.lan/ipa/json
Forwarding 'schema' to json server 'https://ipa.ec.domain.lan/ipa/json'
trying https://ipa.ec.domain.lan/ipa/session/json
Forwarding 'ping' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
Forwarding 'ca_is_enabled' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
```

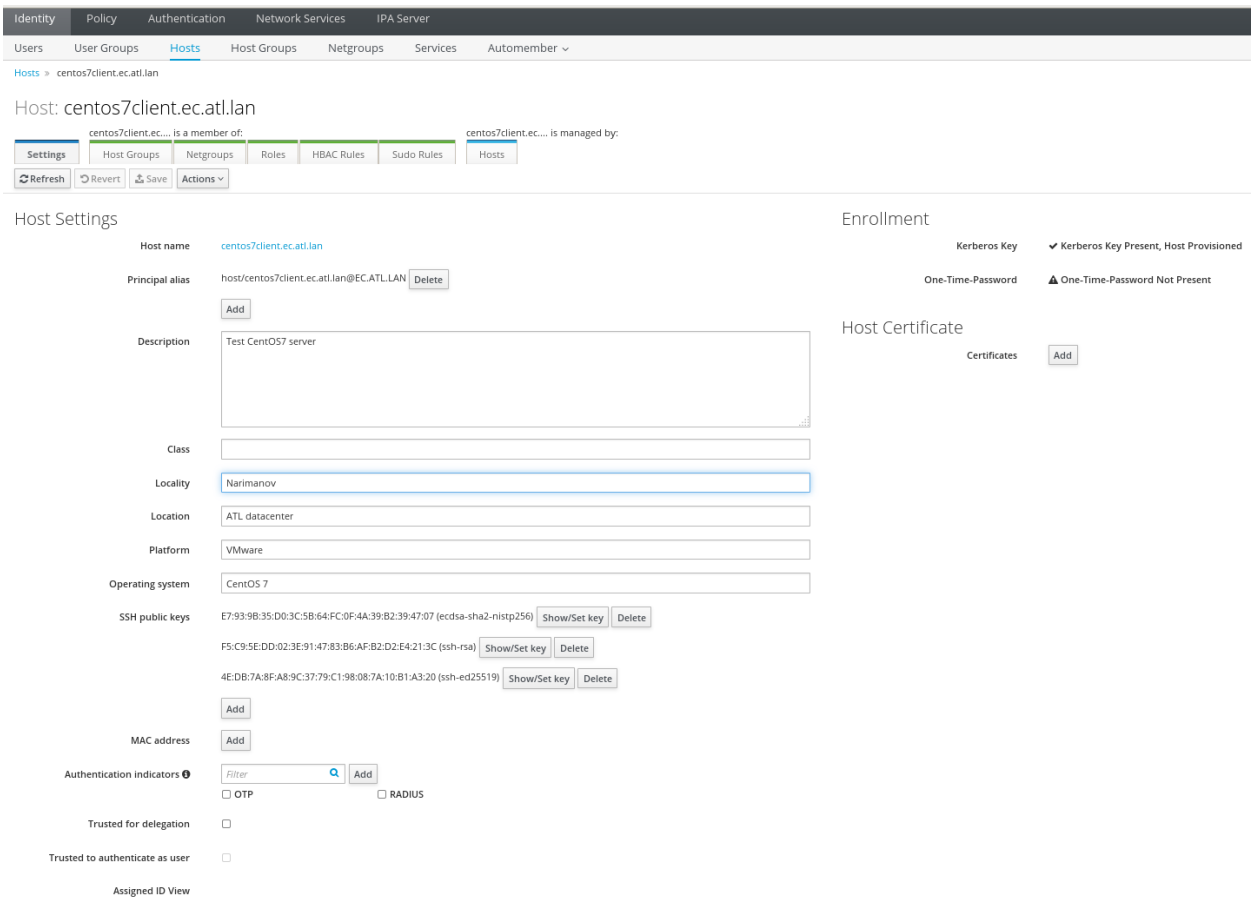
```
Forwarding 'host_mod' to json server 'https://ipa.ec.domain.lan/ipa/session/json'
SSSD enabled
Configured /etc/openldap/ldap.conf
NTP enabled
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring ec.domain.lan as NIS domain.
Client configuration complete.

Try to resolve LDAP servers:
[root@centos7client ~]# dig SRV _ldap._tcp.domain.lan | grep '^_ldap'
_ldap._tcp.domain.lan.      539     IN      SRV     0 100 389 dc01.domain.lan.
_ldap._tcp.domain.lan.      539     IN      SRV     0 100 389 dc02.domain.lan.

[root@centos7client ~]# dig SRV _ldap._tcp.ec.domain.lan | grep '^_ldap'
_ldap._tcp.ec.domain.lan.   86400   IN      SRV     0 100 389
ipa.ec.domain.lan.


Try to login to the FreeIPA server with admin username and look at the ticket
from FreeIPA:
[root@centos7client ~]# kinit admin
Password for admin@EC.DOMAIN.LAN: write_admin_pass
[root@centos7client ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EC.DOMAIN.LAN
Valid starting       Expires              Service principal
12/27/2016 16:34:22  12/28/2016 16:34:16  krbtgt/EC.DOMAIN.LAN@EC.DOMAIN.LAN
```

Go to the FreeIPA server **Network Services** -> **DNS** -> **DNS Zones** click to **ec.domain.lan.** domain and the look at the new records:

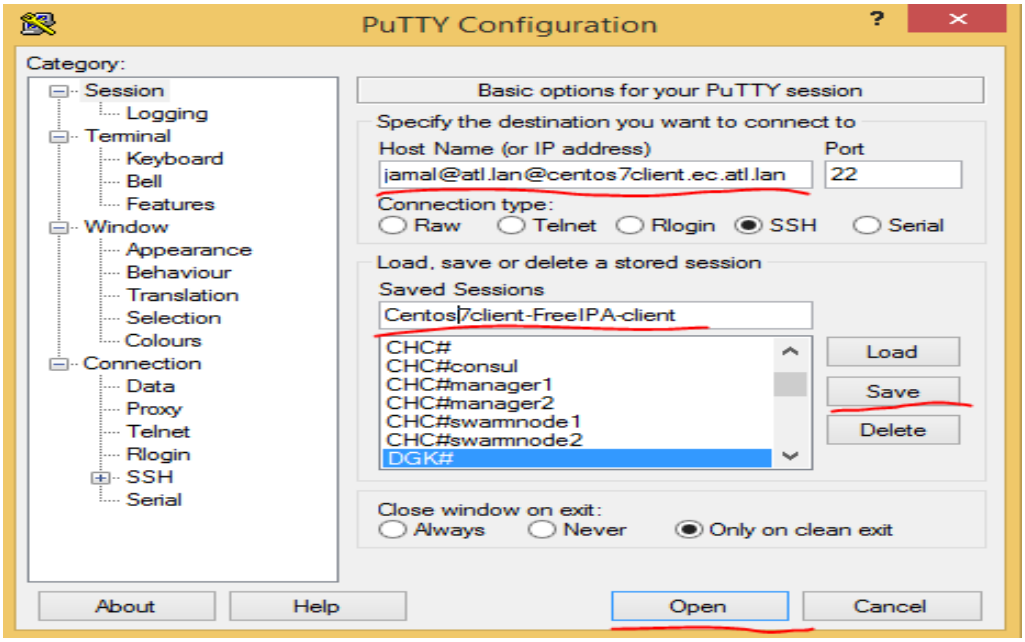
centos7client	A	10.50.3.124
	SSHFP	3 1 B92E24712F5AEC7AD0359E2C066AF27C6A32A2BA
	SSHFP	4 1 4FAAC66B947CA94657B099F07009BDC86D1E8AF1
	SSHFP	4 2 60DABCC878EDA98BA7E12755DAFCFBD8E3C9B8845129A03187AA6164 92D8D8E7
	SSHFP	3 2 B6B6280415F102011F8ABDA22483CB2E3598E93DFA0330A4CD6B43EC 3A984FE0
	SSHFP	1 2 30DBA59640C4F561C03EEB391F287E147A62EE4F3E1044F629E64377 5C180551
	SSHFP	1 1 2A0570529C538EE78FF1302FDA5F077CF9328A72

Then go to the Identity -> Hosts and click to the **centos7client.domain.lan** host to see credentials:

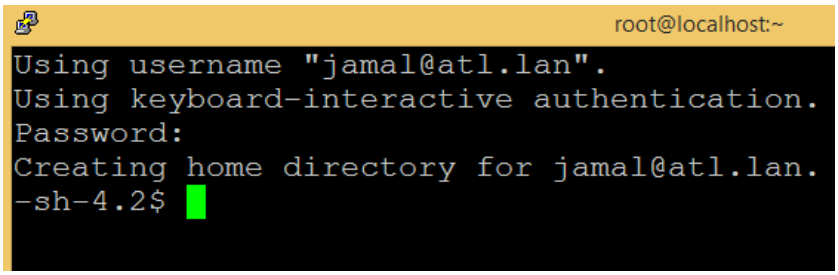




Open Putty client and try to login with domain account to the **centos7client.ec.domain.lan** machine:



First time it will take some time because will create some profile files:

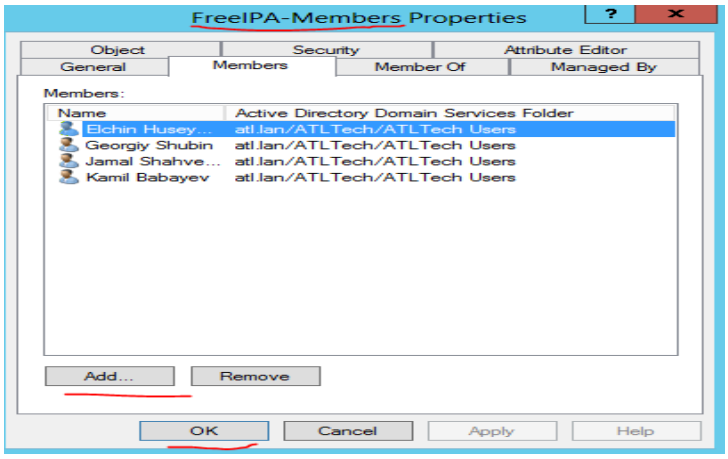


Look at ID and path of home directory:

```
-sh-4.2$ id
uid=349801110(jamal@domain.lan) gid=349801110(jamal@domain.lan)
groups=349801110(jamal@domain.lan),349800513(domain
users@domain.lan),349801113(vpnusers@domain.lan),349801156(rtcuniversalglobal
readonlygroup@domain.lan),349801158(rtcuniversalserverreadonlygroup@domain.la
n),349801159(rtcuniversaluserreadonlygroup@domain.lan),349801164(rtcuniversal
useradmins@domain.lan),349801165(rtcuniversalreadonlyadmins@domain.lan),34980
1171(csuseradministrator@domain.lan),349801210(dl atltech
members@domain.lan),349801280(dl atlgroup members@domain.lan),349801287(dl it
members@domain.lan),349801343(mercurial@domain.lan),349801365(atltech -  it
members@domain.lan),349801384(scomadmins@domain.lan),349801397(owncloudmember
s@domain.lan),349801429(allow vpn to bvim@domain.lan),349801451(allow vpn to
fhn@domain.lan),349801482(xwikimembers@domain.lan),349801498(openvpnfausers@d
omain.lan),349801499(openvpnmausers@domain.lan),349801504(atlwifiusers@domain
.lan),349801538(gitusers@domain.lan),349801540(omusers@domain.lan),349801564(
atlcanvas@domain.lan),349801642(sp_project2013_reportcreators@domain.lan),349
801676(sp_projectstatus_list_members@domain.lan),349801692(proxy_unlimited@do
main.lan),349801847(dlbyodusers@domain.lan),349802123(redminemembers@domain.l
```

```
an),349802143(openfiremembers@domain.lan),349802227(allow send to dl atlgroup
members@domain.lan),349802240(openprojectmembers@domain.lan)

-sh-4.2$ pwd
/home/domain.lan/jamal

-sh-4.2$ who
jamal@domain.lan pts/1        2016-12-27 16:53 (10.50.63.241)
```

Create new Group with **FreeIPA-Members** name in domain controller and add Administrators to this group:



Create new External group with name **"ad_users_external_freeipa"**:

```
[root@ipa ~]# ipa group-add --desc='AD users external for FreeIPA-Members'
ad_users_external_freeipa --external
-----------------------------------------
Added group "ad_users_external_freeipa"
-----------------------------------------
  Group name: ad_users_external_freeipa
  Description: AD users external for FreeIPA-Members
```

Create new internal group with name **"ad_sshaccess_users"** (We will map this group to the external group **"ad_users_external_freeipa"**):

```
[root@ipa ~]# ipa group-add --desc='AD SSH access users' ad_sshaccess_users
-------------------------------
Added group "ad_sshaccess_users"
-------------------------------
  Group name: ad_sshaccess_users
  Description: AD SSH access users
  GID: 1811000005
```

Add external group members from Base DN **"ATL\FreeIPA-Members"**:

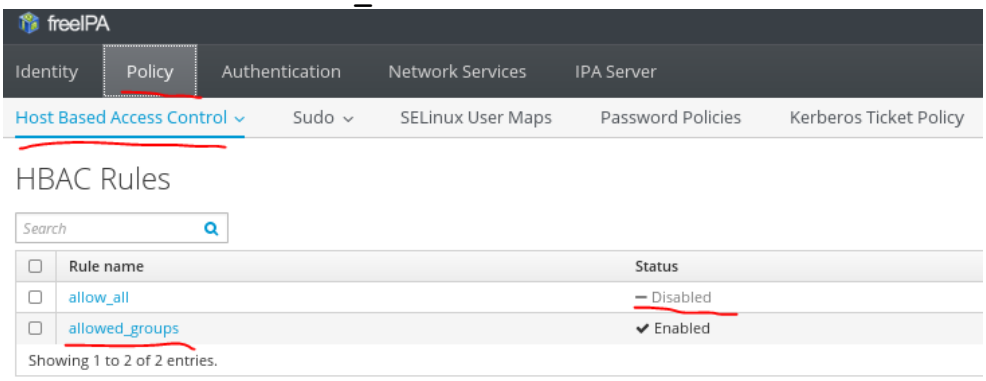
```
[root@ipa ~]# ipa group-add-member ad_users_external_freeipa --external
"ATL\FreeIPA-Members"
[member user]:
[member group]:
  Group name: ad_users_external_freeipa
  Description: AD users external for FreeIPA-Members
```

```
  External member: S-1-5-21-2852957904-459492390-1610673386-2258
-------------------------
Number of members added 1
-------------------------
```

Map external group to our internal group which will go to check FreeIPA-Members group in AD DOMAIN.LAN:

```
[root@ipa ~]# ipa group-add-member ad_sshaccess_users --groups
ad_users_external_freeipa
  Group name: ad_sshaccess_users
  Description: AD SSH access users
  GID: 1811000005
  Member groups: ad_users_external_freeipa
-------------------------
Number of members added 1
-------------------------
```

Then go to the FreeIPA web admin panel and open Policy -> Host Based Access Control. Disable **allow_all** rule and add new rule with name **allowed_groups**:



Then open group **allowed_groups** and add **ad_sshaccess_users** to this group with **Add** button: