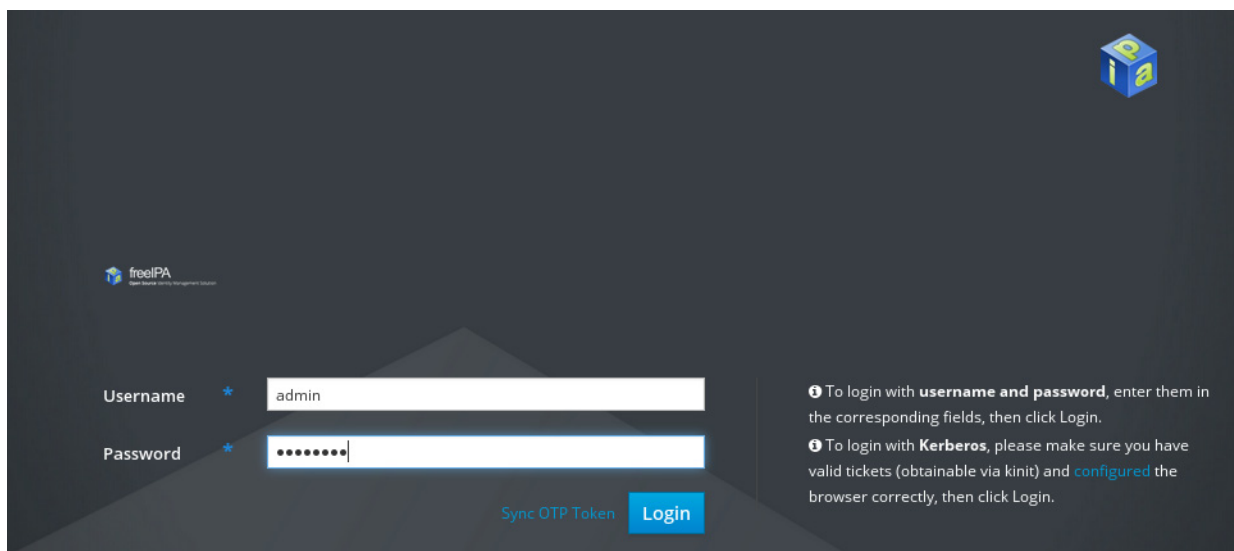


Enterprise Linux 7 Update

FreeIPA - Adding DNS entries

- As well as adding users, the DNS part of FreeIPA will need host entries, especially if you are intending to run services such as kerberised NFS.
- We'll add these entries using the Web GUI.
- As part of the FreeIPA installation, the web server service was configured and started, but it will accept connections only on the FreeIPA server itself, in our case *heron*.
- On the FreeIPA server you will need to be logged in and running the window system, then invoke the Firefox web browser with the server itself as the URL.
- For *heron* this would be *http://heron.fatrain.com*, and you should see:-

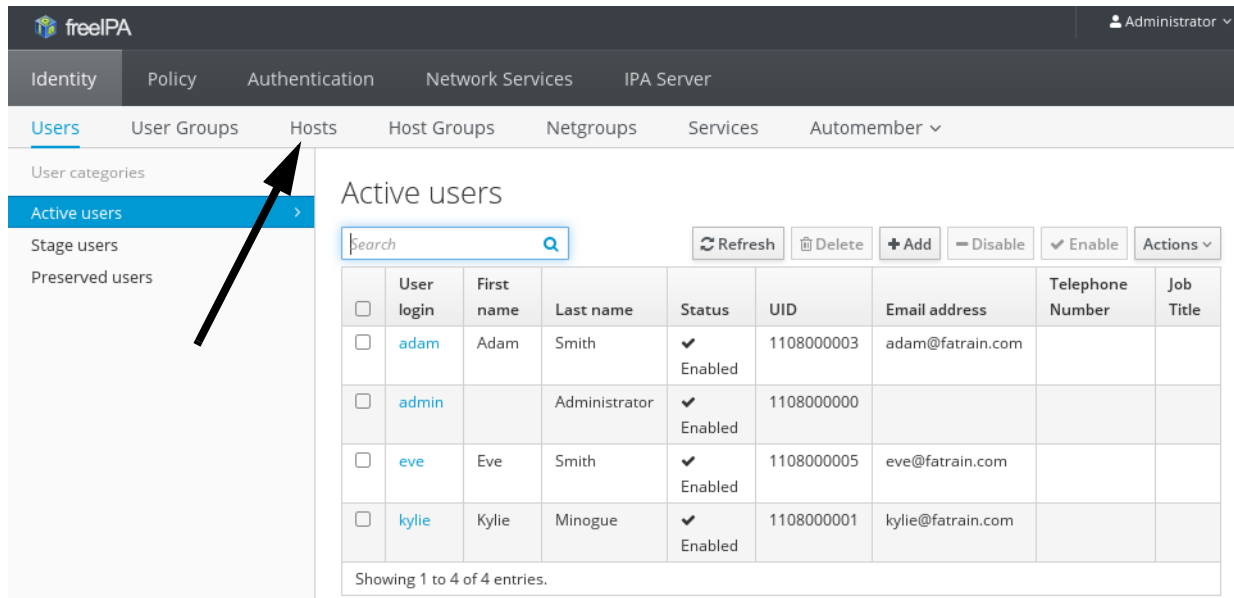


- Enter the username *admin* with password *abc12345*. (Unless you chose something different).

Enterprise Linux 7 Update

FreeIPA - Adding DNS entries

- The first screen you see shows the users:-

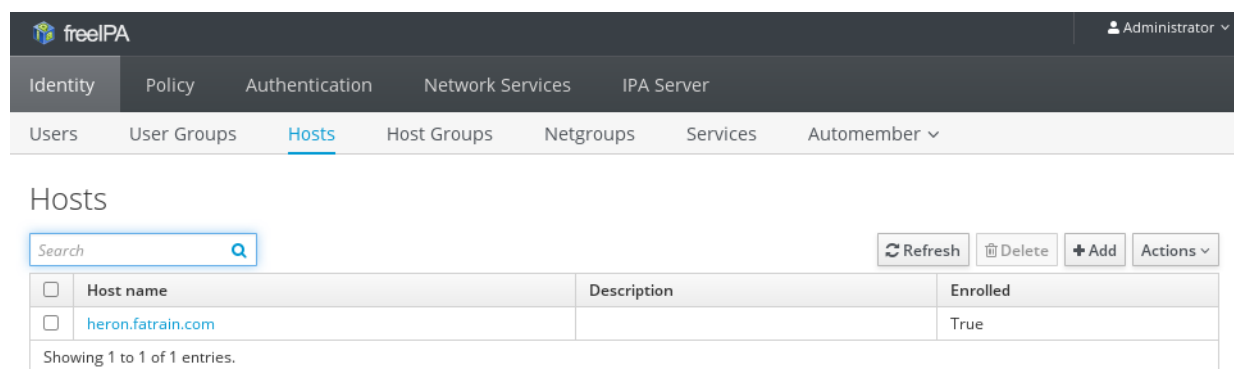


The screenshot shows the FreeIPA web interface. The 'Hosts' tab is selected and highlighted with a black arrow. The 'Active users' page is displayed, showing a table of users. The table has columns for User login, First name, Last name, Status, UID, Email address, Telephone Number, and Job Title. There are four entries in the table, all with a status of 'Enabled'.

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	adam	Adam	Smith	✓ Enabled	1108000003	adam@fatrain.com		
<input type="checkbox"/>	admin		Administrator	✓ Enabled	1108000000			
<input type="checkbox"/>	eve	Eve	Smith	✓ Enabled	1108000005	eve@fatrain.com		
<input type="checkbox"/>	kylie	Kylie	Minogue	✓ Enabled	1108000001	kylie@fatrain.com		

Showing 1 to 4 of 4 entries.

- You can try adding a user if you like, just click on the *+Add* button above the email address column.
- We want to add hosts, so click on the *Hosts* tab as indicated:-



The screenshot shows the FreeIPA web interface with the 'Hosts' tab selected. The 'Hosts' page is displayed, showing a table of hosts. The table has columns for Host name, Description, and Enrolled. There is one entry in the table: heron.fatrain.com, which is enrolled.

<input type="checkbox"/>	Host name	Description	Enrolled
<input type="checkbox"/>	heron.fatrain.com		True

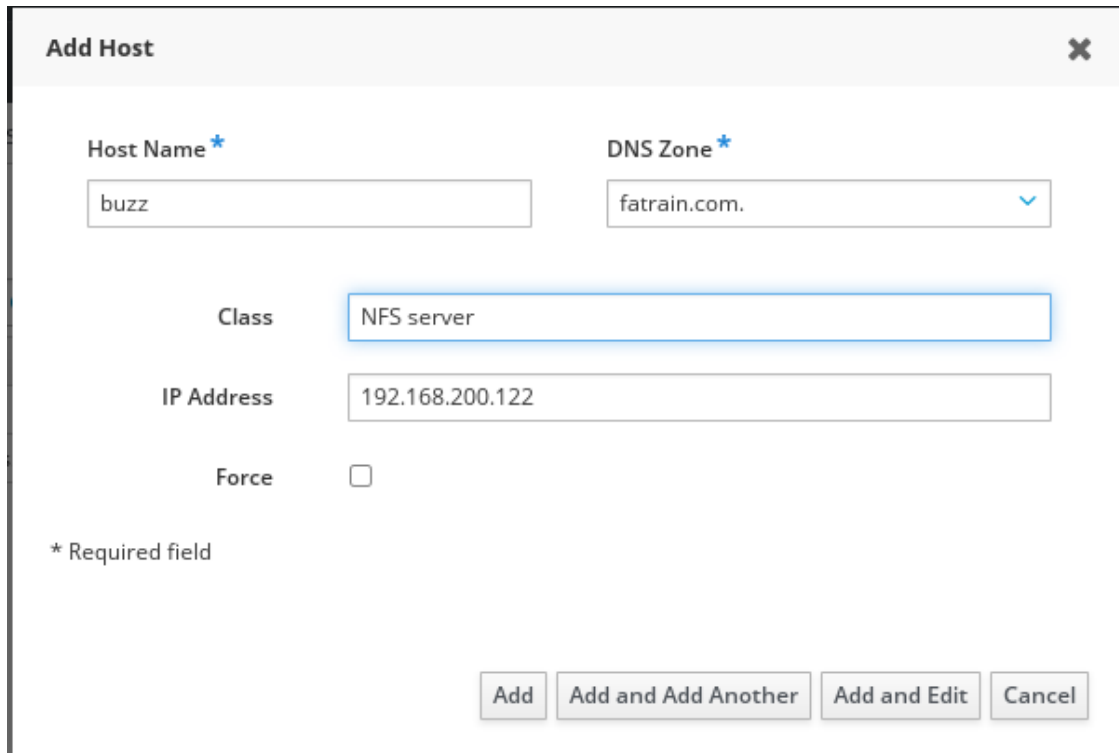
Showing 1 to 1 of 1 entries.

- Now click on *+Add*.

Enterprise Linux 7 Update

FreeIPA - Adding DNS entries

- The follow shows an example for the NFS server *buzz*:-



The screenshot shows a dialog box titled "Add Host" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Host Name ***: A text input field containing the value "buzz".
- DNS Zone ***: A dropdown menu showing "fatrain.com." with a downward arrow.
- Class**: A dropdown menu showing "NFS server".
- IP Address**: A text input field containing the value "192.168.200.122".
- Force**: A checkbox that is currently unchecked.
- * Required field**: A legend indicating that fields with an asterisk are required.
- Buttons**: Four buttons at the bottom: "Add", "Add and Add Another", "Add and Edit", and "Cancel".

- Not sure what the force option is...and the GUI lacks any help facilities.
- Click on *Add* when completed, and add any further hosts in the same way - just ensure that the domain name is set correctly each time.
- Of course, substitute *buzz* with your server name.

Enterprise Linux 7 Update

FreeIPA - Joining the Kerberos realm

- The server *buzz* can now be joined to the Kerberos realm within the FreeIPA server *heron*.
- On *buzz*, make sure the DNS server is set as the FreeIPA server; this may be with or without NetworkManager running.
- This will show if it is using the correct server:-

```
# nslookup
```

```
> buzz
```

```
Server:      192.168.200.201
```

```
Address:    192.168.200.201#53
```

```
Name:  buzz.fatrain.com
```

```
Address: 192.168.200.122
```

```
>
```

- Set a fully-qualified hostname:-

```
# hostnamectl set-hostname buzz.fatrain.com
```

```
*      Install the ipa-client package:-
```

```
# yum install ipa-client
```

```
*      Now run the ipa-client-install command:-
```

```
# ipa-client-install --mkhomedir --enable-dns-updates \
  --force-ntpd
```

```
Discovery was successful!
```

```
Client hostname: buzz.fatrain.com
```

```
Realm: FATRAIN.COM
```

```
DNS Domain: fatrain.com
```

```
IPA Server: heron.fatrain.com
```

```
BaseDN: dc=fatrain,dc=com
```

Enterprise Linux 7 Update

FreeIPA - Joining the Kerberos realm

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

User authorized to enroll computers: **admin**

Password for admin@FATRRAIN.COM: **abc12345**

Successfully retrieved CA cert

Subject: CN=Certificate Authority,O=FATRRAIN.COM

Issuer: CN=Certificate Authority,O=FATRRAIN.COM

Valid From: Mon Jul 04 05:59:17 2016 UTC

Valid Until: Fri Jul 04 05:59:17 2036 UTC

Enrolled in IPA realm FATRRRAIN.COM

Created /etc/ipa/default.conf

New SSSD config will be created

Configured sudoers in /etc/nsswitch.conf

Configured /etc/sss/sss.conf

Configured /etc/krb5.conf for IPA realm FATRRRAIN.COM

trying https://heron.fatrain.com/ipa/json

Forwarding 'ping' to json server 'https://heron.fatrain.com/ipa/json'

Forwarding 'ca_is_enabled' to json server 'https://heron.fatrain.com/ipa/json'

Systemwide CA database updated.

Enterprise Linux 7 Update

FreeIPA - Joining the Kerberos realm

Added CA certificates to the default NSS database.

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://heron.fatrain.com/ipa/json'

SSSD enabled

Configured /etc/openldap/ldap.conf

NTP enabled

Configured /etc/ssh/ssh_config

Configured /etc/ssh/sshd_config

Configuring fatrain.com as NIS domain.

Client configuration complete.

- Now we need to carry further commands on the FreeIPA server.
- We are going to create a service principal for server buzz, which is an identity that Kerberos can authenticate when we set buzz up as an NFS server.
- On the FreeIPA server heron:-

```
# ipa service-add
```

```
Principal: nfs/buzz.fatrain.com
```

```
-----  
Added service "nfs/buzz.fatrain.com@FATRRAIN.COM"  
-----
```

```
Principal: nfs/buzz.fatrain.com@FATRRAIN.COM
```

```
Managed by: buzz.fatrain.com
```

* Where *buzz* is the NFS server.

Enterprise Linux 7 Update

FreeIPA - Joining the Kerberos realm

- Now back on the client *buzz*:-

```
# klist -k
```

```
Keytab name: FILE:/etc/krb5.keytab
```

```
KVNO Principal
```

```
-----  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM
```

- Make sure your Kerberos ticket is still valid:-

```
# klist
```

- If you get:-

```
klist: Credentials cache keyring 'persistent:0:0' not found
```

- Then it has expired, so:-

```
# kinit admin
```

```
Password for admin@FATRRAIN.COM: abc12345
```

```
# klist
```

```
Ticket cache: KEYRING:persistent:0:0
```

```
Default principal: admin@FATRRAIN.COM
```

```
Valid starting    Expires          Service principal  
07/05/2016 11:10:37 07/06/2016 11:10:33 krbtgt/  
FATRRAIN.COM@FATRRAIN.COM
```

Enterprise Linux 7 Update

FreeIPA - Joining the Kerberos realm

- Now run the following on *buzz*:-

```
# ipa-getkeytab -s heron.fatrain.com -p nfs/buzz.fatrain.com \  
-k /etc/krb5.keytab
```

Keytab successfully retrieved and stored in: /etc/krb5.keytab

```
# klist -k
```

Keytab name: FILE:/etc/krb5.keytab

KVNO Principal

```
-----  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 host/buzz.fatrain.com@FATRRAIN.COM  
1 nfs/buzz.fatrain.com@FATRRAIN.COM  
1 nfs/buzz.fatrain.com@FATRRAIN.COM  
1 nfs/buzz.fatrain.com@FATRRAIN.COM  
1 nfs/buzz.fatrain.com@FATRRAIN.COM
```

- Repeat the above process for any other NFS servers that you may wish to create.
- We can now proceed to set up Kerberised NFS services between servers and clients.

Enterprise Linux 7 Update

FreeIPA - Using the Kerberised logins

- Having run the *ipa-client-install* command on *buzz*, we should be able to login as users known only on the FreeIPA server.
- Note that the area of preparing a system for remote authentication is tricky, and you may see mention of doing this using a number of other tools, for example:-
 - * **authconfig** - a CLI interface.
 - * **authconfig-tui** - a menu driven text interface
 - * **authconfig-gtk** - a graphical version of the above.
- In fact, using such a tool is a requirement of the certification exams, and we will see an example soon.
- For now, we'll examine logging in as a FreeIPA user.
- Although we created a couple of users, there are no home directories for them, so we can:-
 - * Manually create the home directory.
 - * Have it created automatically the first time the user logs in.
- In most installations, manual creation would probably be preferred, along with some sort of availability via NFS perhaps.

Enterprise Linux 7 Update

FreeIPA - Using the Kerberised logins

- To find out if our FreeIPA client knows about the user accounts:-

```
# getent passwd eve
```

```
eve:*:1108000005:1108000005:Eve Smith:/home/eve:/bin/bash
```

```
# getent passwd adam
```

```
adam:*:1108000003:1108000003:Adam Smith:/home/adam:/bin/sh
```

- Notice what happens if we *su* to user *eve*:-

```
# su - eve
```

```
Creating home directory for eve.
```

```
Attempting to create directory /home/eve/perl5
```

- * The message about */home/eve/perl5* is because the *perl-homedir* package is installed - nothing to do with our activities.
 - * Note how the home directory is automatically created; this is through a PAM module.
- To manually make a home directory, this time for *adam*:-

```
# mkdir /home/adam
```

```
# chown adam /home/adam
```

- Now login as *adam* or use *su - adam*.

Enterprise Linux 7 Update

FreeIPA - Using the Kerberised logins

- The users should also be able to change their passwords.
- If we run *klist* as *eve* after a login (not an *su*):-

\$ *klist*

Ticket cache: KEYRING:persistent:1108000005:krb_ccache_t8g6wja

Default principal: eve@FATRRAIN.COM

Valid starting	Expires	Service principal
07/05/2016 13:23:43	07/06/2016 13:23:42	krbtgt/FATRRAIN.COM@FATRRAIN.COM