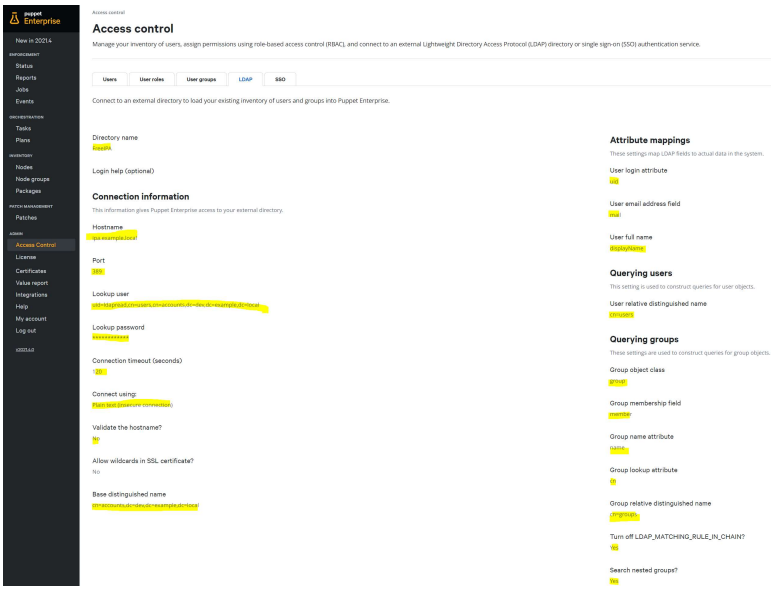
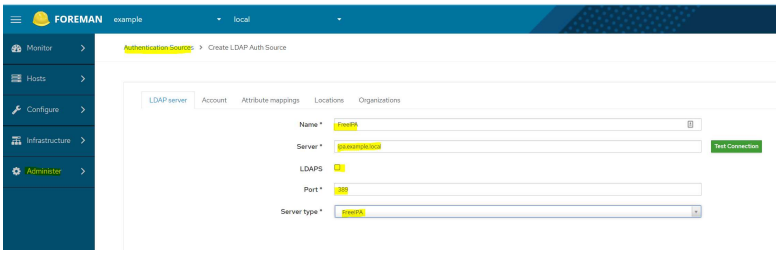
Configure FreeIPA LDAP User Authentication for PE and Foreman

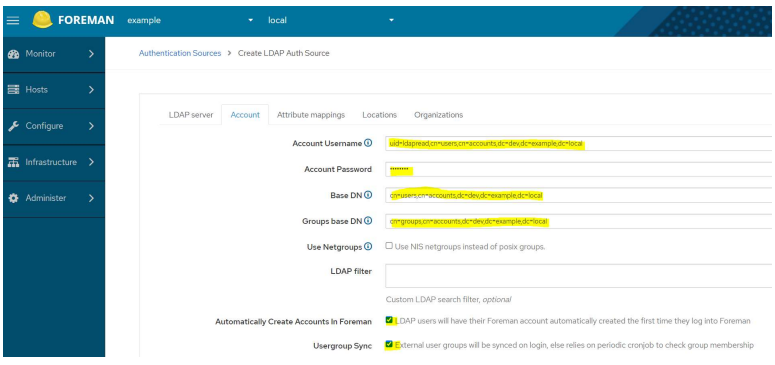
. First create a 'LookUp' FreeIPA account called '**ldapread**' (or it can be any name), set its loginShell to '/usr/sbin/nologin'.
. For PE: **Admin / Access Control / LDAP**



. For Foreman: **Administer / Authentication Source**
1st tab: LDAP Server
Name: **FreeIPA**
Server: **ipa.example.local**
LDAPS: **unchecked**
Port: **389**
Server type: **FreeIPA**



2nd tab: Account
Account Username: **uid=ldapread,cn=users,cn=accounts,dc=dev,dc=example,dc=local**
Account Password: ********
Base DN: **cn=users,cn=accounts,dc=dev,dc=example,dc=local**
Group base DN: **cn=groups,cn=accounts,dc=dev,dc=example,dc=local**
Automatically Create Accounts in Foreman: **checked**
Usergroup Sync: **checked**

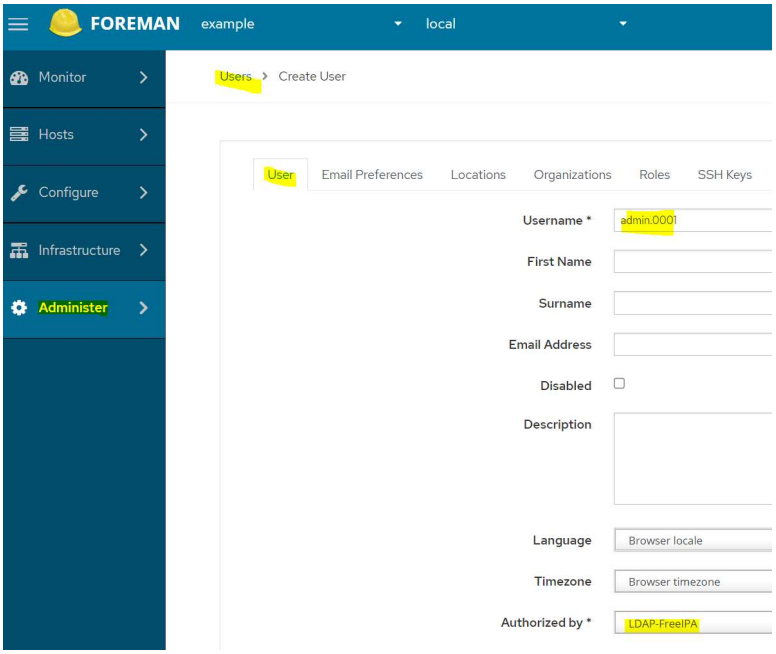


3rd tab: Attribute mappings: take defaults for all fields.
4th tab: Location – **local**
5th tab: Organization - **example**
Back to 1st tab click '**Test Connection**', if it is successful click '**Submit**' to save all tabs.

LDAP Authentication has now been complete, there are two methods to add FreeIPA accounts into PE or Foreman.

The 1st method is obviously preferred.

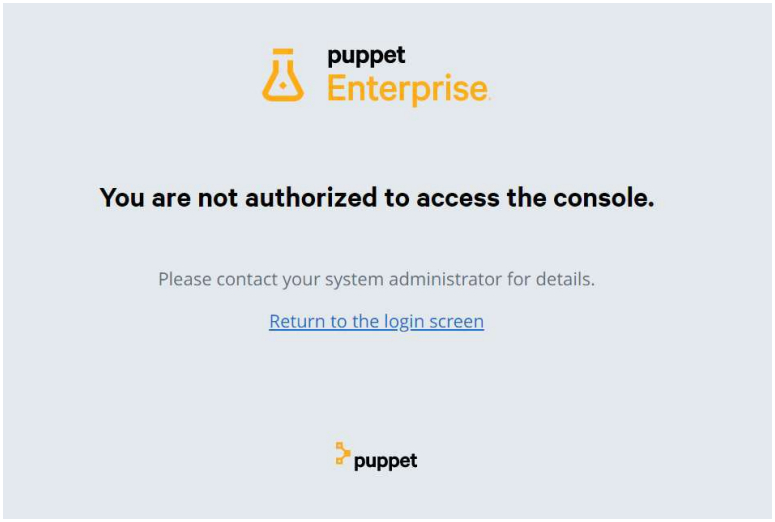
. **1st method: Admin to 'Pre-Add' the FreeIPA account(s),** and grant the appropriate role(s).
For PE: **unfortunately there is no 'Pre-Add' option for 'External' (LDAP) user(s), it is only available for local users.**
For Foreman: example add **admin.0001**
Note: there is no need to to fill-in First Name, Surname and Email Address, as these will be populated when user logs in.
User tab:
Username: **admin.0001**
Authorized by: **LDAP FreeIPA**



Roles tab:
Administrator: **Checked (if so there is no need to select individual role)**
Click '**Submit**'.

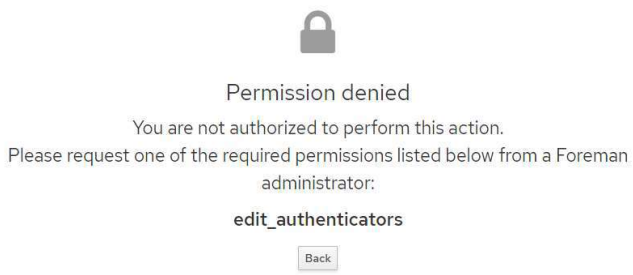
. **2nd Method: user to perform First Time Login using FreeIPA account**, it will display the following screen, do NOT be alarmed.
. What this means the FreeIPA account has been created however the appropriate role(s) has/have not been assigned.
. User should then request PE / Foreman Admin to assign such roles so that subsequent login will be fine.

For PE: example 1st time login admin.0001 at PE GUI



PE Admin can check the AUTO-creation of account, example: admin.0001,
and grant example: Admin role via Admin / Access Control / User Roles / Member users

For Foreman: example 1st time login admin.0001 at Foreman GUI.



Foreman Admin cat check the AUTO-creation of account, example admin.0001 and grant Admin role via Edit User.
Subsequent login by admin.0001 to PE or Foreman GUI will be fine.