

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**

Puppet Enterprise

Free IP 2024.4

Administration

- Status
- Reports
- Jobs
- Events

System resources

- Tasks
- Plans

Environment

- Hosts
- Node groups
- Package sets

Admin

- Access control
- License
- Certificates
- Usage report
- Integrations
- Help
- My account
- Log out

Logout

Access control

Manage your inventory of users, assign permissions using role-based access control (RBAC), and connect to an external Lightweight Directory Access Protocol (LDAP) directory or single sign-on (SSO) authentication service.

UsersUser rolesUser groupsLDAPSSO

Connect to an external directory to load your existing inventory of users and groups into Puppet Enterprise.

Directory name
example

Login help (optional)
No

Connection Information
This information gives Puppet Enterprise access to your external directory.

Hostname
example

Port
389

Lookup user
ldapread

Lookup password
ldapread

Connection timeout (seconds)
300

Connect using:
ldap://example.com:389

Validate the hostname?
No

Allow wildcards in SSL certificate?
No

Base distinguished name
cn=users,cn=accounts,dc=example,dc=local

Attribute mappings
These settings map LDAP fields to actual data in the system.

User login attribute
uid

User email address field
No

User full name
cn

Querying users
This setting is used to construct queries for user objects.

User relative distinguished name
cn

Querying groups
These settings are used to construct queries for group objects.

Group object class
posixGroup

Group membership field
member

Group name attribute
cn

Group lookup attribute
cn

Group relative distinguished name
cn

Turn off LDAP_MATCHING_RULE_IN_CHAIN?
No

Search nested groups?
No

- . For Foreman: **Administer / Authentication Source**

1st tab: LDAP Server

Name: **FreeIPA**
Server: **ipa.example.local**
LDAPS: **unchecked**
Port: **389**
Server type: **FreeIPA**

FOREMANexamplelocal

MonitorHostsConfigureInfrastructureAdminister

Authentication Sources>Create LDAP Auth Source

LDAP serverAccountAttribute mappingsLocationsOrganizations

Name *
FreeIPA

Server *
ipa.example.local

LDAPS
No

Port *
389

Server type *
FreeIPA

Test Connection

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**

FOREMANexamplelocal

MonitorHostsConfigureInfrastructureAdminister

Authentication Sources>Create LDAP Auth Source

LDAP serverAccountAttribute mappingsLocationsOrganizations

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

Groups base DN *
cn=groups,cn=accounts,dc=dev,dc=example,dc=local

Use Netgroups
No

LDAP filter
Custom LDAP search filter, optional

Automatically Create Accounts in Foreman
Yes

Usergroup Sync
Yes

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 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**

The screenshot shows the Foreman Admin web interface. The top navigation bar is blue with the 'FOREMAN' logo and the text 'example' and 'local'. The left sidebar contains a menu with icons and labels: Monitor, Hosts, Configure, Infrastructure, and Administer (highlighted in yellow). The main content area is titled 'Users > Create User'. Below this, there are tabs for 'User', 'Email Preferences', 'Locations', 'Organizations', 'Roles', and 'SSH Keys'. The 'User' tab is active. The form contains the following fields: 'Username *' with the value 'admin.0001', 'First Name', 'Surname', 'Email Address', 'Disabled' (checkbox), 'Description', 'Language' (dropdown with 'Browser locale'), 'Timezone' (dropdown with 'Browser timezone'), and 'Authorized by *' with the value 'LDAP-FreeIPA'.

Roles tab:

Administrator: **Checked (if so there is no need to select individual role)**

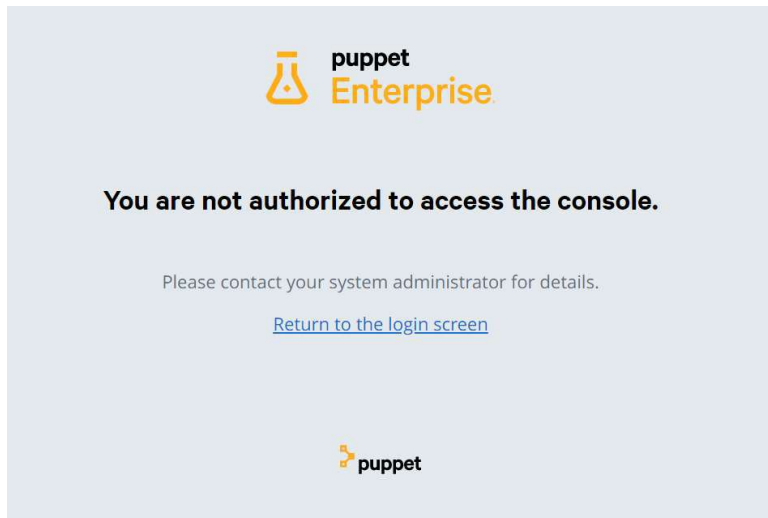
Click '**Submit**'.

. **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.

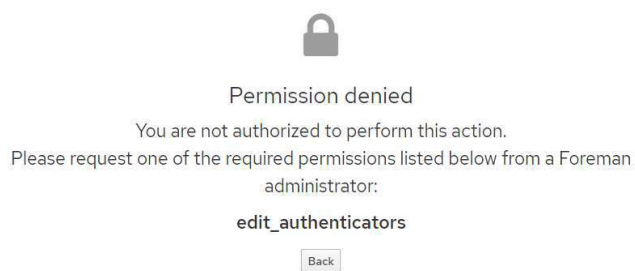
. User should then request PE / Foreman Admin to assign such roles so that subsequent login will be fine.

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.