Internal Notes on PBX and OpenLDAP

Note: OpenLDAP is currently in EDGE

Theory of use

- PBX User Manager module supports multiple LDAP directories.
    - Single LDAP directory must use top level OU in order to sync
    - If there are multiple OU, then admin would create multiple LDAP directories for each OU.

- PBX username must be based on "CN"
    - CN fields must NOT contain a space.
    - This will break Chat feature.
    - Furthermore, LDAP protocol can only authenticate the user based on CN

- Mandatory LDAP fields
    - telephoneNumber - the telephone number binds the LDAP user to an existing extension on the PBX
    - userPassword – PBX authenticates the user via LDAP using the password field

Installation

Update to latest User Manager module.
Minimum Version: 13.0.76.4

- GUI mode
    - Log into the GUI Module Admin
    - Update User Manager module to latest.
        - Minimum Framework version 13.0.191.13

- Console Mode
    - Log into SSH
    - Run
        - fwconsole ma downloadinstall --edge userman
        - fwconsole ma downloadinstall framework --tag 13.0.191.13

PBX Extensions

Admin has two choices on how to manage extensions.

- Auto create
    - LDAP synchronization can auto create extensions based on "telephoneNumber" field in the openLDAP
    - This is controlled by "Create Missing Extensions" in the LDAP Directory configuration.
- Manually create
    - Admin can disable the "Create Missing Extensions" and manually create extensions in the PBX.
    - This way only specific LDAP users will be bound to the PBX extensions based on "telephoneNumber" field.
    - The rest of the users will be imported as contacts only.

Create a LDAP Directory

- Log into GUI
- Navigate to User Management
- Click on Directories: Click on Add

    - General Section
        - Directory Type: OpenLdap Directory
            - Note: do not select (Legacy) one.
        - Directory Name: Specify arbitrary name
        - Enable Directory: Select Yes
        - Synchronize: Default 1h

- Directory Settings

    - Secure connection type: None (Default)
    - Host: OpenLDAP server IP
    - Port: OpenLDAP port number (Default is 389)
    - Bind DN: Must be set to admin LDAP credentials
        - example: cn=admin,dc=companydnsname,dc=com
    - Password: Admin password
    - Base DN: Must be set to base LDAP DN
        - example: dc=companydnsname,dc=com
    - Status: Displays the status of the ldap connection, will update after the LDAP configuration is submitted.

- Operational Settings
    - Create Missing Extensions:
        - PBX can auto create extensions based on the "telephoneNumber" field.
        - Default behavior is not do auto create and let the PBX admin create extensions manually before sync.
    - Manage Groups Locally: Set to YES (Default)
        - This option will allow admin to create a group for the LDAP directory into which all LDAP users can be added to.
        - This is an easy way to add permissions to allLDAP directory users such as: Zulu, UCP etc.

- User Configuration
    - User DN: Must be populated with top level OU
        - example: ou=Engineering Department
    - User object class: inetOrgPerson
    - user object filter: (objectclass=inetOrgPerson)
    - User name attribute: cn
        - Must be set to cn this is the only option
    - User extension Link attribute: telephoneNumber
        - This will bind the user to the existing extension, or will auto create extension if above "Create Missing Extensions" is enabled.

    - The Rest of the User Configuration fields should be set based on OpenLDAP user fields defined in LDAP directory.

- Group Configuration
    - Leave as default as we will use Manage Groups Locally.

- Click Submit to apply settings.

- Specify the LDAP as Default directory in the Directory List.

- On page refresh you the LDAP Status field should be green with status Connected.

Create a LDAP user group

- From the GUI
- Navigate to User Management
- Click on Groups
    - Click on Group Filter ("All Directories")
    - Select the LDAP directory that was just created in above step
        - Click on Add Button.
        - Specify a group name
        - Select ALL users and add them to the group
        - Enable all PBX features such as Contacts, UCP, Zulu, XMPP
            - If contacts do not work in Zulu, you have not enabled Contacts in this section
                - For contact groups select ALL to allow all contacts in Zulu and UCP
            - If you cannot log into Zulu or UCP then you might not have permissions in this section.
        - Save
    - Note: If you cannot add a group for a Directory you did not set "Manage Groups Locally" to YES in the LDAP Directory configuration above.

Sync LDAP users

- Log into SSH
- List all userman directories
    - fwconsole userman --list
- Run sync on the directory ID that relates to LDAP

- fwconsole userman --syncall --force --verbose
- Reload Asterisk
  - fwconsole r   #This step is must be done or Zulu Softphone will not work
- At this point all users are sync
  - Log back into GUI
  - Navigate to User Management
  - Click on Users
    - Select on LDAP Directory filter
    - Admin should see all new imported users.

Change Asterisk HTTP max settings

- Log into GUI
- Advanced Settings
- Session Limit: set to 10000
- Apply