Secure Domain II: LDAP Authentifizierung an Microsoft AD

Software-Pakete nachinstallieren

- Software nachladen per `apt`:

```
apt install dirmngr prosody-modules
```

Benutzer im LDAP für Bind anlegen

```
* Anlegen eines Benutzer für LDAP Bind, z.B.
''CN=jitsi_ldap,OU=Administration,DC=example,DC=local''
```

- ggf. Anlegen einer Gruppe für Videokonferenzen

Prosody konfigurieren

```
* Anlegen einer Datei ''/etc/prosody/conf.d/ldap.cfg.lua''
```

```
-- Authentication configuration --

authentication = 'ldap2' -- Indicate that we want to use LDAP for
authentication
ldap = {
    hostname      = '192.168.1.2:389',    -- LDAP server location
    use_tls       = false,      -- disabled
    bind_dn       = 'CN=jitsi_ldap,OU=Administration,DC=example,DC=local', -
- Bind DN for LDAP authentication (optional if anonymous bind is supported)
    bind_password = 'secret', -- Bind password (optional if anonymous bind
is supported)
    user = {
      basedn        = 'DC=DOMAIN,DC=LOCAL',
      -- filter        =
'(&(objectClass=Person)(memberof=CN=Videoconference-
Users,OU=videoconference,OU=Groups,OU=SUB,DC=EXAMPLE,DC=LOCAL))',
      filter = '(objectClass=Person)',
      usernamefield = 'sAMAccountname',
      namefield     = 'cn',
    },
}
```

- Anmerkung: man könnte auch noch eine Gruppe einrichten, zu der ein Benutzer gehören muß, der eine Konferenz starten will. Der Filter hierfür ist oben auskommentiert

- Weiter geht mit Änderungen an der `/etc/prosody/conf.d/meet.domain.net.cfg.lua`:
  - die *anonymous* Authentication auskommentieren und durch `ldap2` ersetzen
  - den Eintrag des virtuellen Host auf `enabled` setzen
  - `consider_bosh_secure = true` ergänzen

```
consider_bosh_secure = true;

VirtualHost "meet.domain.net"
        enabled = true -- Remove this line to enable this host
        -- authentication = "anonymous"
        authentication = "ldap2"
```

- Schauen das `bosh` aktiv ist

```
        -- we need bosh
        modules_enabled = {
            "bosh";
            "pubsub";
            "ping"; -- Enable mod_ping
        }

        c2s_require_encryption = false
```

- sollen sich auch nicht-authentifizierte Benutzer als Gäste an bestehende Konferenzen verbinden können, einen Virtual Host `guest.meet.example.net` einrichten:

```
VirtualHost "guest.meet.example.net"
    authentication = "anonymous"
    c2s_require_encryption = false
```

Kicofo konfigurieren

- in der `/etc/jitsi/jicofo/sip-communicator.properties` ergänzen:

```
org.jitsi.jicofo.auth.URL=XMPP:meet.example.net
net.java.sip.communicator.service.gui.ALWAYS_TRUST_MODE_ENABLED=true
```

Jitsi Meet konfigurieren

- weiter die `/etc/jitsi/meet/meet.example.net-config.js` bearbeiten und ggf. die Domain für `anonymous` Registrierung eintragen

```
        // XMPP domain.
        domain: 'meet.example.net',

        // When using authentication, domain for guest users.
        anonymousdomain: 'guest.meet.example.net',
```