Kimai

- Manual de Integración LDAP Active Directory con Kimai 2.67
- Integración de Ldap

Manual de Integración LDAP Active Directory con Kimai 2.67

Guía completa de instalación, configuración y validación para replicación en nuevos ambientes.

1. Objetivo

Implementar Kimai integrado con Active Directory mediante LDAP StartTLS para permitir autenticación centralizada, creación automática de usuarios y asignación dinámica de roles mediante grupos de Active Directory.

2. Arquitectura

```
Usuarios
   |
   ▼
Apache
   |
   ▼
Kimai
   |
   ▼
LDAP StartTLS
   |
   ▼
Active Directory
```

3. Información del Ambiente

Componente	Valor

Sistema Operativo	Debian 12
Aplicación	Kimai 2.67
Servidor Web	Apache2
Base de Datos	MariaDB
Dominio AD	ghz.mx
Controlador de Dominio	192.168.30.2
Puerto LDAP	389
Seguridad LDAP	StartTLS

4. Instalación de Paquetes Base

```
apt update

apt install apache2 mariadb-server unzip curl wget git -y
```

5. Instalación de PHP

```
apt install -y \
php \
php-cli \
php-common \
php-intl \
php-mysql \
php-gd \
php-xml \
php-mbstring \
php-curl \
php-zip \
php-bcmath \
php-imap \
php-ldap
```

6. Instalación Composer

```
apt install composer -y
```

7. Instalación Kimai

```
cd /opt

wget https://www.kimai.org/download/kimai-latest.zip

unzip kimai-latest.zip

mv kimai* kimai

cd /opt/kimai

composer install --no-dev --optimize-autoloader
```

8. Configuración MariaDB

```
mysql -u root -p

CREATE DATABASE kimai_db;

CREATE USER 'kimai'@'localhost'
IDENTIFIED BY 'PasswordSeguro';

GRANT ALL PRIVILEGES
ON kimai_db.*
TO 'kimai'@'localhost';

FLUSH PRIVILEGES;
```

9. Instalación LDAP

Verificar módulo PHP LDAP

```
php -m | grep ldap
```

Resultado:

```
ldap
```

Verificar laminas-ldap

```
find /opt/kimai/vendor -iname "*ldap*"
```

Resultado esperado:

```
vendor/laminas/laminas-ldap
```

10. Validación LDAP

Prueba de autenticación

```
ldapwhoami \
-ZZ \
-H ldap://192.168.30.2 \
-D "kimai@ghz.mx" \
-W
```

Resultado esperado:

```
u:GHZ\kimai
```

Búsqueda de usuario

```
ldapsearch \
-ZZ \
-H ldap://192.168.30.2 \
-D "kimai@ghz.mx" \
-W \
-b "OU=Usuarios,OU=ghz.mx,DC=ghz,DC=mx" \
"(sAMAccountName=soporte)"
```

11. Creación de Grupos en Active Directory

Grupo AD	Rol Kimai
Kimai_Admins	ROLE_SUPER_ADMIN
Kimai_TeamLead	ROLE_TEAMLEAD
Kimai_Users	ROLE_USER

12. Configuración local.yaml

Archivo:

```
/opt/kimai/config/packages/local.yaml
```

```
kimai:
  ldap:
    activate: true

    connection:
      host: 192.168.30.2
      port: 389

      username: "kimai@ghz.mx"
      password: "PASSWORD"

      accountDomainName: "ghz.mx"
      accountDomainNameShort: "GHZ"

      accountCanonicalForm: 3

      accountFilterFormat: "(&(objectClass=user)(sAMAccountName=%s))"

      useStartTls: true
      useSsl: false

      bindRequiresDn: false

    user:
      baseDn: "OU=Usuarios,OU=ghz.mx,DC=ghz,DC=mx"

      filter: "(&(objectCategory=Person)(objectClass=User))"

      usernameAttribute: sAMAccountName

      attributes:
        - { ldap_attr: userprincipalname, user_method: setEmail }
        - { ldap_attr: displayname, user_method: setAlias }
        - { ldap_attr: samaccountname, user_method: setUserIdentifier }

    role:
      baseDn: "OU=Usuarios,OU=ghz.mx,DC=ghz,DC=mx"

      filter: "(objectClass=group)"

      groups:
        - { ldap_value: Kimai_Admins, role: ROLE_SUPER_ADMIN }
        - { ldap_value: Kimai_TeamLead, role: ROLE_TEAMLEAD }
        - { ldap_value: Kimai_Users, role: ROLE_USER }
```

13. Configuración Security.yaml

```
secured_area:

    kimai_ldap: ~

    provider: chain_provider

    form_login:
        check_path: security_check
        login_path: login
```

14. Aplicar Configuración

```
cd /opt/kimai

php bin/console cache:clear

systemctl restart apache2
```

15. Validaciones

Validar LDAP

```
php bin/console debug:config kimai ldap
```

Validar Firewall LDAP

```
php bin/console debug:firewall secured_area
```

Validar Login

```
https://proyectos.ghz.mx
```

Usuario:

```
soporte@ghz.mx
```

16. Problemas Encontrados

Error:

```
Credenciales no válidas
```

Solución: Autenticarse utilizando el correo UPN:

```
soporte@ghz.mx
```

Error:

```
500 Internal Server Error
```

Solución: Cambiar:

```
ldap_attr: mail
```

por:

```
ldap_attr: userprincipalname
```

Error:

```
Class DoctrineFixturesBundle not found
```

Solución: Regresar a producción:

```
APP_ENV=prod
APP_DEBUG=0
```

17. Consultas Útiles

Usuarios Kimai

```
php bin/console doctrine:query:sql --force-fetch \
"SELECT username,email,auth FROM kimai2_users"
```

Listar Usuarios

```
php bin/console kimai:user:list
```

Crear Usuario

```
php bin/console kimai:user:create
```

18. Resultado Final

 LDAP operativo Active Directory integrado Grupos sincronizados Usuarios creados automáticamente Login corporativo funcional Administración mediante grupos AD Plataforma lista para producción

Implementación Exitosa

Kimai 2.67 + Active Directory LDAP + StartTLS

Documento técnico para replicación en ambientes DEV, QA y PRODUCCIÓN.

Integración de Ldap

Manual de Integración LDAP Active Directory con Kimai 2.67

Versión: Producción Validada

Objetivo: Integrar Kimai con Microsoft Active Directory mediante LDAP StartTLS, permitiendo autenticación corporativa, creación automática de usuarios y asignación dinámica de roles mediante grupos LDAP.

---

1. Arquitectura

```
Usuarios
    |
    ▼
Apache / PHP
    |
    ▼
Kimai 2.67
    |
    ▼
LDAP StartTLS (389)
    |
    ▼
Microsoft Active Directory
```

---

2. Requisitos

- Kimai 2.67

- PHP 8.2 o superior
- Apache o Nginx
- MariaDB
- Composer
- Active Directory
- Puerto TCP 389
- StartTLS habilitado

---

3. Instalación del soporte LDAP para PHP

Debian / Ubuntu

```
apt update

apt install php-ldap -y
```

AlmaLinux / Rocky Linux

```
dnf install php-ldap -y
```

Validar módulo LDAP

```
php -m | grep ldap
```

Resultado esperado:

```
ldap
```

FPM y CLI utilizan configuraciones diferentes. Siempre validar que el módulo LDAP aparezca cargado mediante `php -m`.

---

4. Instalación de Laminas LDAP

Kimai requiere la librería Laminas LDAP para integrarse con Active Directory.

```
cd /var/www/kimai

composer require laminas/laminas-ldap \
--update-no-dev \
--optimize-autoloader
```

Validación

```
composer show | grep laminas
```

Resultado esperado:

```
laminas/laminas-ldap
```

También puede validarse:

```
find vendor -iname "*ldap*"
```

Resultado:

```
vendor/laminas/laminas-ldap
```

---

5. Configuración TLS para LDAP

Cuando el controlador de dominio utiliza certificados autofirmados:

AlmaLinux / Rocky

```
echo "TLS_REQCERT never" > /etc/openldap/ldap.conf
```

Debian / Ubuntu

```
echo "TLS_REQCERT never" > /etc/ldap/ldap.conf
```

Validación

```
cat /etc/openldap/ldap.conf
```

Resultado esperado:

```
TLS_REQCERT never
```

---

6. Validaciones LDAP

Validar usuario de servicio

```
ldapwhoami -ZZ \
-H ldap://172.16.2.201 \
-D "kimai@bpm.mty" \
-W
```

Resultado esperado:

```
u:BPM\kimai
```

Validar usuario final

```
ldapwhoami -ZZ \
-H ldap://172.16.2.201 \
-D "rsanchez@bpm.mty" \
-W
```

Resultado esperado:

```
u:BPM\rsanchez
```

Buscar usuario LDAP

```
ldapsearch -ZZ \
-H ldap://172.16.2.201 \
-D "kimai@bpm.mty" \
-W \
-b "OU=Usuarios,OU=BPM-MTY,DC=bpm,DC=mty" \
"(sAMAccountName=rsanchez)"
```

---

7. Grupos LDAP en Active Directory

Grupo AD	Rol Kimai
Kimai_Admins	ROLE_SUPER_ADMIN
Kimai_TeamLead	ROLE_TEAMLEAD
Kimai_Users	ROLE_USER

8. Configuración LDAP de Kimai

Archivo:

```
/var/www/kimai/config/packages/local.yaml
```

```
kimai:
    ldap:
        activate: true

        connection:
            host: 172.16.2.201
            port: 389

            username: "kimai@bpm.mty"
            password: "PASSWORD"

            accountDomainName: "bpm.mty"
            accountDomainNameShort: "BPM"

            accountFilterFormat: "(&(objectClass=Person)(sAMAccountName=%s))"

            useStartTls: true
            useSsl: false

            bindRequiresDn: false

        user:
            baseDn: "OU=Usuarios,OU=BPM-MTY,DC=bpm,DC=mty"

            filter: "(&(objectClass=Person))"

            usernameAttribute: samaccountname

            attributesFilter: "(objectClass=Person)"

            attributes:
                - { ldap_attr: mail, user_method: setEmail }
                - { ldap_attr: displayname, user_method: setAlias }
                - { ldap_attr: samaccountname, user_method: setUserIdentifier }

        role:
```

```
            baseDn: "OU=Usuarios,OU=BPM-MTY,DC=bpm,DC=mty"

            filter: "(&(objectClass=group))"

            groups:
                - { ldap_value: Kimai_Admins, role: ROLE_SUPER_ADMIN }
                - { ldap_value: Kimai_Admins, role: ROLE_TEAMLEAD }
                - { ldap_value: Kimai_Admins, role: ROLE_USER }
                - { ldap_value: Kimai_Users, role: ROLE_USER }

            usernameAttribute: dn
            nameAttribute: cn
            userDnAttribute: member
```

---

9. Configuración Security.yaml

Archivo:

```
/var/www/kimai/config/packages/security.yaml
```

Validar que el proveedor LDAP aparezca primero:

```
chain_provider:
    chain:
        providers:
            - kimai_ldap
            - kimai_internal
```

LDAP debe aparecer antes de kimai_internal.

---

10. Aplicar Configuración

```
cd /var/www/kimai

php bin/console cache:clear

php bin/console cache:warmup
```

Debian

```
systemctl restart apache2
```

AlmaLinux

```
systemctl restart httpd
```

---

11. Validar Sintaxis

```
php bin/console lint:yaml config/packages/local.yaml
```

Resultado esperado:

```
[OK] All YAML files contain valid syntax.
```

---

12. Problemas Encontrados y Soluciones

Error: Strong(er) authentication required

```
useStartTls: true
useSsl: false
```

Error: certificate verify failed

```
echo "TLS_REQCERT never" > /etc/openldap/ldap.conf
```

Error: Credenciales no válidas

Posibles causas:

- Laminas LDAP no instalado.
- Usuario fuera de grupo LDAP.
- chain_provider incorrecto.

Error: 500 Internal Server Error

Diagnóstico:

```
ausearch -m avc -ts recent
```

Causa encontrada:

```
SELinux bloqueando cache y logs de Kimai.
```

Validar SELinux

```
getenforce
```

Prueba temporal

```
setenforce 0
```

Corrección permanente

```
dnf install -y policycoreutils-python-utils

semanage fcontext -a -t httpd_sys_rw_content_t \
"/var/www/kimai/var(/.*)?"

restorecon -Rv /var/www/kimai/var
```

---

13. Validaciones Finales

Ver usuarios LDAP creados

```
php bin/console doctrine:query:sql --force-fetch \
"SELECT username,email,auth FROM kimai2_users"
```

Listar usuarios

```
php bin/console kimai:user:list
```

Acceso Web

```
https://horas.bpmconsulting.cloud
```

Usuario:

```
rsanchez
```

Contraseña:

```
Contraseña de Active Directory
```

- LDAP operativo
- Active Directory integrado
- StartTLS funcionando
- Laminas LDAP instalado
- Usuarios creados automáticamente
- Roles asignados mediante grupos LDAP
- Login corporativo funcional
- Kimai listo para Producción