Itop

- Manual Técnico: Integración de iTop con Active Directory (LDAPS)

Manual Técnico: Integración de iTop con Active Directory (LDAPS)

Manual Técnico: Integración de iTop con Active Directory (LDAPS)

Este documento detalla el procedimiento paso a paso, los ajustes necesarios en el sistema operativo, la configuración de la aplicación y las medidas de seguridad recomendadas para integrar **iTop** con un controlador de dominio de **Active Directory** utilizando comunicaciones cifradas (LDAPS).

1. Requisitos y Consideraciones de Seguridad en Active Directory

Por motivos de cumplimiento y seguridad, las directivas modernas de Active Directory bloquean las consultas de autenticación en texto plano a través del puerto 389. Por ello, se deben cumplir los siguientes puntos:

- **Cifrado Obligatorio (LDAPS):** El controlador de dominio exige integridad de canal, lo que obliga a realizar las consultas a través del puerto seguro **636** mediante SSL/TLS.
- **Cuenta de Servicio:** Se requiere una cuenta dedicada en el directorio (por ejemplo, `itop_svc@bpm.mty`) con privilegios de lectura sobre los objetos para efectuar las búsquedas de usuarios y validaciones de enlace (`bind`).

- **Delimitación de la Base DN:** Identificar la ruta exacta de la Unidad Organizativa (OU) donde se encuentran los usuarios que accederán a la plataforma (ej. `OU=Usuarios,OU=BPM-MTY,DC=bpm,DC=mty`).

2. Configuración de Seguridad en el Servidor Linux (Ubuntu)

Debido al uso del puerto seguro **636**, el servidor de aplicaciones debe configurarse para gestionar correctamente los certificados del dominio.

1. Accede por terminal al servidor donde opera iTop.
2. Abre el archivo de configuración global de LDAP:
   Bash
   ```
   sudo nano /etc/ldap/ldap.conf
   ```
3. Añade o verifica la directiva para omitir restricciones estrictas de cadena de certificados (útil si el AD utiliza certificados internos o autofirmados):
   Plaintext
   ```
   TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
   TLS_REQCERT never
   ```
4. Guarda los cambios y cierra el editor (`Ctrl + O`, luego `Ctrl + X`).

3. Configuración del Módulo en iTop (`config-itop.php`)

La autenticación por directorio se configura dentro del archivo de parámetros de la aplicación (`conf/production/config-itop.php`). Modifica o integra el bloque del módulo `authent-ldap` con la siguiente estructura optimizada:

PHP
```
□'authent-ldap' => array (
□□'host' => 'ldaps://ad.tudominio.com',
□□'port' => 636,
```

```
    'default_user' => 'itop_svc@tudominio.com',
    'default_password' => 'TuPassword',
    'base_dn' => 'OU=Usuarios,OU=BPM-MTY,DC=tudominio,DC=com',
    'user_query' => '(&(objectClass=user)(sAMAccountName=%1$s))',
    'options' => array (
      LDAP_OPT_PROTOCOL_VERSION => 3,
      LDAP_OPT_REFERRALS => 0,
    ),
    'bind_requires_dn' => false,
  ),
```

4. Pruebas de Conexión y Validación (Troubleshooting)

Antes de realizar pruebas en la interfaz web, es indispensable comprobar que la comunicación y la sintaxis de búsqueda funcionan correctamente desde la terminal de Linux mediante `ldapsearch`:

Bash

```
ldapsearch -H ldaps://bpmprdad01.bpm.mty -x -D "itop_svc@bpm.mty" -w "BPMsvcs1#" -b "OU=Usuarios,OU=BPM-MTY,DC=bpm,DC=mty" "(sAMAccountName=maguilar)"
```

- **Resultado Exitoso:** El comando retornará los atributos detallados del usuario consultado en pantalla. Si devuelve un error de certificado o de conexión, verifica la directiva `TLS_REQCERT` y el estado del puerto 636 en la red.

5. Pasos Finales y Buenas Prácticas

1. **Reiniciar PHP-FPM:** Para que el servidor web reconozca los cambios en los certificados y en la configuración, reinicia el servicio PHP desde el panel de control (aaPanel).
2. **Formato de Usuario:** Al iniciar sesión en iTop, los usuarios deben ingresar estrictamente su identificador corto (ej. `maguilar`), el cual corresponde al atributo `sAMAccountName` de Active Directory, omitiendo dominios o sufijos de correo.
3. **Rotación de Credenciales:** En caso de actualizar la contraseña de la cuenta de servicio (`itop_svc`) en el directorio activo, recuerda reflejar inmediatamente el cambio en el parámetro `'default_password'` dentro del archivo de configuración de iTop para evitar interrupciones de acceso.