**赛肯内网ldap代理认证环境搭建指南**

赛肯（北京）科技有限公司

二〇一五年九月

目录

概述 3

一、安装前的准备 4

1、可用的内网服务器 4

2、域名解析的配置 4

3、secken提供的ldap代理模块secken-openldap-2.4.42 4

二、配置secken-openldap-2.4.42 5

1、安装流程 5

2、配置openldap 6

3、配置secken.conf 7

概述

本文为赛肯（北京）科技有限公司为企业提供的企业私有云产品内网系统环境（代理）搭建的指导文档，本文档旨在指导运维人员对其公司的内网环境进行修改，并使之嵌入赛肯公司的私有云产品模块，从而进行企业内网账号的二次验证，保障内网账号安全。

赛肯（北京）科技有限公司为企业提供的企业私有云产品内网系统的代理分为两部分：

1. ldap认证代理。
2. radius认证代理。

本文为ldap认证代理环境搭建的指导文档。

本文旨在对不了解openldap配置的管理员提供一份简单指导，若您已经足够了解openldap的配置，请着重阅读“配置secken-openldap-2.4.42”章节中的“配置secken.conf”一节。其他配置请根据自己需要进行。

本文适用人群：

1. 企业内部内网管理员。
2. 企业内部账号管理员。

*注：本文仅提供关于模块的最小可用代理配置，若想用关于openldap的其他高级功能，请参照openldap的相关文档对其进行配置。本模块基于openldap开发，完全遵循openldap的编译及配置方法。*

# 一、安装前的准备

## 1、可用的内网服务器

请尽量为赛肯内网ldap代理模块单独分配一台服务器（或虚拟机），若没有，也可准备一台已经资源仍然足够的服务器。

## 2、域名解析的配置

请为赛肯内网ldap代理模块所在的服务器分配一个内网的全局域名，供客户端寻找。

## 3、secken提供的ldap代理模块secken-openldap-2.4.42

暂无

## 4、依赖的软件包

libevent

openssl

cyrus-sasl

# 二、配置secken-openldap-2.4.42

## 1、安装流程

#### 解压secken-openldap-2.4.42.tar

tar –xvf secken-openldap-2.4.42.tar

#### 进入secken-openldap-2.4.42

cd secken-openldap-2.4.42

#### 对secken-openldap-2.4.42代码的编译进行configure

*注：本模块是基于openldap开发，安装配置与openldap相同，此处提供的是可供代理使用的最小配置*

./configure \

--prefix=/usr/local/sicken-ldap-proxy \

--with-tls \

--with-cyrus-sasl \

--enable-ldap \

--enable-lmpasswd \

--enable-spasswd \

--enable-crypt \

--enable-bdb=no \

--enable-hdb=no \

--enable-mdb=no   \

--enable-syncprov=no \

--enable-monitor=no \

--enable-relay=no

#### 编译代码

make

make depend

##### 安装代码

make install

至此，模块已经安装到prefix配置指定的位置。

***注意事项：***

1. *请在--prefix字段里设置你所想要的安装路径*
2. *请在./configure之前安装openssl、和cyrus-sasl系列软件包*

## 2、配置openldap

#### 修改slapd.conf

slapd.conf为openldap本身的主配置文件，在这里我们可以配置openldap的代理功能。

slapd.conf在安装目录下的相对位置为：etc/openldap/slapd.conf

修改slapd.conf在文件底部添加字段：



database：此处指明开启openldap的ldap代理功能。

Suffix：指明需要代理的dn

Uri：目的服务器的地址，或域名。

*注：此处可添加多个database，完成不同的dn代理。*

## 3、配置secken.conf

secken.conf是代理模块与内网管理中心之间交互的配置文件，通过此文件的配置，可以打通代理模块与内网管理中心的二次认证通道。

#### 找到secken.conf

secken.conf在安装目录下的相对位置为：etc/openldap/secken.conf

#### secken.conf字段解释



|  |  |
| --- | --- |
| timeout | Proxy向管理中心请求的超时时间，以秒为单位 |
| result\_req\_interval | proxy向管理中心定时查询认证结果的时间间隔 |
| auth\_req\_url | 认证请求接口，由管理中心中心进行配置并提供 |
| result\_req\_url | 认证结果请求接口，由中心进行配置并提供 |
| power\_id | 权限ID，用来标识此proxy的认证权限，由管理中心中心进行配置并提供 |
| power\_key | 权限秘钥，用来标识此proxy唯一，由管理中心进行配置并提供 |

填写以上字段，完成配置

# 三、启动代理

代理可执行文件的位置： 安装目录/libexec/slapd

1. 在命令行./slapd，程序会退回后台执行。若想添加ssl加密，请加启动参数：./slapd –h “ldap:/// ldaps:///”

2、重定向openldap客户端的认证服务器位置，将服务器认证位置指向为代理的位置。

3、在内网管理中心添加账号，使内网用户名对应上洋葱账号。

4、让ldap客户端进行认证操作，此时会有认证推送推送到手机终端进行认证，认证通过后ldap客户端会收到认证成功的消息。

注意：

1. 为防止客户端超时影响用户体验，请在二次认证的认证方式上请尽量选择便捷的认证方式（例如按键确认）
2. 二次验证的过程可能会消耗一定时间，若可能，请尽量延长终端设备的认证超时时间。