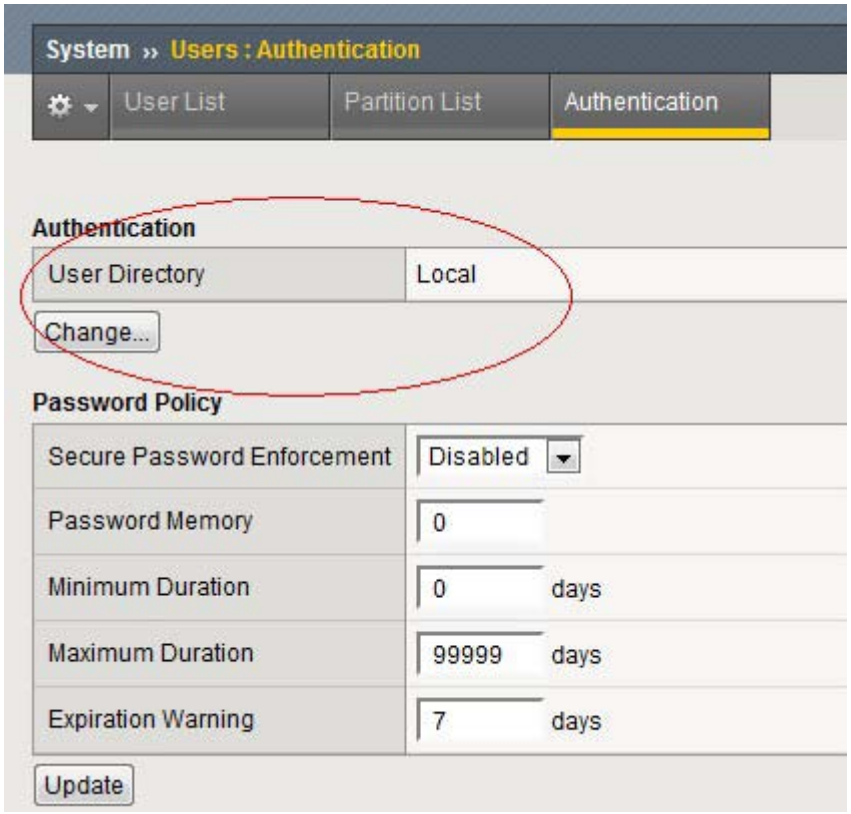
F5 设备管理帐号远程认证、授权之 ldap 版

V10.1 在管理帐号的集中统一验证授权方面有了很大的提高，本文介绍如何实现基于 ldap 进行管理帐号认证及授权。

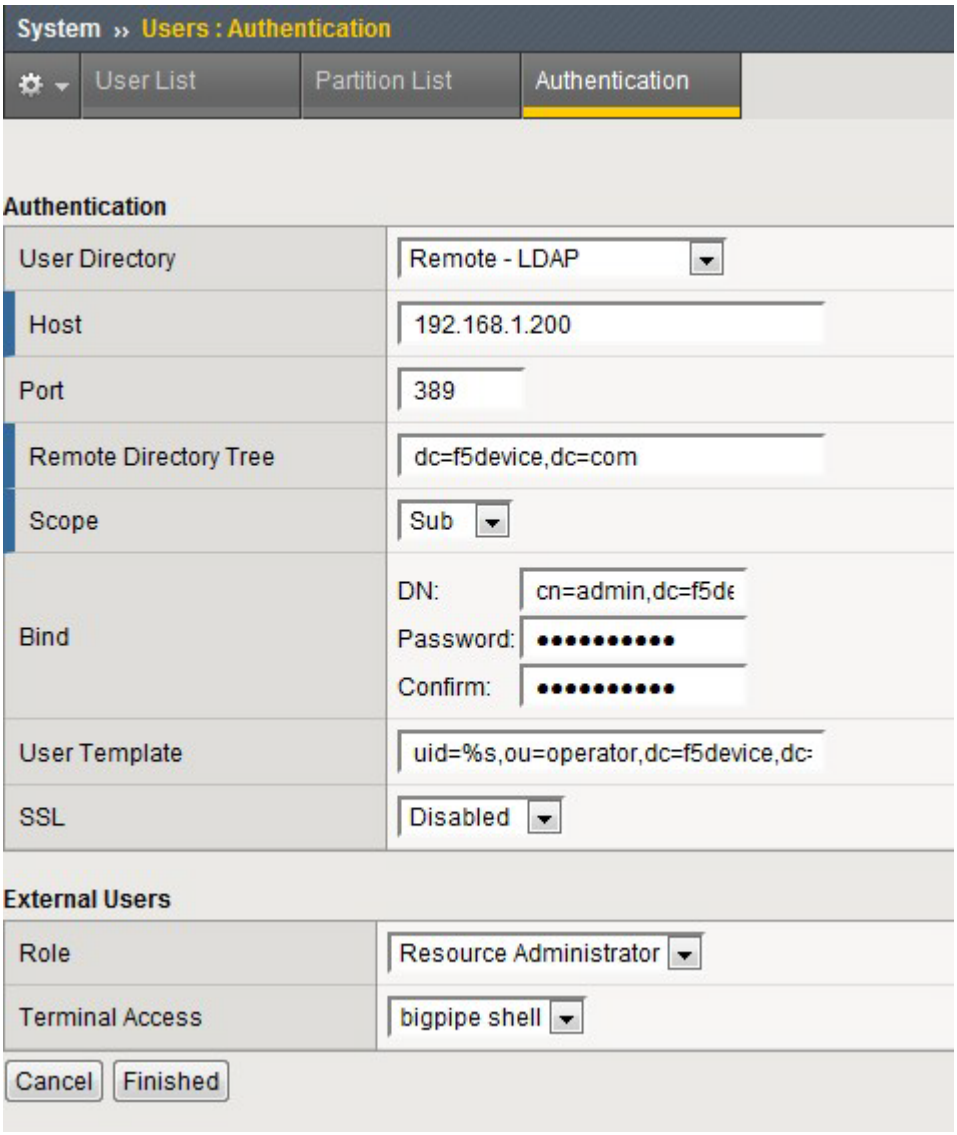
原理：
当用户登录时 F5 能够与 ldap 服务器进行通信，得到 ldap 对身份验证的结果。
如果身份验证失败，拒绝登陆，并在/var/log/secure,/var/log/aduit 日志文件中记录失败信息
如果身份验证通过，则利用 ldap 服务器返回的属性在本地查找对应匹配的 remoterole，根据 remoterole 中的定义赋予用户 console/user partition 以及对应的 role（即系统内置的 guest,operator,manager 等内置的 role 权限），同时记录相关日志
如果身份验证通过，但无法找到匹配的 remoterole，那么使用配置 ldap 时候所指定的“External Users”设置赋权---系统默认为 no access，即默认情况下即使验证通过也禁止访问。

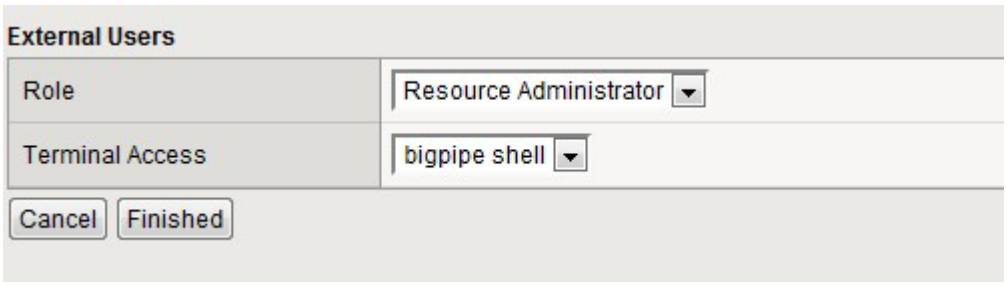
设置方法：
一、F5 部分设置

1. 点击 system-users 菜单进入下图，并点击 change，将验证位置改为 remote-ldap



2.随后将出现如下界面：





解释：

host 处填写 ldap 服务器服务 IP，注意 F5 使用管理口 IP 与验证服务器通信

remote directory tree: 指定 ldap 上登录 F5 的账号在哪个目录树下，例如如果用户都在 ou=f5,dc=f5device,dc=com 下，则这里可以填写 ou=f5,dc=f5device,dc=com。F5 在 BINDrequest 并查到用户后，将会在这个目录下去 filter 登录的账号，ldap 服务器将会返回相关的属性。F5 即可根据属性里的一些定义来关联 remoterole。上图示例中，登录 F5 的用户会在 dc=f5device,dc=com 下的多个 ou 里，所以只用填写 dc=f5device,dc=com 即可。

Scope：------在 scope 所指定的范围内检索账号是否存在

-Sub，意味着 F5 将在 remote directory tre 这个目录下的所有子目录中 filter 所登录的账号。如果帐户风散在 remote directory tree 下的多个层次中，应该选择 sub

-one，意味着 F5 将只检索 remote directory tree 这个目录下的账号，不检索子目录。

-base，选择这个项目将导致 F5 发起的检索只在有权限检索部分的 base object（BIND 中所配置的 DN 的 base directory）中检索

BIND: F5 利用这里配置的 DN 与 ldap 建立 BIND，BIND 成功后 F5 在 ldap 上查询登录的用户，如果查到 ldap 会返回对应的属性，接着 F5 再次发起一个 bindrequest 以验证所提交的密码（默认明文传输）。一般这里配置一个 ldap 存在的用户即可，建议配置 ldap 的管理员账号。

User template：和 BIND 部分互斥，因为 F5 将直接用登录名替代%s 的变量后，直接用登录账号向 ldap server 发起 BINDrequest 建立信任连接（可以理解为这也是一种 BIND）。如果这里配置则 BIND 部分要全部留空！

使用 template，个人感觉非常局限，如果用户是存在于一个不同的目录节点下，则将导致登录失败。

External users 部分配置缺省外部用户所用的 role 及 shell 的级别。注意不同版本的这部分关于 shell 的选项不同。10.0 的版本不支持配置 tmsh 在这里，10.1 即可。

3．至此，基本 F5 端配置完成，但是上述配置存在缺陷，即缺省所有外部用户都只能被赋予相同的 role，显然实际工作中肯定有很多不同 role 的用户，因此必须实现不同的用户或用户组能有不同的 role 权限，方法有两种：

A.在 F5 的 user 中添加所有外部用户的用户名，并逐一为其设置各自的 role。此方法的好处是 ldap 服务器端不用考虑分组，ldap 服务器等于只负责验证，不负责授权，授权由本地来进行。

B.使用 b remoterole 命令在 F5 上配置不同的用户组管理不同的 role，F5 将在 ldap 服务器所返回的响应中查找是否存在匹配的 attribute，如果查到匹配则分配对应的 role

本文只讲述 B 方法。具体的 b remoterole 如何设置见下文。

二、LDAP 服务器设置

不同的软件设置方法不同，本文以 openldap 为例。

1． Openldap 安装方法略，测试用的话 openldap 有 windows 版的

2． 配置 openldap 的配置文件 slapd.conf，大部分缺省，注意红色部分：

```
# 0x4161 (16737 = 0x4000sync + 0x100stats + 0x40config + 0x20filter + 1trace)
loglevel            16928

password-hash     {MD5}

require             LDAPv3

pidfile             ../var/run/slapd.pid
argsfile            ../var/run/slapd.args
logfile             ../var/run/slapd.log
```

```
threads          4
sizelimit        500
tool-threads     1

include          ../schema/core.schema
include          ../schema/cosine.schema
include          ../schema/nis.schema
include          ../schema/inetorgperson.schema
#注意上面的 include 应该都包含，否则 uid 属性可能无法支持，而 F5 发起查询的是用 uid，而不是 cn

access to attrs=userPassword
        by anonymous auth
        by self write
        by * none

access to *
        by self write
        by * read


database         bdb

dbnosync
dirtyread
cachesize        10000

suffix           "dc=f5device,dc=com"
checkpoint       4096 15

rootdn           "cn=manage,dc=f5device,dc=com"
rootpw           manage

directory        ../var/openldap-data
index            objectClass eq,pres
index            cn,sn,uid,mail eq,sub,subinitial,subany
```

3.配置一个 ldif 文件以便导入 ldap 中，下面是一个示例，配置了多个用户和 2 个组：

```
dn: dc=f5device,dc=com
dc: f5device
ou: f5device Dot Com
objectClass: dcObject
objectClass: organizationalUnit
```

```
dn: cn=admin, dc=f5device,dc=com
userPassword:: c2VjcmV0
description: LDAP administrator
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin

dn: ou=operator, dc=f5device,dc=com
ou: operator
objectClass: organizationalUnit

dn: uid=mycisco3,ou=operator, dc=f5device,dc=com
userPassword:: MTExMTEx
uid: mycisco3
objectClass: inetOrgPerson
sn: mycisco3
cn: mycisco3

dn: uid=mycisco4,ou=operator, dc=f5device,dc=com
userPassword:: MTExMTEx
uid: mycisco4
description: operator
objectClass: inetOrgPerson
sn: mycisco4
cn: mycisco4

dn: uid=mycisco_base, dc=f5device,dc=com
userPassword:: MTExMTEx
uid: mycisco_base
description: operator
objectClass: inetOrgPerson
sn: mycisco4
cn: mycisco_base

dn: ou=guest, dc=f5device,dc=com
ou: guest
objectClass: organizationalUnit

dn: uid=mycisco_guest,ou=guest, dc=f5device,dc=com
userPassword:: MTExMTEx
uid: mycisco_guest
ou: guest
description: guest
```

```
objectClass: inetOrgPerson
sn: mycisco_guest
cn: mycisco_guest
```

将上述复制到一个f5.ldif文件中，然后使用sldapadd 命令导入：

```
slapadd –l f5.ldif
```

然后可以使用 ldapsearch 来验证是否可以被查询了：

```
ldapsearch.exe -x -b "dc=f5device,dc=com"  uid=mycisco4
```

应该返回如下信息，表示成功：

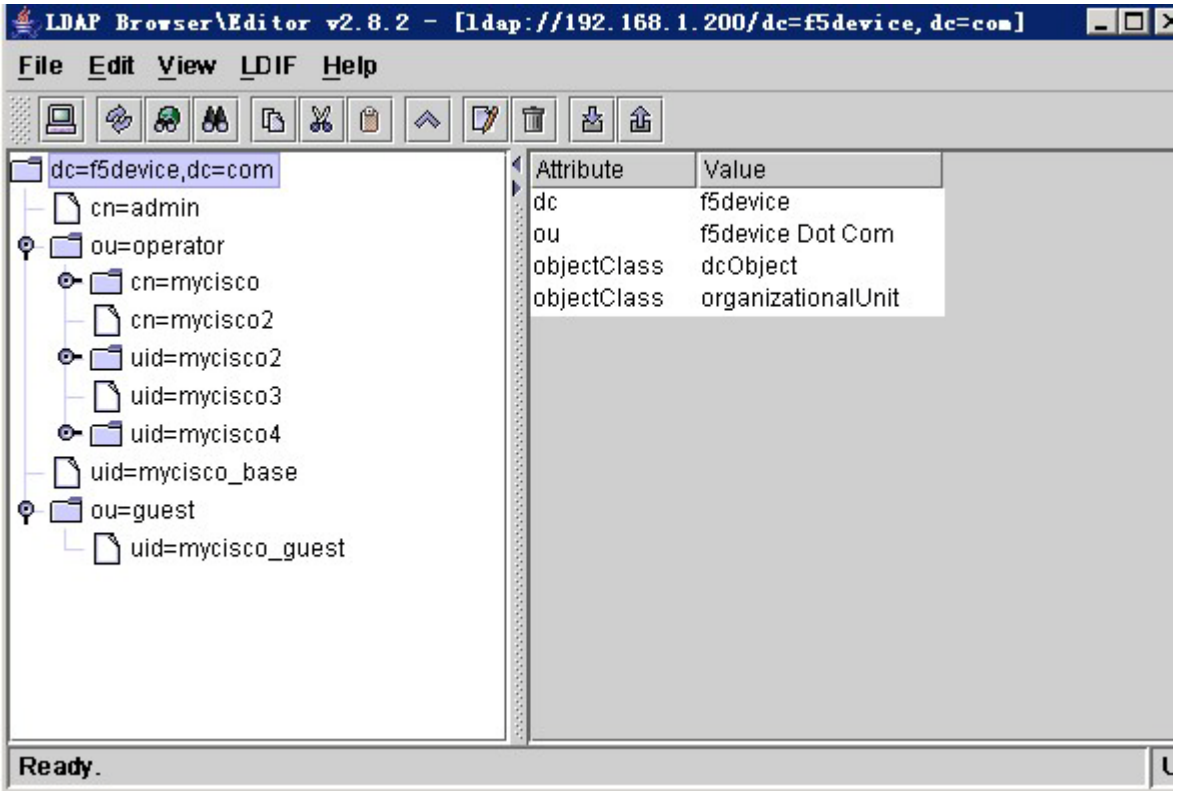
```
# extended LDIF
#
# LDAPv3
# base <dc=f5device,dc=com> with scope subtree
# filter: uid=mycisco4
# requesting: ALL
#

# mycisco4, operator, f5device.com
dn: uid=mycisco4,ou=operator,dc=f5device,dc=com
objectClass: inetOrgPerson
uid: mycisco4
cn: mycisco4
sn: mycisco4
description: operator

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

还可以利用 ldap browser 这个图形化工具来验证服务器是否正常工作：



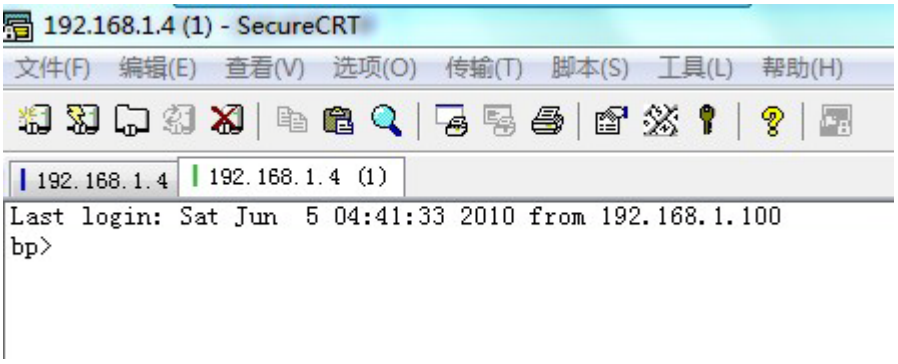
如以后想添加和修改删除用户，用 ldapadd,ldpmodify,ldapdelete 命令。

小结：

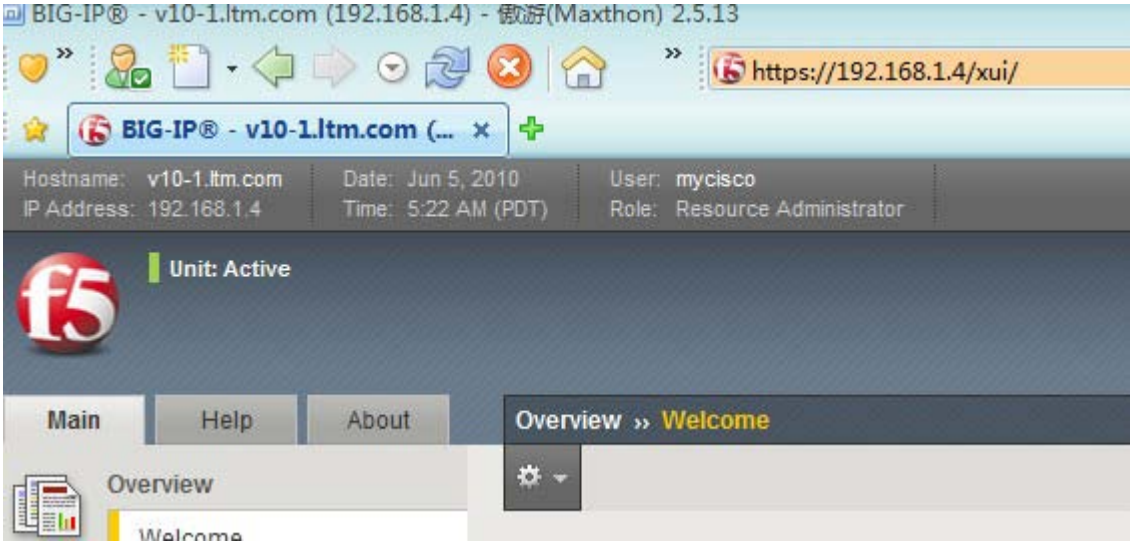
1. F5 启用了外部验证，不加密，设置了缺省的外部用户 role 及 sh 权限 （resource administrator/bigpiple shell），没有设置额外的 remoterole
2. Ldap 配置中主要注意 slapd.conf 文件配置，以及确认可以正常检索

三、调试

1. 尝试使用 mycisco 帐号登录 ssh 和 web



Ssh 登录得到上述效果,符合要求，自动进入 b shell。



WEB 登录，显示 role 为 resource administrator ，符合要求。

2. 添加 remoterole 配置来 override 当前缺省的 role，在命令行中输入如下命令：

[root@v10-1:Active] config # b remoterole role info myrole2 {attribute "description=operator" console "tmsh" line order 2 role "administrator" user partition "all"} Myrole2 定义的 role 名字

description=operator 这是在 ldap 中设置的用户的一个属性

Console 部分指定 shell 级别 或禁用

Line order 用来排序配置在配置文件的顺序，F5 顺序检查，查到第一个匹配即认为成功

Uer partition 指定用户管理域

命令配置完毕后，可以用 b remoterole list 显示：

```
myrole2 {
    attribute "description=operator"
    console "tmsh"
    line order 2
    role "administrator"
    user partition "all"
}
```

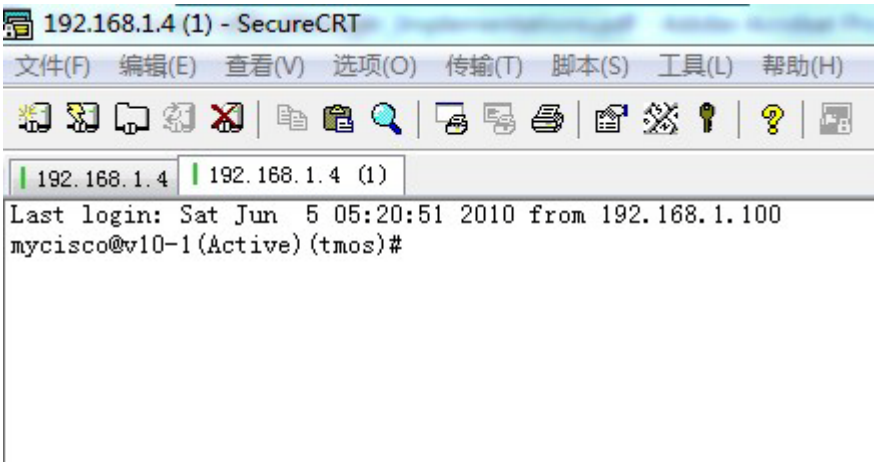
命令结构：

**bigpipe remoterole role info <user group> attribute (<string> | none) console **

**(enable | disable) line order <number> role <user role> user partition **

(<string> | none)

3. 检查上述配置是否生效，使用 mycisco4 帐户登录，如果生效，此时应该拥有管理员权限及 tmsh 的权限



至此配置完成，测试成功。

附 1：

www.myf5.net 查看TACACS+、radius版 设置方法！