v7SSL VPN+IMC EMO

l11617 2015-12-25 发表

1. 移动终端登录SSL VPN时，输入的用户名密码必须到IMC进行radius认证
2. 移动办公只对部分领导进行开放授权

基础环境：

F1050：Version 7.1.064, Demo 9310

IMC：PLAT 7.1 E0303P06

EIA 7.1 E0302P10

EMO 7.1E0305

EIP 7.1E0302P10

VAPP服务器 根域服务器 IMC EMO 服务器： WIN2008R2

Ip地址规划：

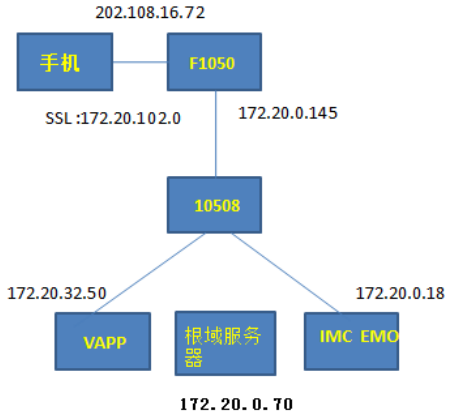
F1050公网ip：202.108.16.72 ssl vpn拨号的地址

SSL VPN分配网段：172.20.102.0 终端获取SSL VPN的地址

VAPP应用服务器： 172.20.32.50

Imc emo服务器：172.20.0.18

根域服务器：172.20.0.70



全网ip互通 省略

全部服务器关闭防火墙，加入域之后火墙会自动开启.IMC 服务器不用加域

#配置SSL VPN网关地址

interface SSLVPN-AC0

ip address 172.20.102.1 255.255.255.0

#创建终端用户地址池ippool，指定IP地址范围

sslvpn ip address-pool ippool 172.20.102.10 172.20.102.100

#把相应的接口加入到安全区域

security-zone name Trust

import interface GigabitEthernet1/0/13

import interface Vlan-interface3

security-zone name Untrust

import interface GigabitEthernet1/0/0

import interface GigabitEthernet1/0/15

import interface SSLVPN-AC0

#配置域间策略

zone-pair security source Any destination Any

packet-filter 3000

acl advanced 3000

rule 5 permit ip

#配置radius认证 用户登录SSL VPN需要IMC来授权

radius scheme emo

primary authentication 172.20.0.18
primary accounting 172.20.0.18
key authentication cipher xxxxx
key accounting cipher xxxxx
user-name-format without-domain

#配置ISP域domain，指定用户授权属性为用户组group1，认证、授权和计费使用的RADIUS方案为rs
cheme
domain emo
authorization-attribute user-group group1
authentication sslvpn radius-scheme emo
authorization sslvpn radius-scheme emo
accounting sslvpn radius-scheme emo

 # 配置PKI域sslvpn
pki domain sslvpn
public-key rsa general name sslvpn
undo crl check enable

 # 导入CA证书ca.cer和服务器证书server.pfx。
pki import domain sslvpn der ca filename ca.cer
pki import domain sslvpn p12 local filename server.pfx
 # 配置SSL服务器端策略ssl，引用PKI
ssl server-policy ssl
pki-domain sslvpn
ciphersuite rsa_aes_128_cbc_sha

ip http enable
ip https enable

#配置SSL VPN网关gw的IP地址，并引用SSL服务器端策略ssl。
sslvpn gateway gw
ip address 202.108.16.72
ssl server-policy ssl
service enable

 # 配置SSL VPN访问实例imc引用SSL VPN网关gw
sslvpn context imc
gateway gw domain emo

#在SSL VPN访问实例imc中，为客户端指定的EMO服务器
emo-server address 172.20.0.18 port 9058

 # 在SSL VPN访问实例imc中引用SSL VPN AC接口1
ip-tunnel interface SSLVPN-AC0

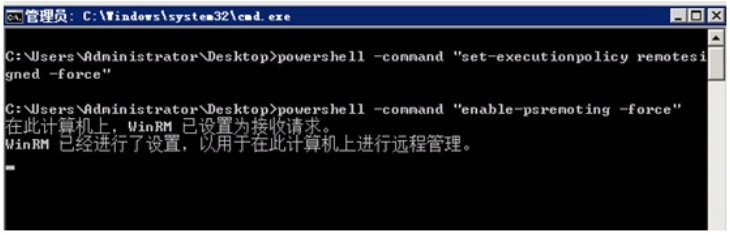
#在SSL VPN访问实例imc中，创建路由列表，并进入路由列表视图
ip-route-list iplist
include 172.20.0.0 255.255.0.0

#在SSL VPN访问实例imc中，配置SSL VPN策略组视图
policy-group pgroup

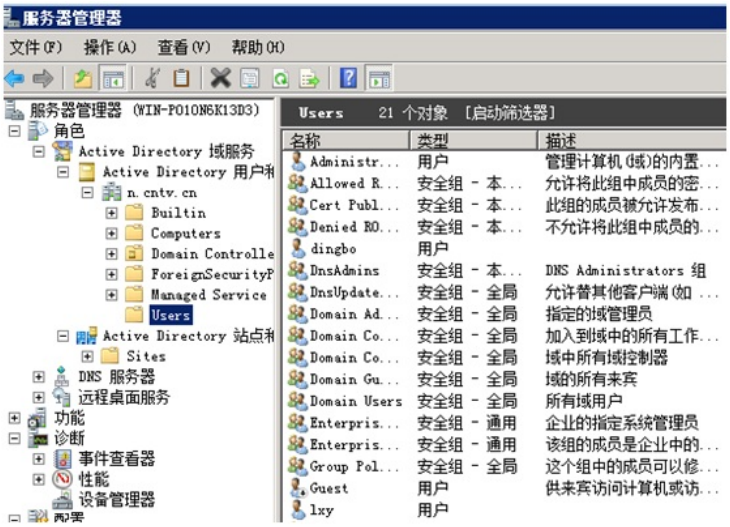
#在SSL VPN策略组视图下配置IP接入引用地址池和路由表
ip-tunnel address-pool ippool mask 255.255.0.0
ip-tunnel access-route ip-route-list iplist
问实例使用指定的ISP域进行AAA认证
aaa domain emo
service enable
根服务器配置
搭建域服务 DNS服务 远程桌面服务 省略
根服务器用户名administrator

域名n.cntv.cn

运行EMOTOOL工具，EMOTOOL工具路径 iMC\emo\tool



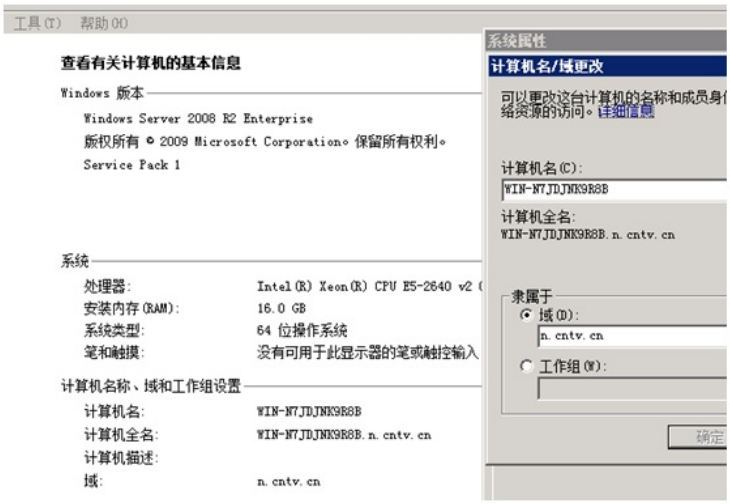
创建测试账号lxy



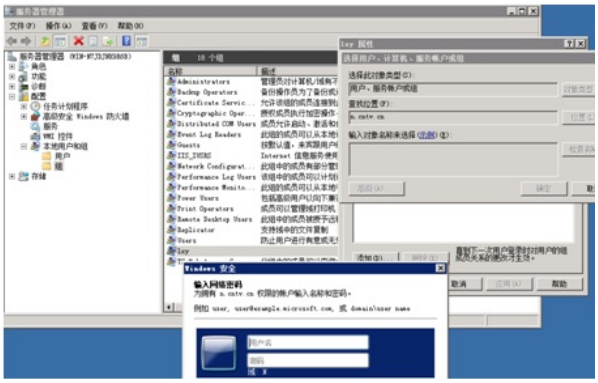
VAPP服务器配置

把VAPP服务器加入到域，注意DNS一定要能解析到n,cntv.cn不然加域失败

VAPP服务器用户名administrator

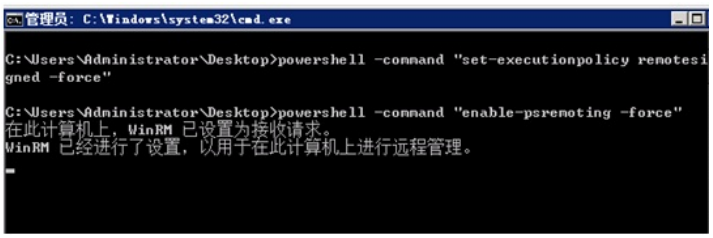


查看VAPP加入域是否成功，在VAPP的服务器管理里，进入配置----本地用户和组---组
创建一个组名称lxy 在lxy组内添加域用户，点击高级 如果提示要域密码就是加域成功.
如果加域失败请重新添加.



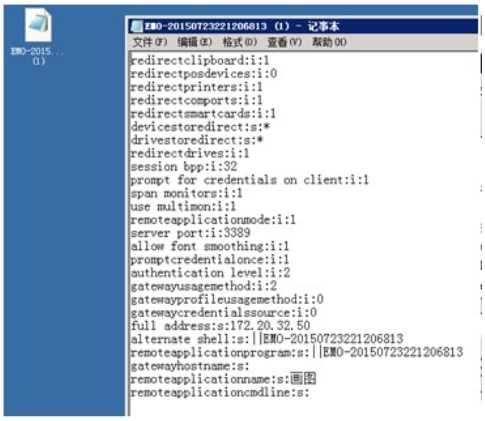
添加远程应用服务

运行EMOTOOL工具，EMOTOOL工具路径 iMC\emo\tool

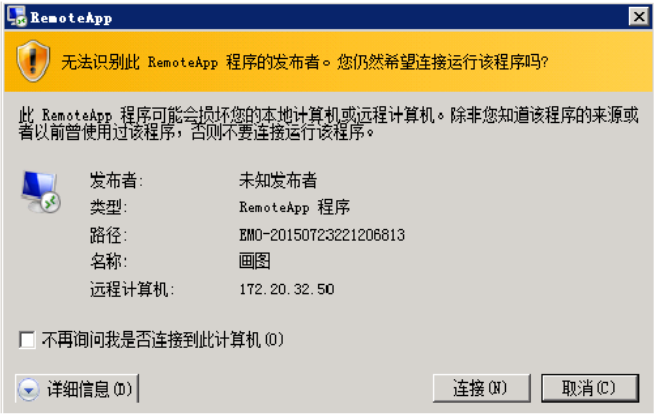


检查所发布的应用是否正常.在服务管理中-----远程桌面服务-----Remotoapp---选择一个应用
右侧有个创建.rdp文件创建到桌面

以文本方式打开，修改里面的full address地址，改为vapp服务器地址

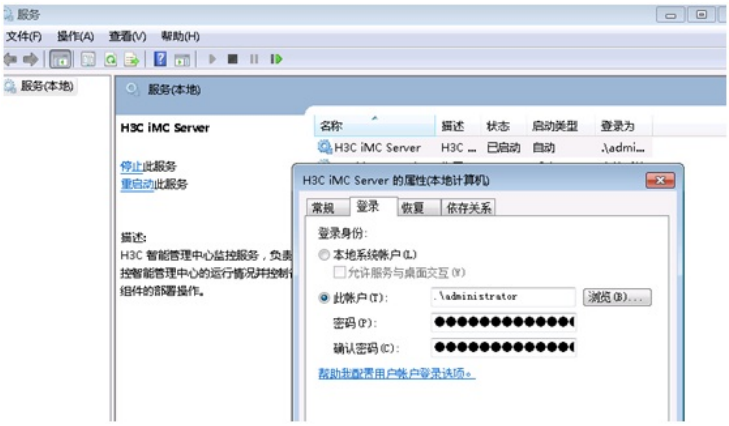


把修改好的.rdp文件拷贝到一台其他的服务器上保证和vapp互通即可
打开方式选择远程桌面连接，如果输入完用户名密码可以正常打开表示发布成功



IMC EMO服务器配置

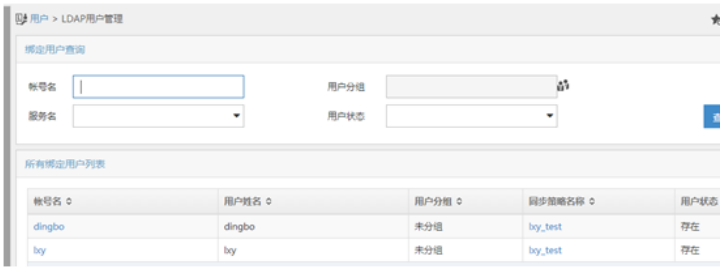
用户账号administrator
如果iMC服务器的操作系统为windows 2008 R2，则H3C iMC server服务的启动方式必须为.\administrator；具体操作流程：停止iMC监控代理，修改服务启动方式为.\administrator，然后重启H3C iMC server服务，最后启动监控代理；



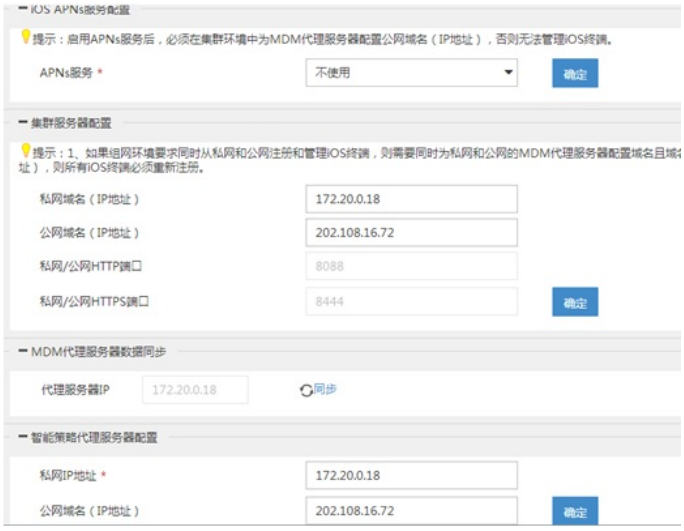
配置LDAP服务i
VAPP应用，账号必须从LDAP同步

设置LDAP同步策略

查看用户是否从LDAP同步成功



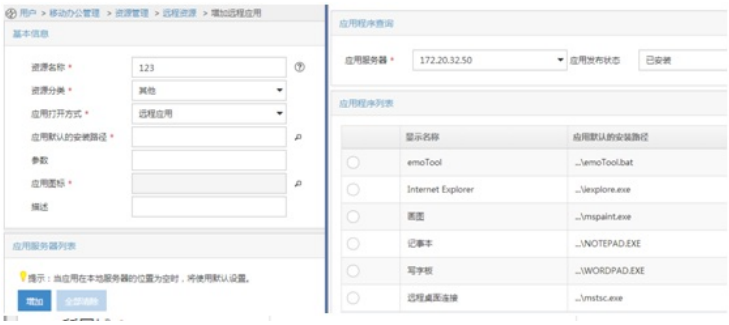
在移动办公管理---系统参数进行配置



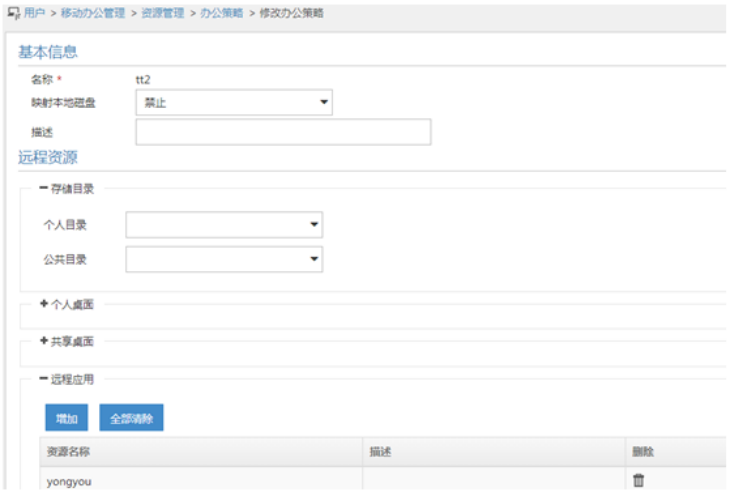
在移动办公管理---系统参数-----域服务器配置 域用户DN：cn=administrator;cn=users;dc=n;dc=cntv;dc=cn

在移动办公管理----资源管理----服务管理---添加应用服务器

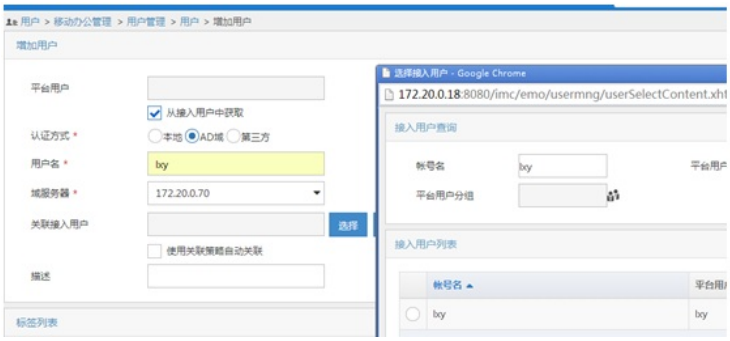
在移动办公管理---资源管理----远程资源-----添加远程应用



在移动办公管理---资源管理----办公策略 把远程应用进行添加



在移动办公管理—用户管理添加用户lxy



与用户进行授权

用手机INODE进行连接

在移动办公管理---终端管理—终端信息进行授权

在手机商店中进行安装应用

在应用中选择发布的工具