

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:

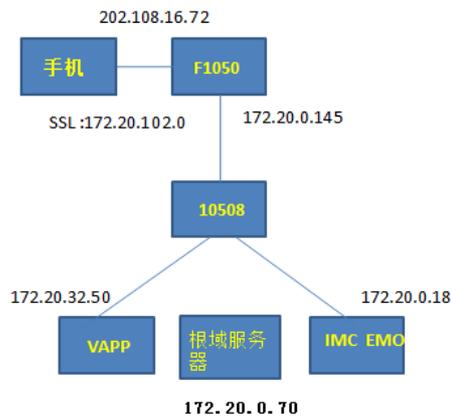
F1050公网ip : 202.108.16.72 ssl vpn拨号的地址

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，加入域之后防火墙会自动开启.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rscheme

```
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
```

向实例使用指定的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
```



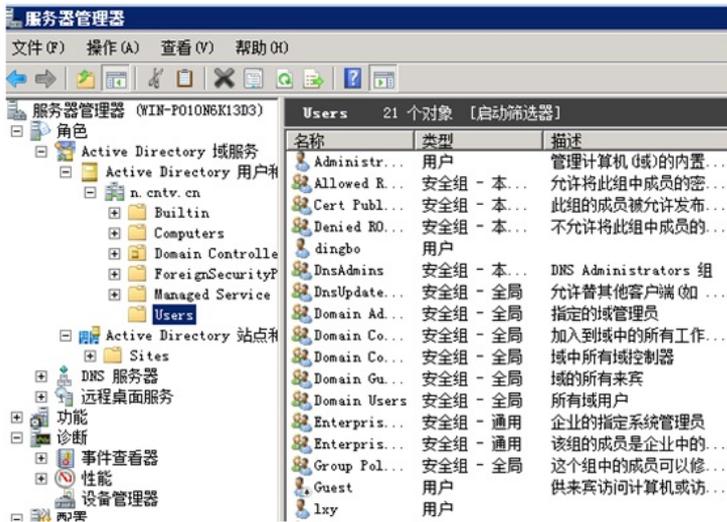
域名n.cntv.cn



运行EMOTOOL工具，EMOTOOL工具路径 iMC\emo\tool



创建测试账号lxy



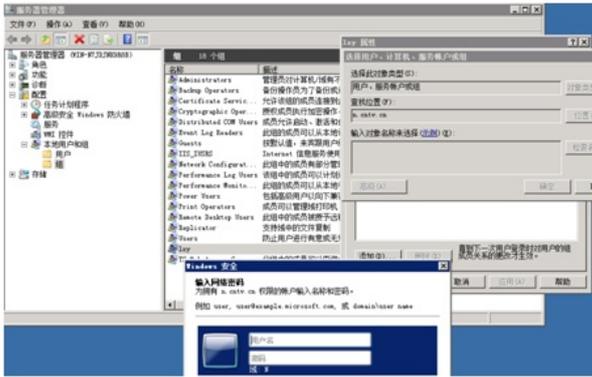
VAPP服务器配置

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



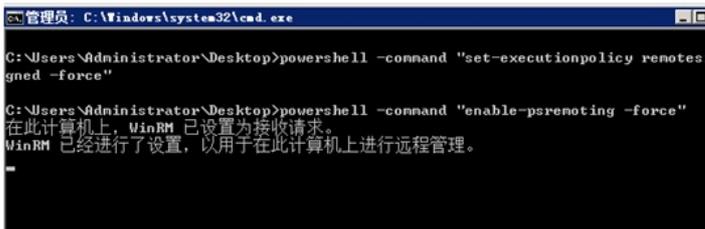
查看VAPP加入域是否成功，在VAPP的服务器管理里，进入配置----本地用户和组---组创建一个组名称xy 在xy组内添加域用户，点击高级 如果提示要域密码就是加域成功。如果加域失败请重新添加。



添加远程应用服务



运行EMOTOOL工具，EMOTOOL工具路径 iMC\emotool



检查所发布的应用是否正常.在服务器管理中-----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

```

EMO-2015... (1) - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
redirectclipboard:i:1
redirectposdevices:i:0
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:1
devicestoredirect:s:*
drivestoredirect:s:*
redirectdrives:i:1
session bpp:i:32
prompt for credentials on client:i:1
span monitors:i:1
use multimon:i:1
remoteapplicationmode:i:1
server port:i:3389
allow font smoothing:i:1
promptcredentialonce:i:1
authentication level:i:2
gatewayusagemethod:i:2
gatewayprofileusagemethod:i:0
gatewaycredentialssource:i:0
full address:s:172.20.32.50
alternate shell:s:|EMO-20150723221206813
remoteapplicationprogram:s:|EMO-20150723221206813
gatewayhostname:s:
remoteapplicationname:s:画图
remoteapplicationcmdline:s:

```

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

基本信息

服务器名称 * 服务器版本

服务器地址 * 端口 *

服务器类型 服务同步方式

实时认证 连接超时时长 *

连接超时时间(秒) * 同步超时时间(秒) *

用户分组 *

业务分组 * 启用SSL连接 连通服务器

服务器信息

Base DN *

管理员DN

管理员密码

用户名属性名称 *

用户密码属性名称

设置LDAP同步策略

修改LDAP同步策略

同步策略名称 *

服务器名称

业务分组

同步优先级 * ?

Base DN

子BaseDN * ?

过滤条件 *

状态 *

同步的用户类型 接入用户 设备管理用户

同步选项 自动同步 按需同步 新增用户及其接入帐号 为已存在用户新增接入帐号 仅同步当前节点下的用户 过滤计算机帐号

查看用户是否从LDAP同步成功

用户 > LDAP用户管理

绑定用户查询

帐号名 用户分组

服务名 用户状态

所有绑定用户列表

帐号名	用户名	用户分组	同步策略名称	用户状态
dingbo	dingbo	未分组	lxy_test	存在
lxy	lxy	未分组	lxy_test	存在

在移动办公管理---系统参数进行配置

iOS APNs服务配置

提示：启用APNs服务后，必须在集群环境中为MDM代理服务器配置公网域名（IP地址），否则无法管理iOS终端。

APNs服务 *

集群服务器配置

提示：1、如果组网环境要求同时从私网和公网注册和管理iOS终端，则需要同时为私网和公网的MDM代理服务器配置域名且域地址），则所有iOS终端必须重新注册。

私网域名（IP地址）

公网域名（IP地址）

私网/公网HTTP端口

私网/公网HTTPS端口

MDM代理服务器数据同步

代理服务器IP

智能策略代理服务器配置

私网IP地址 *

公网域名（IP地址）

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

用户 > 移动办公管理 > 系统参数 > 域服务器配置 > 修改域服务器

服务器信息

名称	172.20.0.70
域名	n.cntv.cn
NetBIOS名称	N
IP地址	172.20.0.70
域用户DN *	cn=administrator;cn=users;dc=n;dc
域用户密码 *	*****
描述	

在移动办公管理---资源管理---服务管理---添加应用服务器

用户 > 移动办公管理 > 资源管理 > 服务器管理 > 修改应用服务器

服务器信息

名称	172.20.32.50
IP地址或计算机全名	172.20.32.50
端口号 *	3389
隐藏服务器磁盘 *	是
所属域 *	n.cntv.cn
管理员登录名 *	.\administrator
管理员密码 *	*****
结束已断开的会话	1分钟
空闲会话限制	1小时
负载均衡中的会话数因子 *	1000

在移动办公管理---资源管理---远程资源---添加远程应用

用户 > 移动办公管理 > 资源管理 > 远程资源 > 添加远程应用

基本设置

应用名称 * 123

应用分类 * 其他

应用打开方式 * 远程应用

应用默认的安装路径 *

参数

应用图标 *

描述

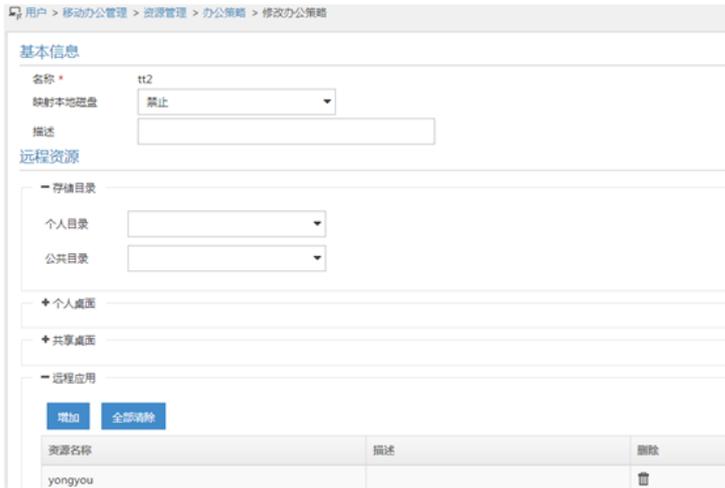
应用服务器列表

应用程序清单

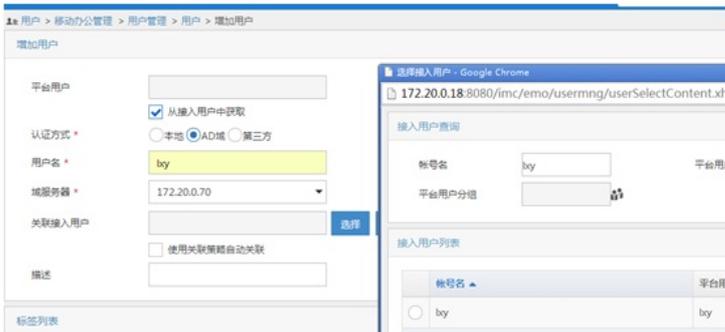
应用服务器 * 172.20.32.50 应用发布状态 已安装

应用名称	应用默认的安装路径
emoTool	..\emoTool.bat
Internet Explorer	..\iexplore.exe
画图	..\mspaint.exe
记事本	..\NOTEPAD.EXE
写字板	..\WORDPAD.EXE
远程桌面连接	..\rsmisc.exe

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

