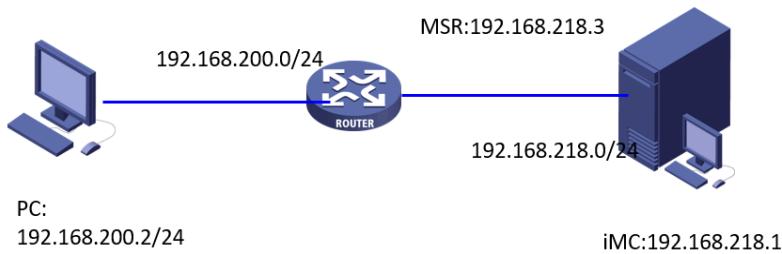


iMC EIA V7版本和V7设备配合实现portal认证的典型配置案例

Portal 李树兵 2016-08-01 发表

Portal认证作为一个简单快捷的认证方式，越来越多的公司采用。本文档介绍远程Portal认证典型配置举例。本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。本文档假设您已了解AAA、Portal认证。



认证PC的地址为192.168.200.2，网关为192.168.200.1，位于路由器上，路由器另外一个接口地址为192.168.218.3，和iMC互联，iMC的地址为192.168.218.1，作为portal服务器和RADIUS服务器。

iMC EIA版本信息：7.1 E0302P18

VBRAS版本信息：7.1 E0321

一.设备配置：

```
interface GigabitEthernet1/0 //配置连接外网的接口，用于NAT转换出去
port link-mode route
description nat-shangwang-vnet8
ip address 192.168.226.4 255.255.255.0
nat outbound
#
interface GigabitEthernet2/0 //配置连接认证客户端的接口地址
port link-mode route
description qiaojie-youxian-wangka-vnet2
ip address 192.168.200.1 255.255.255.0
portal enable method direct //接口下发portal服务
portal domain imc //制定接口下portal认证的domain域为imc
portal apply web-server imc //接口应用portal服务，服务的名字为imc
#
interface GigabitEthernet3/0 //配置连接iMC的接口地址
port link-mode route
description zhiji-pc-vnet1
ip address 192.168.218.3 255.255.255.0
snmp-agent //配置SNMP参数，用于iMC网管
snmp-agent local-engineid 800063A280000C29B1FDD600000001
snmp-agent community write private
snmp-agent community read public
snmp-agent sys-info version all
trap address udp-domain 192.168.218.1 params securityname public v2c
snmp-agent trap enable arp
snmp-agent trap enable radius
radius session-control enable //使能RADIUS session control功能，这个命令比较重要。iMC使用ses
sion control报文向设备发送授权信息的动态修改请求以及断开连接请求。使能RADIUS session control
功能后，设备会打开知名UDP端口1812来监听并接收RADIUS服务器发送的session control报文。需要
注意的是，该功能仅能和H3C IMC的RADIUS服务器配合使用。开启之后iMC发送的强制下线报文设备
才会处理。
```

```

#
radius scheme imc //配置 radius scheme imc
primary authentication 192.168.218.1 //指定认证的服务器地址为192.168.218.1
primary accounting 192.168.218.1 //指定计费的服务器地址为192.168.218.1
accounting-on enable //打开计费功能。在accounting-on功能处于使能的情况下，若集中式设备或分布式设备上的单板重启，则设备或单板会在重启之后发送accounting-on报文通知该方案所使用的RAD
US计费服务器，要求RADIUS服务器停止计费且强制该设备的用户下线。
accounting-on extended //accounting-on扩展功能是分布式设备对accounting-on功能的增强。在分布
式架构下，用户接入到设备的业务板上，当用户所在业务板重启而整机没有重启时，设备会通过accou
nting-on报文通知RADIUS服务器，让对应单板的用户停止计费。本扩展功能仅适用于PPP、IPoE和
lan-access用户。本扩展功能不适用于Portal用户，因为所有的Portal用户数据都保存在主控板，只需
要开启普通accouning-on功能即可。
key authentication cipher $c$3$HxkbNWxQgnU/haGwlFivTmu4ZVkl6g== //配置认证的key，这里配
置为h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。
key accounting cipher $c$3$mO0sPfgT7zSvJl0UqqJerV40K39OyA== //配置计费的key，这里配置为
h3c，此处的密钥要和iMC侧接入设备配置的密钥一致。这两个密钥要保持一致，因为iMC侧只能配置
一个密钥，所以认证和计费密钥要一致。
user-name-format without-domain //配置认证用户不带domain域，对应iMC侧接入服务不能添加服务
后缀

```

```

#
domain imc //配置domain域imc
authorization-attribute idle-cut 10 10240000 //类似于V5设备上的idle-cut，用于在设备上检测用户是
否在线。指定ISP域imc下的用户闲置切断时间为10分钟，闲置切断时间内产生的流量为10240000字节
。
authentication portal radius-scheme imc //设置用户认证的radius方案为imc
authorization portal radius-scheme imc //设置用户授权的radius方案为imc
accounting portal radius-scheme imc //设置用户计费的radius方案为imc
#
portal free-rule 1 destination ip 192.168.200.1 255.255.255.255
portal free-rule 2 destination 221.130.33.52 //放通目的地址为DNS，用于用户访问域名的时候进行DN
S解析
portal free-rule 3 destination 221.130.33.60
#
portal web-server imc // 配置Portal Web服务器的URL为http://192.168.218.1:8080/portal
url http://192.168.218.1:8080/portal
#
portal server imc //配置portal服务器imc
ip 192.168.218.1 key cipher $c$3$vr9TyOUwjLrWZsZ+9qMb8e6WT7JHcA== //配置portal服务器的地
址为192.168.218.1，以及认证的密钥key，此处的key为h3c，此处的配置要和iMC侧portal服务管理里
面的设备配置的key一致。
#
二.iMC配置：

```

第一步：将设备加入到iMC网管



资源 > 增加设备

设备基本信息	
主机名或IP地址 *	192.168.218.3
设备标签	
掩码	
设备分组	
登录方式	Telnet
<input checked="" type="checkbox"/> 将设备的Trap发送到本网管系统	
<input checked="" type="checkbox"/> 设备支持Ping操作①	
<input type="checkbox"/> Ping不连也加入②	
<input type="checkbox"/> 将LoopBack地址作为管理IP	
配置SNMP参数	
①设置	
参数类型	SNMPv2c
只读团体字	*****
读写团体字	*****

资源 > 设备视图 > 视图-路由器

状态	设备标签	型号	IP地址	类型	操作
<input type="checkbox"/>	H3C(192.168.218.3)	H3C VRAS1000P	192.168.218.3	路由器	...

共有1条记录，当前第1 - 1，第 1/1 页。

数据获取时间：2016-07-16 08:24:14

第二步：增加接入设备

Intelligent Management Center

- 首页
- 资源
- 用户
- 业务
- 告警
- 报表
- 系统管理

默认视图 admin 桌面版 帮助 关于

增加设备 SNMP模板 系统参数

搜索设备IP、标签、状态

生成图表 删除 管理 取消管理 同步 刷新 更多 视图

状态 设备标签 型号 IP地址 类型 操作

警告 H3C(192.168.218.3) H3C VRAS1000P 192.168.218.3 路由器 ...

共有1条记录，当前第1 - 1，第 1/1 页。

数据获取时间：2016-07-16 08:24:14

增加用户 所有用户 用户附加信息 用户批量操作 导入用户 帐号封禁管理 接入用户管理 访客管理 终端管理 用户接入日志 来宾接入管理 快速入门 接入策略管理 接入条件管理 接入设备管理 LDAP业务管理 Portal服务器管理 业务参数配置 第三方认证配置 导出任务管理 终端界面定制 页面推送策略

取消管理 同步 刷新 更多 视图

搜索设备IP、标签、状态

增加设备 SNMP模板 系统参数

搜索设备IP、标签、状态

增加设备 视图

增加设备 IP地址 类型 操作

8.3) H3C VRAS1000P 192.168.218.3 路由器 ...

共有1条记录，当前第1 - 1，第 1/1 页。

数据获取时间：2016-07-16 08:24:14

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置

加入收藏 帮助

高级查询

设备IP地址从 至 设备名称 接入设备类型 查询 重置

[增加] 新建 修改 下发配置 同步端口配置 与平台设备同步 批量导入 刷新

AAA下发结果 命令行下发结果

设备名称	设备IP地址	设备型号	下发配置类型	备注	下发结果	端口配置同步结果	详细信息	操作
H3C	192.168.218.3	H3C VRAS1000P	H3C有线		未下发	未同步	<input type="checkbox"/>	...

共有1条记录，当前第1 - 1，第 1/1 页。

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 修改接入设备

认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	LAN接入业务
接入设备类型	H3C(General)	接入设备分组	无
共享密钥 *	***	确认共享密钥 *	***

设备列表

设备名称	设备IP地址	设备型号	备注
H3C	192.168.218.3	H3C VRAS1000P	

共有1条记录。

确定 **取消**

置共享密钥，保证和设备里面radius scheme 配置的密钥一致，增加设备，保证设备的IP地址和设备上的nas-ip地址一致。设备上如果没有指定nas-ip，设备默认是以离iMC最近的IP地址来发送radius报文，本案例中设备是以192.168.218.3来发送的。

第三步：在portal服务管理中增加portal设备

用户 > 接入策略管理 > Portal服务管理 > 设备配置

设备名	版本
下发结果	业务分组

增加

设备名	版本	业务分组	IP地址	最近一次下发时间	下发结果	操作
vbras	Portal 2.0	未分组	192.168.200.1	未下发		

共有1条记录，当前第1 - 1，第 1/1 页。

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备名 *	vbras	业务分组 *	未分组
版本 *	Portal 2.0	IP地址 *	192.168.200.1
监听端口 *	2000	本地Challenge *	否
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *	否	支持用户心跳 *	否
密钥 *	***	确认密钥 *	***
组网方式 *	直连		
设备描述			

确定 **取消**

第四步：增加portal认证的IP地址组

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置

IP地址组名	业务分组	起始地址	终止地址	类型	转换后起始地址	转换后终止地址	起始IPv6地址	终止IPv6地址	修改	删除
200	未分组	192.168.200.1	192.168.200.254	普通						

共有1条记录，当前第1 - 1，第 1/1 页。

修改IP地址组

IP地址组名 *	200
起始地址 *	192.168.200.1
终止地址 *	192.168.200.254
业务分组	未分组
类型 *	普通

确定 **取消**

第五步：配置端口组信息管理

设备信息查询

设备名	<input type="text"/>	版本	<input type="text"/>
下发结果	<input type="text"/>	业务分组	<input type="text"/>

查询 **重置**

增加

设备名	版本	业务分组	IP地址	最近一次下发时间	下发结果	操作
vbras	Portal 2.0	未分组	192.168.200.1		未下发	

共有1条记录，当前第1 - 1, 第1/1页。

端口组信息查询

端口组名	<input type="text"/>	开始端口 >=	<input type="text"/>	终止端口 <=	<input type="text"/>
协议类型	<input type="text"/>	是否NAT	<input type="text"/>		

查询 **重置**

增加 **返回**

端口组名	开始端口	终止端口	协议类型	是否NAT	详细信息	修改	删除
bras	0	zzzzzz	HTTP	否			

共有1条记录，当前第1 - 1, 第1/1页。

修改端口组信息

端口组名 *	<input type="text" value="bras"/>	提示语言 *	<input type="text" value="动态检测"/>
开始端口 *	<input type="text" value="0"/>	终止端口 *	<input type="text" value="zzzzzz"/>
协议类型 *	<input type="text" value="HTTP"/>	快速认证 *	<input type="text" value="否"/>
是否NAT *	<input type="text" value="否"/>	错误透传 *	<input type="text" value="是"/>
认证方式 *	<input type="text" value="CHAP认证"/>	IP地址组 *	<input type="text" value="200"/>
心跳间隔(分钟) *	<input type="text" value="0"/>	心跳超时(分钟) *	<input type="text" value="0"/>
用户名	<input type="text"/>	端口组描述	<input type="text"/>
无感知认证	<input type="text" value="不支持"/>	客户端防破解 *	<input type="text" value="否"/>
页面推送策略	<input type="text"/>	缺省认证页面	<input type="text"/>

确定 **取消**

第六步：增加接入策略。

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 接入策略管理

接入策略查询

接入策略名: 业务分组: [查询] [重置]

[增加]

接入策略名	描述	业务分组	修改	删除
imc		未分组		

共有1条记录，当前第1 - 1, 第1/1页。 [前一页] [后一页] [第1页] [第50页]

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 修改接入策略

基本信息

接入策略名: 业务分组:

描述:

授权信息

接入时段: 分配IP地址:

下行速率(Kbps): 上行速率(Kbps):

优先级: 启用RSA认证

证书认证: 不启用 EAP证书认证 WAPI证书认证

认证证书类型:

下发VLAN:

下发User Profile

下发用户名:

第七步：增加接入服务。

资源 用户 业务 告警 报表 系统管理

用户 > 接入策略管理 > 接入服务管理

[增加] [刷新]

服务名	服务描述	服务后端	业务分组	修改
imc			未分组	

用户 > 接入策略管理 > 修改接入服务

基本信息

服务名: 服务后端:
业务分组: 缺省接入策略:
缺省私有属性下发策略: 缺省单帐号最大绑定终端数: 缺省单帐号在线数量限制:
 可申请 Portal无感知认证

接入场景列表

[增加]

名称	接入策略	私有属性下发策略	优先级	修改	删除
未找到符合条件的记录。					

第八步：增加本地接入用户，绑定imc服务。

Intelligent Management Center

首页 资源 用户 业务 告警 报表 系统管理

默认视图 admin 登录版 帮助 关于 注销

帮助

增加用户

本地接入服务

服务后端: 缺省接入策略:
服务分组: 使用:
缺省单帐号在线数量限制: 可申请 Portal无感知认证

接入场景列表

用户 > 增加用户

基本信息

用户名 *	123	证件号码 *	123	检查是否可用
通讯地址				电话
电子邮件	② 用户分组 *			未分组

开通自助帐户

操作

确定 取消



用户

接入信息

用户名 *	123	选择	增加用户
帐号名 *	123		
<input type="checkbox"/> 预开户用户	<input type="checkbox"/> 缺省BYOD用户	<input type="checkbox"/> MAC地址认证用户	<input type="checkbox"/> 主机名用户
<input type="checkbox"/> 快速认证用户			
密码 *	...	密码确认 *	...
<input checked="" type="checkbox"/> 允许用户修改密码	<input type="checkbox"/> 启用用户密码控制策略	<input type="checkbox"/> 下次登录须修改密码	
生效时间	2024-01-01	失效时间	2024-12-31
最大闲置时长(分钟)	10	在线数量限制	10
Portal无感知认证最大绑定数 *	1		
登录提示信息			

接入服务

服务名	服务后端	状态	分配IP地址
<input checked="" type="checkbox"/> imc		可申请	

接入设备绑定信息

配置完成。

三.验证配置：

用户上线测试，浏览器中随便输入任意地址，跳转出iMC的portal认证页面，输入用户名和密码之后，提示上线成功：



上线成功。
[查看终端信息](#)

在iMC侧查看在线用户可以看到此用户的信息：

在设备上查看在线用户信息：

[H3C] dis portal user all

Total portal users: 1 //在线用户是1个

Username: 123 //用户名为123

Portal server: imc //所在的portal服务为imc

State: Online //状态为在线模式

VPN instance: N/A

MAC IP VLAN Interface

3863-bbb8-a21a 192.168.200.2 -- GigabitEthernet2/0 //显示用户的IP地址和MAC地址，是在设备的2/0接口接上来的

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

[H3C] dis portal user all ver

[H3C]dis portal user all verbose

Total portal users: 1

Basic:

Current IP address: 192.168.200.2

Original IP address: 192.168.200.2

Username: 123

User ID: 0x10000004

Access interface: GigabitEthernet2/0

Service-VLAN/Customer-VLAN: -/-

MAC address: 3863-bbb8-a21a

Domain name: imc

VPN instance: N/A

Status: Online

Portal server: imc

Portal authentication method: Direct

AAA:

Realtime accounting interval: 720s, retry times: 5

Idle cut: N/A

Session duration: 86401 sec, remaining: 86056 sec

Remaining traffic: N/A

Login time: 2016-07-16 08:14:16 UTC

IP pool: N/A

ACL&QoS&Multicast:

Inbound CAR: N/A

Outbound CAR: N/A

ACL number: N/A

User profile: N/A

Session group profile: N/A

Max multicast addresses: 4

Flow statistic:

Uplink packets/bytes: 4206/406137

Downlink packets/bytes: 6280/5203087

[H3C]dis portal user all verbose

Total portal users: 1

Basic:

Current IP address: 192.168.200.2

Original IP address: 192.168.200.2
Username: 123
User ID: 0x10000004
Access interface: GigabitEthernet2/0
Service-VLAN/Customer-VLAN: -/-
MAC address: 3863-bbb8-a21a
Domain name: imc
VPN instance: N/A
Status: Online
Portal server: imc
Portal authentication method: Direct

AAA:

Realtime accounting interval: 720s, retry times: 5
Idle cut: N/A
Session duration: 86401 sec, remaining: 85985 sec
Remaining traffic: N/A
Login time: 2016-07-16 08:14:16 UTC
IP pool: N/A

ACL&QoS&Multicast:

Inbound CAR: N/A
Outbound CAR: N/A
ACL number: N/A
User profile: N/A
Session group profile: N/A
Max multicast addresses: 4

Flow statistic:

Uplink packets/bytes: 5248/478794
Downlink packets/bytes: 7278/5565765

[H3C]dis portal user all verbose

Total portal users: 1

Basic:

Current IP address: 192.168.200.2
Original IP address: 192.168.200.2
Username: 123
User ID: 0x10000004
Access interface: GigabitEthernet2/0
Service-VLAN/Customer-VLAN: -/-
MAC address: 3863-bbb8-a21a
Domain name: imc
VPN instance: N/A
Status: Online
Portal server: imc
Portal authentication method: Direct

AAA:

Realtime accounting interval: 720s, retry times: 5
Idle cut: N/A
Session duration: 86401 sec, remaining: 85970 sec
Remaining traffic: N/A
Login time: 2016-07-16 08:14:16 UTC
IP pool: N/A

ACL&QoS&Multicast:

Inbound CAR: N/A
Outbound CAR: N/A
ACL number: N/A
User profile: N/A
Session group profile: N/A
Max multicast addresses: 4

Flow statistic:

Uplink packets/bytes: 6614/664888
Downlink packets/bytes: 8946/6654640

