

portal server认证用户老化时间不生效

Portal认证 陈美静 2024-08-20 发表

问题描述

现场使用ACG结合IMC做的portal server认证，ACG用户在线时长长达九百多小时没有被踢下线。

序号	用户名	所属组	主机IP地址	认证方式	终端类型	登录时间	在线时长	状态	操作
1	11-03	市行机关	15.167	Portal Server认证	移动终端(Android系统[12-Android])	2024/07/08 14:58	864 小时15 分钟	正常	删除
2	8-17	市行机关	212	Portal Server认证	PC(Windows)	2024/07/22 11:03	532 小时11 分钟	正常	删除
3	8-7	市行机关	217	Portal Server认证	移动终端(未知类型移动终端)	2024/08/13 09:05	6 小时59 分钟	正常	删除
4	81-13	市行机关	1	静态绑定	PC(Windows)	2024/08/13 08:23	6 小时59 分钟	正常	删除
5	81-13	市行机关	1	静态绑定	正在识别	2024/07/26 00:51	446 小时22 分钟	正常	删除
6	81-13	市行机关	3	静态绑定	正在识别	2024/07/26 00:51	446 小时23 分钟	正常	删除
7	81-13	市行机关	4	静态绑定	正在识别	2024/07/26 00:51	446 小时23 分钟	正常	删除
8	81-13	市行机关	2	静态绑定	正在识别	2024/07/26 00:51	446 小时23 分钟	正常	删除
9	81-13	市行机关	11	静态绑定	正在识别	2024/07/26 07:27	439 小时46 分钟	正常	删除
10	81-24	市行机关	181	Portal Server认证	移动终端(未知类型移动终端)	2024/07/05 17:51	933 小时23 分钟	正常	删除
11	81-24	市行机关	26	Portal Server认证	移动终端(iOS系统[iPhone])	2024/07/22 19:12	524 小时2 分钟	正常	删除
12	81-24	市行机关	70	Portal Server认证	移动终端(未知类型移动终端)	2024/07/22 21:47	521 小时27 分钟	正常	删除
13	81-24	市行机关	78	Portal Server认证	移动终端(未知类型移动终端)	2024/08/01 14:30	288 小时44 分钟	正常	删除
14	81-24	市行机关	124	Portal Server认证	正在识别	2024/08/02 08:36	270 小时37 分钟	正常	删除
15	81-24	市行机关	185	Portal Server认证	移动终端(未知类型移动终端)	2024/08/02 10:24	268 小时50 分钟	正常	删除
16	81-24	市行机关	228	Portal Server认证	正在识别	2024/08/02 10:36	268 小时38 分钟	正常	删除
17	81-24	市行机关	159	Portal Server认证	正在识别	2024/08/02 10:49	268 小时25 分钟	正常	删除
18	81-24	市行机关	1153	Portal Server认证	移动终端(未知类型移动终端)	2024/08/02 10:53	268 小时20 分钟	正常	删除
19	81-24	市行机关	204	Portal Server认证	移动终端(未知类型移动终端)	2024/08/02 11:11	268 小时2 分钟	正常	删除
20	81-24	市行机关	1.A.229	Portal Server认证	移动终端(Android系统[1210X1AC])	2024/08/02 20:17	258 小时57 分钟	正常	删除

过程分析

1、现场超时时间设置15min:

Portal Server Portal 逃生

认证服务器: IMC

portal服务器: [IP地址或域名, 例如: 192.168.1.1或2002::1或example.com, 3-255 字符]

快速无感知:

超时时间: 15 (1-144000 分钟)

认证URL: http://[IP地址或域名]?usermac=<USERMAC>&origurl=

(3-255 字符)

(例如: http://www.example.com/portal?userip=<USERIP>&usermac=<USERMAC>&origurl=<ORIGURL>&nasip=naip)

提交 取消

2、确定ACG上没有会话，IMC侧没有用户在线列表项:

H3C SecPath ACG1000

会话统计 会话详情 会话监控

全部 fuzzy=1F

用户	用户组	源地址	源端口	目的地址	目的端口	协议
暂无数据						

接入用户管理

本地在线用户 漫游在线用户 设备在线用户

本地在线用户管理

账号名: [输入框] 登录名: [输入框]

用户IP地址: 1. [输入框] 至: 10.1.130.191

用户名: [输入框] 用户分组: [输入框]

删除 下线 刷新下线 强制在线信息 批量导出 加入黑名单 更多

账号名 登录名 用户名 服务器名 接入时间 接入时长 设备IP地址 用户IP地址 用户分组 无线SSID 用户MAC地址 NAS ID

未找到符合条件的记录。

共有0条记录, 当前页0 / 0, 第 1 / 1 页

3、snmp同步状态正常，配置现场核查无误:

名称	描述	同步类型	同步策略	自动录入	同步状态	状态	操作
1	天行	SNMP 同步	289	否	同步成功	●	≡ 删除
2	shang	SNMP 同步	289	否	同步成功	●	≡ 删除
3	行	SNMP 同步	1389	否	同步成功	●	≡ 删除
4	?	SNMP 同步	289	否	同步成功	●	≡ 删除
5	?	SNMP 同步	289	否	同步成功	●	≡ 删除
6	?	SNMP 同步	289	否	同步成功	●	≡ 删除
7	?	SNMP 同步	289	否	同步成功	●	≡ 删除
8	?	SNMP 同步	289	否	同步成功	●	≡ 删除
9	行	SNMP 同步	289	否	同步成功	●	≡ 删除
10	行	SNMP 同步	289	否	同步成功	●	≡ 删除
11	天行	SNMP 同步	289	否	同步成功	●	≡ 删除
12	行	SNMP 同步	289	否	同步成功	●	≡ 删除
13	行	SNMP 同步	289	否	同步成功	●	≡ 删除
14	天行	SNMP 同步	289	否	同步成功	●	≡ 删除
15	?	SNMP 同步	289	否	同步成功	●	≡ 删除
16	?	SNMP 同步	289	否	同步成功	●	≡ 删除
17	?	SNMP 同步	289	否	同步成功	●	≡ 删除
18	行	SNMP 同步	289	否	同步成功	●	≡ 删除
19	?	SNMP 同步	289	否	同步成功	●	≡ 删除
20	行	SNMP 同步	289	否	同步成功	●	≡ 删除

4、超时时间改成5min，挑了其中一个故障ip抓了6min包，抓包文件为空，没有流量上来：

基础配置

接口

协议

源IP

目的IP

同时抓取出口报文

高级选项 >>

文件列表

(注：仅保留最后一次抓包生成的文件，请及时导出抓包文件)

文件名称	文件大小(Byte)	结束时间	操作
capture_file_any_20240813_155546.pcap	24	2024-08-13 16:00:4	

解决方法

策略超时优先级高于认证方式里的超时下线，修改超时时间为15min可解决（尽可能保证在线用户就是实际活跃用户的话，是得把超时时间改小，具体时间请根据现场需求修改）。

H3C SecPath ACG1000 主页 数据中心 策略配置 用户管理 网络配置 系统管理

用户管理 认证策略 认证方式 认证服务器 用户自注册 高级选项 客户审计 终端行为管理

认证策略

启用

名称 (1-63字符)

描述 (0-127字符)

源接口

源地址

目的接口

目的地址

认证方式

时间

用户组

用户有效时间 永久有效 有效期至 临时有效

IP-MAC绑定

录入用户绑定 IP MAC 有效期 * (1-30 天)

超时时间 15 * (1-144000分钟)

强制重登录间隔 * (1-144000分钟)