

知 某局点数据库审计web页面无法登陆的经验案例

数据库审计

姜霖琛 2019-07-04 发表

组网及说明

不涉及

问题描述

现场D2050-G数据库审计设备突然无法登陆web页面，之前可以正常登陆，测试换了几个电脑都是一样的情况，console可以进命令行后台。除了官网推荐的火狐之外现场还测试了几个其他的浏览器比如e, 360，故障依旧



无法访问此网站

的响应时间过长。

请试试以下办法：

- 检查网络连接
- 检查代理服务器和防火墙
- 运行 Windows 网络诊断

ERR_CONNECTION_TIMED_OUT

重新加载

详细信息

过程分析

查看现场版本为ESS6202，使用ge0/0口登录web，接口up了，电脑上可以ping通这个地址。让现场测试过重启设备（命令行reboot），清空浏览器缓存，故障依旧

```
> display device
H3C i-ware Software, Version 3.10, ESS 6202, 18Q2x64(uy201807112140.405)
Copyright © 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath D2050-G uptime is 0 days,0 hour,31 minutes,55 sec

Serial Number: 219801A1M1718BE00006
BIOS version: Default string
CPU type: Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
Memory: 15.50G
Hard disk:
Disk0: 256.1 GB
Disk1: 4000.8 GB

slot:
slot0: default

Interfaces all:
GE0/0 UP
GE0/1 DOWN
GE0/2 UP
GE0/3 UP
```

```
> ifconfig
ifconfig [-i interface]
ifconfig, can use ifconfig -i interface,default is not any variable
-i interface interface

ifconfig
GE0-0 Link encap:Ethernet HWaddr 00:00:00:00:00:00
inet addr:192.168.1.128 Bcast:192.168.1.255 Mask:255.255.255.128
inet6 addr: ::::: Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:30875069 errors:0 dropped:0 overruns:0 frame:0
TX packets:292161 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2170392005 (2.0 GiB) TX bytes:162729839 (155.1 MiB)
```

测试0口地址可以ping通

```
C:\Users\16922>ping 10.201.5.7

正在 Ping 10.201.5.7 具有 32 字节的数据:
来自 10.201.5.8 的回复: 字节=32 时间=1ms TTL=64
来自 10.201.5.9 的回复: 字节=32 时间<1ms TTL=64
来自 10.201.5.10 的回复: 字节=32 时间<1ms TTL=64
来自 10.201.5.11 的回复: 字节=32 时间=1ms TTL=64

10.201.5.7 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms

C:\Users\16922>ping 10.201.5.7
```

解决方法

怀疑现场配置了管理主机导致。让现场使用数据库审计的其他接口登陆设备web管理页面，删除配置的管理主机后，可以正常从0口登录web页面了。

新数据库审计配置时建议慎重配置管理主机，如果配置的话，建议先配置自身PC的IP地址，避免发生无法登陆的情况