

# 服务器日志

尚云互联服务器部署说明书

深圳市尚云互联技术有限公司 yc

v1.2.0(2020.03.31)

## 版权宣告与免责声明

- 版权声明:

本文之所有内容(包括但不限于文字内容与图片), 均为深圳市尚云互联技术有限公司所有, 非经允许不得以任何形式全文或部份抄袭, 引用。

- 免责声明:

本文之内容及信息不能保证其正确性、实时性或完整性。因为相关内容随时可能被修改或改版。

- 深圳市尚云互联技术有限公司保留文档内容的最后解释修改权利。

## 修订历史

Version	Date	Author	Modification
1.2.0	2020/03/31	yc	更新 log 内容。
1.1.0	2019/07/12	yc	增加转发服务器的日志说明。
1.0.0	2019/02/22	yc	初始版本

## 目录

### 服务器日志

版权宣告与免责声明

修订历史

目录

PPC 平台日志说明

P2P Server 的日志

日志打开、查看和关闭

日志内容说明

Wakeup Server 的日志

Relay Server 的日志

实时查日志工具 – cs2Tail

## PPC 平台日志说明

- PPC 平台包括 P2P Server、Wakeup Server 和 Relay Server，三个服务器都会产生对应的 Log，默认情况下是关闭的。
- Relay Server 和 Wakeup Server 打开 Log 的方式是在程序运行目录下创建对应的 Log 文件夹，Relay Server 需要创建 RSLog 文件夹，Wakeup Server 需要创建 WSLog 文件夹，当对应的文件夹创建后，有连接产生就会创建对应的 Log 信息。
- P2P Server 打开 Log 的方式需要满足两个条件：
  1. 在程序运行目录下创建 Log 目录。
  2. 运行 Management 程序打开 Log。
    - 必须同时满足上述两个条件，P2P Server 的 Log 才会产生。
- 三个服务器程序的 Log 日志都是在对应的 Log 目录下生成 DDHH.log 文件，“DD”对应云主机的日期，“HH”对应云主机的小时。

### • P2P Server 的日志

#### - 日志打开、查看和关闭

##### 1. 使用 Management 程序打开 P2P Server 的 Log

- Management 程序是部署 P2P 服务器时，配置文件中包含的程序文件，每一个平台的程序都不同，名称规则为：平台名称\_Management。
- Management 程序参数：

```
root@yc-virtual-machine:~/PPC# ./PPCS_Management64
Usage: ./PPCS_Management64 1 --> Dump all login DID into ./Log/DID_Dump.html and ./Log/DID_Dump.log
Usage: ./PPCS_Management64 2 --> Dump all login DID into ./Log/DID_Dump.log with detail info
Usage: ./PPCS_Management64 3 DID --> Show latest login time of DID (seconds before) into ./Log/DID_Login.log
Usage: ./PPCS_Management64 4 0 --> Turn Off Log
Usage: ./PPCS_Management64 4 1 --> Turn ON Log
root@yc-virtual-machine:~/PPC#
```

关闭 Log

打开 Log

- 打开指令： `./PPCS_Management64 4 1`
- 程序运行后，Log 目录下会生成日志文本，文本以当前服务器的时间命名：DDHH.log，DD：00~31 (每个月的日期) HH：00~23 (小时)，即每小时一份档案。
- P2P不会自动删除日志文本，因此建议客户一个月删除一次日志信息或将日志文本移动保存。

##### 2. 查看日志

- 进入 Log 目录，使用指令打印 Log 文件最新信息。
- 进入指令： `cd Log`
- 打印 Log 指令： `tail -f DDHH.log`
- 上述指令能够实时的打印文本的最后十行的信息，若没有打印，可以尝试进行测试连接，同步查看 Log 日志。

##### 3. 关闭 Log 日志记录

- 查看完日志后，如无必要，建议关闭日志记录。
- 指令： `./PPCS_Management 4 0`

#### - 日志内容说明

- P2P 服务器的 Log 内容包括设备端注册、用户端联机请求、转发服务器登入等封包的实时纪录。

##### • A. Device Login log (设备登录 Log)

- Error: Login [XXXX] 'DID' from IP: Port
  - XXXX = Invalid Prefix -> Prefix is not supported by this server
  - XXXX = Invalid DID -> This DID is not valid, because, it's check sum is not correct!
  - XXXX = Blacked DID -> This DID is in black list.

- *XXXX = Login Out of Date -> DID License is Out of Date.*
- **Successfully:** Login 'DID' from IP: Port, NATType=#, APIVersion:##.##, LocalAddr=IP: Port
  - *NATType, 0: Unknown, 1: IP-Restricted cone NAT, 2: PortRestricted Cone NAT, 3: Symmetric NAT*
  - *API Version: The API version, ##.##*
  - *Local Address: Local address of Login device*
- **B. Device relay function (设备转发信息登录)**
  - **Error:** SDev Login [XXXX] 'DID' from IP:Port
    - *XXXX = refer to A. Device Login log*
  - **Successfully:** SDev Login 'DID' from IP:Port
- **C. P2P Request log (P2P 请求)**
  - **Error:** P2PReq [XXXX] 'DID' from IP: Port
    - *XXXX = refer to A. Device Login log*
  - **Successfully:** P2PReq 'DID' from IP: Port, LocalAddr= IP: Port
- **D. Relay Server Login (Relay Server 登录)**
  - **Error:** RSLogin Login [XXXX] 'SID' from IP: Port
    - *XXXX = refer to A. Device Login log*
    - *SID: The Relay Server's ID*
  - **Successfully:** RSLogin Login 'SID' from IP: Port, BandWidth=##, UserNumber=##
    - *BandWidth is not yet implemented, so, just ignore it!!*
    - *User Number is not yet implemented, so, just ignore it!!*
- **E. Relay Request (转发请求)**
  - **Error:** RLYReq [XXXX] 'DID' from IP: Port
    - *XXXX = refer to A. Device Login log*
  - **Successfully:** RLYReq 'DID' from IP:Port, RLYAddr=IP: Port
    - *RLYAddr: the relay service provider's IP: Port*
- **F. Relay server list request log (转发服务器列表请求)**
  - **Error:** ListReq1 [XXXX] 'DID' from IP: Port
    - *XXXX = refer to A. Device Login log*
  - **Successfully:** No Log when successful.
- **G. API Report (Listen&Connect 回报 P2PServer v3.5.0以上)**
  - **Listen Report:** Report form IP:Port, Listen('DID'), ret=N, P2P, Rmt=IP:Port, Wan=IP:Port, Lan=IP:Port (x/XXX)
    - *N = Listen the return value.*
    - *x/XXX = The API supports session at most.*
  - **Connect Report:** Report form IP:Port, Connect('DID', bEnableLanSearch), ret=N, P2P, Rmt=IP:Port, Wan=IP:Port, Lan=IP:Port (x/XXX)
    - *N = Listen the return value.*
    - *x/XXX = The API supports session at most.*

## • Wakeup Server 的日志

- 唤醒服务器产生的Log格式如下: [YYYY-MM-DD hh:mm:ss]Logging - [XXX]<YYY>ZZZ(DDD)
  - YYYY-MM-DD hh:mm:ss :该笔Log产生的日期时间
  - XXX: Log的性质,可能的内容为:
    - Error: 异常错误的 Log
    - Alarm: 非异常但是值得注意的 Log
    - OK: 执行结果是正确无误的 Log
  - YYY: Log 的来源, 可能的内容为:
    - remote UDP: 这是来自于Internet的客户端的查询封包
    - loopback UDP: 本机的P2P Server发送过来的唤醒封包
    - TCP Accept: 来自设备的TCP联机建立请求
    - TCP Read: 来自与设备建立好的TCP联机的封包
  - ZZZ: Log的本体内容:通常为可以直接理解的描述(如有不明白可咨询 CS2 技术支持)
  - DDD: Log 的具体参数, 包括
    - Skt: socket ID
    - IP:Port: 来源的地址及端口
    - DID 信息: 与本 Log 相关的 DID 信息(可能是前缀-流水号 或者是完整的 DID)

## • Relay Server 的日志

- Relay Server 程序从 3.5.0 版本开始使用新版 log 记录, 低于 3.5.0 版本的 log 都是可以直接判读的, 如果想要更新 Relay Server 的版本, 请联系尚云互联技术支持。
- 成功连线日志: [2019-07-05 10:10:10.888]Logging - RSPort=10000, PPCS-999999-ABCDE, C:{IP:Port, 99.999Sec, 0G,000000KB}, D:{IP:Port, 88.888Sec, 0G,000000KB} (1)
  - [2019-07-05 10:10:10.888]:
  - RSPort=10000: 本次转发服务器线程所使用的端口。
  - PPCS-999999-ABCDE: 设备的 DID。
  - C:{...}: Client 端的统计资料, 依次为: Client IP 地址和端口, 从连线开始到收到最后一个封包的时间, 收到来自 Client 的总数据量。
  - D:{...}: Device 端的统计资料, 依次为: Device IP 地址和端口, 从连线开始到收到最后一个封包的时间, 收到来自 Device 的总数据量。
  - (1): 数字代表当前还有多少转发服务线程正在执行。
- 失败连线日志:

### 1. Device / Client 任一方没有响应:

```
[2019-07-05 12:00:14.084]Logging - RSPort=10185, Relay thread timeout exit!! DID=-000000-, Client Device did not response
[2019-07-05 12:00:22.570]Logging - RSPort=10186, Relay thread timeout exit!! DID=PPCS-004539-URHLR, Device did not response
```

- 明确记录是哪一端没有响应。

### 2. 出现未知来源封包:

```
[2019-07-05 12:51:40.252]Logging - RSPort=10187 <Packet from unknown addr> Addr=176.192.51519, MsgType=0x83, Size=28
```

- 出现未知来源封包的原因是: 本次转发服务线程收到了既不是用户端地址也不是设备端地址发来的封包, 这种记录只是单纯提示作用, 该封包不会被转发给用户端或设备端而是直接被舍弃。
- 为了避免过多的打印, 每一个转发服务线程只会第一次收到不明来源封包的时候打印, 因此有可能不止一个异常封包。
- 这种异常来源封包有时代表着设备端或者用户端的外网地址发生变化!!

## 实时查日志工具 – cs2Tail

- cs2Tail 程序是实时查看 P2P 平台 Log 的一个工具, 只会显示程序运行后 DID 的 Log 信息。