MySQL、Redis、MongoDB 網絡抓包工具

點擊關注 逆鋒起筆 2021-12-23 14:40

收錄於話題
#mysql 3 #軟件 1

以下內容來自公眾號逆鋒起筆，關注每日干貨及時送達 👇

逆鋒起筆
全網最新編程視頻教程、大佬們推薦的pdf 學習資料，全部免費分享！來到這裡，你不...
95篇原創內容

公眾號

來源:https://www.cnblogs.com/zhoujinyi/p/15343188.html

簡介

`go-sniffer` 可以抓包截取項目（MySQL、Redis、MongoDB）中的請求並解析成相應的語句，並格式化輸出。類似於在之前的文章MySQL抓包工具： MySQL Sniffer中介紹的mysql-sniffer。而go-sniffer 可以對更多數據庫進行抓包分析，現在來介紹在什麼情況下會使用該工具的。

使用

下載:

> github 地址：https://github.com/40t/go-sniffer

安裝:

安裝依賴包:

Centos：

```
yum -y install libpcap-devel
```

Ubuntu：

```
apt-get install libpcap-dev
```

另外還需要安裝golang，並且版本需要在1.10.3以上。

```
wget https://golang.org/dl/go1.10.3.linux-amd64.tar.gz
```

設置好相關的環境變量。如果不想要go環境，則可以直接在其他地方安裝好go-sniffer之後，複製到目標服務器上直接使用。

下載安裝

-- 安裝好go環境的服務器上：

```
go get -v -u github.com/40t/go-sniffer cp -rf $(go env GOPATH)/bin/go-sniffer /usr/local/bin
```

--安裝到設置好的go環境變量的目錄裡go-sniffer

參數說明：go-sniffer --help

```
[使用說明]

    go-sniffer [設備名] [插件名] [插件參數(可選)]

    [例子]
          go-sniffer en0 redis          抓取redis數據包
          go-sniffer en0 mysql -p 3306  抓取mysql數據包,端口3306

    go-sniffer --[命令]
               -- help 幫助信息
```

```
                --env  環境變量
                --list 插件列表
                --ver  版本信息
                --dev  設備列表
    [例子]
          go-sniffer --list 查看可抓取的協議

==========================================================================
[設備名] : lo0 :   127.0.0.1
[設備名] : en0 : x:x:x:x:x5:x  192.168.1.3
[設備名] : utun2 :   1.1.11.1
```

語法:

```
 $ go-sniffer lo0 mysql
 $ go-sniffer en0 redis
 $ go-sniffer eth0 http -p 8080
 $ go-sniffer eth1 mongodb
```

使用場景

—Redis： 審計、發現熱點key

關於Redis的知識點就不說了，主要來說明如何使用go-sniffer來抓包分析。如果想發現哪個key的操作比較多或則是否存在熱點key，在Redis4.0之前沒有什麼好辦法（4.0之後的LFU可以查看hotkey），只有通過統計各個客戶端發來的命令進行統計。雖然monitor可以看到某一刻的key操作，但是該命令消耗巨大，可能會造成客戶端緩衝區溢出。並且也沒有合適的插件來進行實現。即使有的話，對Redis的性能肯定有一定的損耗，所以只有監控其網絡來分析操作是對Redis服務的影響最小的。如對一個實例進行監控:

go-sniffer eth0 redis -p 6379 >> out.log 對通過eth0網卡的客戶端訪問端口為6379的Redis服務進行抓包，並把信息寫到文件中。該文件的日誌格式:

```
tcp and port 6379 get abc
 get abc
 get abc
 get abc
 get opq
 get opq
 get opq
 get opq
```

```
get xyz
get xyz
get xyz
```

可以看到，該文件的信息就是操作日誌，最後可以通過使用awk來分析，也可以把該日誌文件寫入到數據庫的表裡進行統計分析：

```
grep -avEi  "^#|^$|^tcp|^ INFO|^ AUTH|^ REPLCONF ACK|^ CONFIG GET"  out.txt |awk  '{print $1
      5 get abc
      4 get opq
      3 get xyz
```

注意：go-sniffer也需要消耗一定的資源，大致的消耗可以看以下表格：

OPS	Redis CPU	sniffer CPU
1.2W	20%	30%
5.5W	80%	140%
7.5W	98%	180%

從上面看到，go-sniffer所需要的CPU資源是Redis的2倍左右。所以，在使用該工具之前，先判斷本身服務器的資源是否夠用。

二MySQL：審計

```
go-sniffer eth0 mysql -p 3306 >> out.log
```

三MongoDB：審計

```
go-sniffer eth0 mongodb -p 27017 >> out.log
```

> `dot` 關注！

常用的抓包工具有哪些?

常見內網穿透工具使用總結

這才叫程序員的命令行生產力工具!

橫空出世，比Visio 快10 倍的畫圖工具來了

混淆後OKHTTP 框架的通用抓包方案探索

閱讀原文