**云密钥安全管理系统V1.5.1性能测试报告**

|  |  |
| --- | --- |
| 编 号： |  |
| 版 本： | V1.5.1 |

广东省电子商务认证有限公司





目录

[目录 1](#_Toc16690807)

[1 测试说明 3](#_Toc16690808)

[2 测试结论 3](#_Toc16690809)

[2.1 高配置服务器 3](#_Toc16690810)

[2.2 低配置服务器 4](#_Toc16690811)

[3 测试策略 5](#_Toc16690812)

[4 场景设计 5](#_Toc16690813)

[4.1 高配置服务器，P1签名100个并发 5](#_Toc16690814)

[4.2 高配置服务器，P1签名200个并发 6](#_Toc16690815)

[4.3 高配置服务器，P1签名500个并发 6](#_Toc16690816)

[4.4 高配置服务器，P1签名1000个并发 6](#_Toc16690817)

[4.5 高配置服务器，P7签名100个并发 6](#_Toc16690818)

[4.6 高配置服务器，P7签名200个并发 6](#_Toc16690819)

[4.7 高配置服务器，P7签名500个并发 7](#_Toc16690820)

[4.8 高配置服务器，P7签名1000个并发 7](#_Toc16690821)

[4.9 低配置服务器，P1签名100个并发 7](#_Toc16690822)

[4.10 低配置服务器，P1签名200个并发 7](#_Toc16690823)

[4.11 低配置服务器，P1签名500个并发 7](#_Toc16690824)

[4.12 低配置服务器，P1签名1000个并发 8](#_Toc16690825)

[4.13 低配置服务器，P7签名100个并发 8](#_Toc16690826)

[4.14 低配置服务器，P7签名200个并发 8](#_Toc16690827)

[4.15 低配置服务器，P7签名500个并发 8](#_Toc16690828)

[4.16 低配置服务器，P7签名1000个并发 8](#_Toc16690829)

[5 测试环境 9](#_Toc16690830)

[6 性能测试结果附图 10](#_Toc16690831)

[6.1 高配置服务器性能结果截图 10](#_Toc16690832)

[6.2 低配置服务器性能结果截图 13](#_Toc16690833)

# 测试说明

本次测试是为了测试云密钥管理系统P1签名、P7签名的短时间高并发响应时间，且分别在高低配置服务器下测试，以供后续分析性能瓶颈、优化系统性能做参考。

参考文档：

1. <http://192.168.0.11:8081/svn/rdrelease/软件发布/云密钥安全管理系统/5.接口文档/云密钥后台对外接口/云密钥安全管理系统对外接口文档(完整).docx>

# 测试结论

本次性能测试分别在高低配置服务器下测试云密钥安全管理系统P1签名和P7签名，测试结论总结如下：

1、两种服务器下，P1签名和P7签名均能支持1000并发，测试过程未出现过异常。

2、相同并发下，高配置服务器P1签名和P7签名性能略微优于低配置服务器。

具体测试结果如下：

## 高配置服务器

1. P1签名和P7签名均能支持1000并发，1000并发时平均响应约为2.9秒。
2. 测试并发过程未出现过服务器异常情况。

|  |  |  |
| --- | --- | --- |
| **高配置服务器（物理机）** | CPU | 2 × Intel Xeon Processor E5-2630V4 10C/20T 2.2GHz 25M 8.0GT/s 85W |
| 内存 | 2 × 32GB/DDR4/2133或2400或2666MHz/ECC/REG |
| 硬盘 | 2 × 1.8TB/SAS/10000RPM/2.5寸/企业级 |
| 加密卡 | SJK1555加密卡 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测试场景 | | 100并发运行2min | | 200并发运行2min | 500并发运行2min | 1000并发运行2min |
| P1签名 | 平均响应时间（s） | 0.301 | | 0.595 | 1.46 | 2.917 |
| 吞吐量（事务数/sec） | 328.8 | | 333.3 | 338.1 | 337 |
| 成功率 | 100% | 100% | | 100% | 100% |
| P7签名 | 平均响应时间（s） | 0.305 | | 0.61 | 1.49 | 2.966 |
| 吞吐量（事务数/sec） | 324.6 | | 325.1 | 332 | 331.4 |
| 成功率 | 100% | 100% | | 100% | 100% |

## 低配置服务器

1. P1签名和P7签名均能支持1000并发，1000并发时平均响应约为3秒。
2. 测试并发过程未出现过服务器异常情况。

|  |  |  |
| --- | --- | --- |
| **低配置服务器（物理机）** | CPU | Intel Xeon Processor E3-1220V5 4C/4T 3.0GHz 8M |
| 内存 | 8G/DDR4/2133或2400MHz/ECC-Unbuffer/2Ranks(单路专用） |
| 硬盘 | 2 × 1T企业级硬盘 |
| 加密卡 | SJK1555加密卡 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测试场景 | | 100并发运行2min | | 200并发运行2min | 500并发运行2min | 1000并发运行2min |
| P1签名 | 平均响应时间（s） | 0.376 | | 0.77 | 1.619 | 3.076 |
| 吞吐量（事务数/sec） | 263 | | 256.9 | 304.4 | 318.4 |
| 成功率 | 100% | 100% | | 100% | 100% |
| P7签名 | 平均响应时间（s） | 0.368 | | 0.687 | 1.502 | 2.963 |
| 吞吐量（事务数/sec） | 269.1 | | 287.9 | 328.3 | 331.1 |
| 成功率 | 100% | 100% | | 100% | 100% |

# 测试策略

1. 本次测试分别在高配置服务器和低配置服务器下，测试云密钥安全管理系统P1签名和P7签名的短时间高并发性能，分析签名性能的结果，以供后续调优系统性能。
2. 本次测试对虚拟用户进行平均比例分配:

|  |  |  |
| --- | --- | --- |
| 证书 | 状态 | 虚拟用户比例 |
| RSA单证书 | 有效 | 25% |
| SM2单证书 | 有效 | 25% |
| RSA双证书 | 有效 | 25% |
| SM2双证书 | 有效 | 25% |

# 场景设计

## 高配置服务器，P1签名100个并发

1. P1签名，运行虚拟用户为100个，其中RSA单证书25个虚拟用户，SM2单证书证书25个虚拟用户，RSA双证书25个虚拟用户，SM2双证书证书25个虚拟用户。
2. 1秒内增加100个虚拟用户，满100用户后，运行场景2分钟。
3. 满2分钟后，1秒停止100个虚拟用户。

## 高配置服务器，P1签名200个并发

1. P1签名，运行虚拟用户为200个，其中RSA单证书50个虚拟用户，SM2单证书证书50个虚拟用户，RSA双证书50个虚拟用户，SM2双证书证书50个虚拟用户。
2. 1秒内增加200个虚拟用户，满200用户后，运行场景2分钟。
3. 满2分钟后，1秒停止200个虚拟用户。

## 高配置服务器，P1签名500个并发

1. P1签名，运行虚拟用户为500个，其中RSA单证书125个虚拟用户，SM2单证书证书125个虚拟用户，RSA双证书125个虚拟用户，SM2双证书证书125个虚拟用户。
2. 1秒内增加500个虚拟用户，满500用户后，运行场景2分钟。
3. 满2分钟后，1秒停止500个虚拟用户。

## 高配置服务器，P1签名1000个并发

1. P1签名，运行虚拟用户为1000个，其中RSA单证书250个虚拟用户，SM2单证书证书250个虚拟用户，RSA双证书250个虚拟用户，SM2双证书证书250个虚拟用户。
2. 1秒内增加1000个虚拟用户，满1000用户后，运行场景2分钟。
3. 满2分钟后，1秒停止1000个虚拟用户。

## 高配置服务器，P7签名100个并发

1. P7签名，运行虚拟用户为100个，其中RSA单证书25个虚拟用户，SM2单证书证书25个虚拟用户，RSA双证书25个虚拟用户，SM2双证书证书25个虚拟用户。
2. 1秒内增加100个虚拟用户，满100用户后，运行场景2分钟。
3. 满2分钟后，1秒停止100个虚拟用户。

## 高配置服务器，P7签名200个并发

1. P7签名，运行虚拟用户为200个，其中RSA单证书50个虚拟用户，SM2单证书证书50个虚拟用户，RSA双证书50个虚拟用户，SM2双证书证书50个虚拟用户。
2. 1秒内增加200个虚拟用户，满200用户后，运行场景2分钟。
3. 满2分钟后，1秒停止200个虚拟用户。

## 高配置服务器，P7签名500个并发

1. P7签名，运行虚拟用户为500个，其中RSA单证书125个虚拟用户，SM2单证书证书125个虚拟用户，RSA双证书125个虚拟用户，SM2双证书证书125个虚拟用户。
2. 1秒内增加500个虚拟用户，满500用户后，运行场景2分钟。
3. 满2分钟后，1秒停止500个虚拟用户。

## 高配置服务器，P7签名1000个并发

1. P7签名，运行虚拟用户为1000个，其中RSA单证书250个虚拟用户，SM2单证书证书250个虚拟用户，RSA双证书250个虚拟用户，SM2双证书证书250个虚拟用户。
2. 1秒内增加1000个虚拟用户，满1000用户后，运行场景2分钟。
3. 满2分钟后，1秒停止1000个虚拟用户。

## 低配置服务器，P1签名100个并发

1. P1签名，运行虚拟用户为100个，其中RSA单证书25个虚拟用户，SM2单证书证书25个虚拟用户，RSA双证书25个虚拟用户，SM2双证书证书25个虚拟用户。
2. 1秒内增加100个虚拟用户，满100用户后，运行场景2分钟。
3. 满2分钟后，1秒停止100个虚拟用户。

## 低配置服务器，P1签名200个并发

1. P1签名，运行虚拟用户为200个，其中RSA单证书50个虚拟用户，SM2单证书证书50个虚拟用户，RSA双证书50个虚拟用户，SM2双证书证书50个虚拟用户。
2. 1秒内增加200个虚拟用户，满200用户后，运行场景2分钟。
3. 满2分钟后，1秒停止200个虚拟用户。

## 低配置服务器，P1签名500个并发

1. P1签名，运行虚拟用户为500个，其中RSA单证书125个虚拟用户，SM2单证书证书125个虚拟用户，RSA双证书125个虚拟用户，SM2双证书证书125个虚拟用户。
2. 1秒内增加500个虚拟用户，满500用户后，运行场景2分钟。
3. 满2分钟后，1秒停止500个虚拟用户。

## 低配置服务器，P1签名1000个并发

1. P1签名，运行虚拟用户为1000个，其中RSA单证书250个虚拟用户，SM2单证书证书250个虚拟用户，RSA双证书250个虚拟用户，SM2双证书证书250个虚拟用户。
2. 1秒内增加1000个虚拟用户，满1000用户后，运行场景2分钟。
3. 满2分钟后，1秒停止1000个虚拟用户。

## 低配置服务器，P7签名100个并发

1. P7签名，运行虚拟用户为100个，其中RSA单证书25个虚拟用户，SM2单证书证书25个虚拟用户，RSA双证书25个虚拟用户，SM2双证书证书25个虚拟用户。
2. 1秒内增加100个虚拟用户，满100用户后，运行场景2分钟。
3. 满2分钟后，1秒停止100个虚拟用户。

## 低配置服务器，P7签名200个并发

1. P7签名，运行虚拟用户为200个，其中RSA单证书50个虚拟用户，SM2单证书证书50个虚拟用户，RSA双证书50个虚拟用户，SM2双证书证书50个虚拟用户。
2. 1秒内增加200个虚拟用户，满200用户后，运行场景2分钟。
3. 满2分钟后，1秒停止200个虚拟用户。

## 低配置服务器，P7签名500个并发

1. P7签名，运行虚拟用户为500个，其中RSA单证书125个虚拟用户，SM2单证书证书125个虚拟用户，RSA双证书125个虚拟用户，SM2双证书证书125个虚拟用户。
2. 1秒内增加500个虚拟用户，满500用户后，运行场景2分钟。
3. 满2分钟后，1秒停止500个虚拟用户。

## 低配置服务器，P7签名1000个并发

1. P7签名，运行虚拟用户为1000个，其中RSA单证书250个虚拟用户，SM2单证书证书250个虚拟用户，RSA双证书250个虚拟用户，SM2双证书证书250个虚拟用户。
2. 1秒内增加1000个虚拟用户，满1000用户后，运行场景2分钟。
3. 满2分钟后，1秒停止1000个虚拟用户。

# 测试环境

|  |  |  |
| --- | --- | --- |
| **客户机环境** | Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz 3.40GHz 8G | |
| **操作系统** | Win7 64位 | |
| **云密钥安全管理系统版本** | V1.5.1 | |
| **高配置服务器（物理机）** | CPU | 2 × Intel Xeon Processor E5-2630V4 10C/20T 2.2GHz 25M 8.0GT/s 85W |
| 内存 | 2 × 32GB/DDR4/2133或2400或2666MHz/ECC/REG |
| 硬盘 | 2 × 1.8TB/SAS/10000RPM/2.5寸/企业级 |
| 加密卡 | SJK1555加密卡 |
| **低配置服务器（物理机）** | CPU | Intel Xeon Processor E3-1220V5 4C/4T 3.0GHz 8M |
| 内存 | 8G/DDR4/2133或2400MHz/ECC-Unbuffer/2Ranks(单路专用） |
| 硬盘 | 2 ×1T企业级硬盘 |
| 加密卡 | SJK1555加密卡 |
| **测试接口** | P1签名 | <http://192.168.200.93:8080/cloudkeyserver/pki/sign>  <http://192.168.200.80:8080/cloudkeyserver/pki/sign> |
| P7签名 | <http://192.168.200.93:8080/cloudkeyserver/pki/signdata>  <http://192.168.200.80:8080/cloudkeyserver/pki/signdata> |
| **测试脚本** | <http://192.168.0.11:8081/svn/rdrelease/软件发布/云密钥安全管理系统/3.测试/V1.5/云密钥安全管理系统V1.5.1性能测试脚本.jmx> | |
| **测试工具** | Jmeter V3.2 | |
| **测试人员** | 叶秋菊 | |
| **测试日期** | 2019-08-09~2019-08-09 | |

# 性能测试结果附图

结果参数说明如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Label | Samples | Average | Min | Max |
| 名称 | 请求总数 | 平均响应时间ms | 最小响应时间ms | 最大响应时间ms |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Std.Dev | Error% | Throughout | Received KB/sec | Sent KB/sec | Avg.Bytes |
| 所有请求响应时间的标准差 | 错误率 | 吞吐量（每秒事务数） | 每秒从服务器端接收到的数据量 | 每秒从客户端发送的请求的数量 | 平均数据流量 |

## 高配置服务器性能结果截图

图1：P1签名接口【100并发2分钟】



图2：P1签名接口【200并发2分钟】



图3：P1签名接口【500并发2分钟】



图4：P1签名接口【1000并发2分钟】



图5：P7签名接口【100并发2分钟】



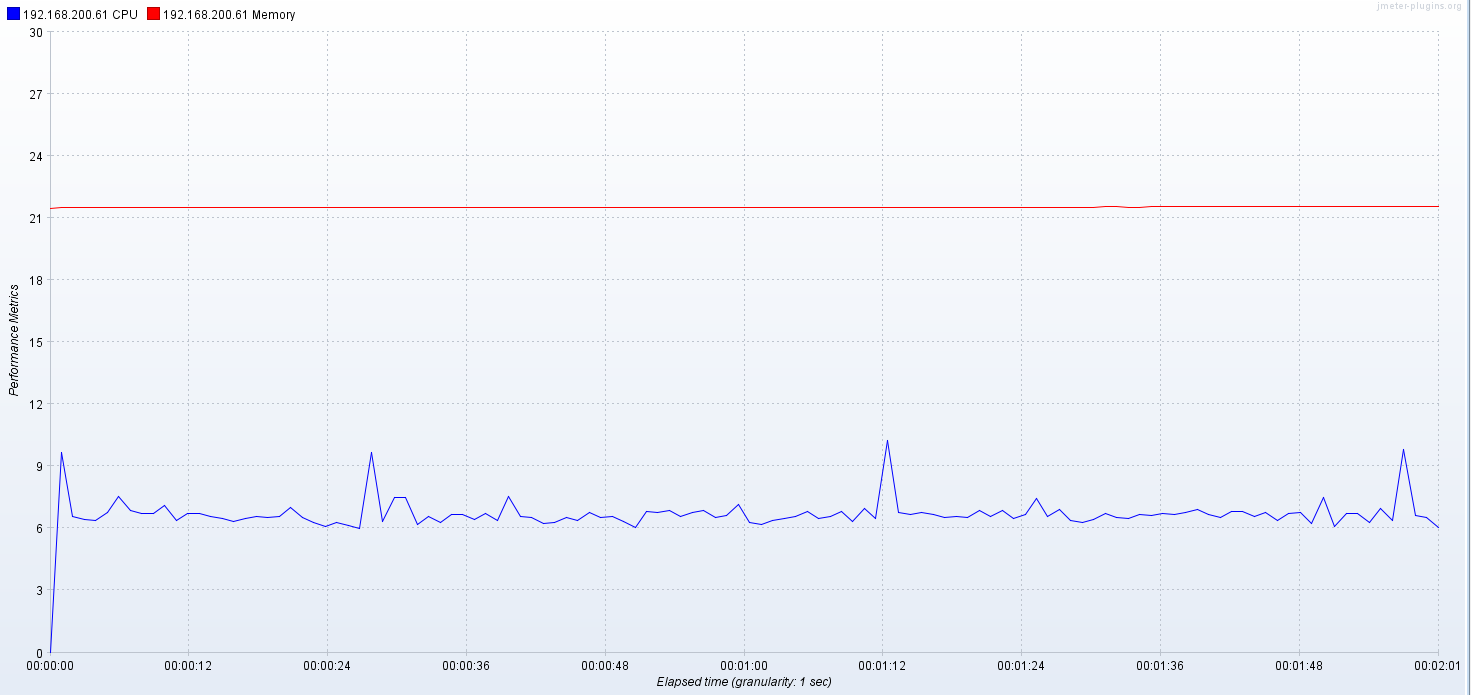
图6：P7签名接口【200并发2分钟】



图7：P7签名接口【500并发2分钟】



服务器CPU、内存监测情况



服务器硬盘I/O、网络I/O监测情况

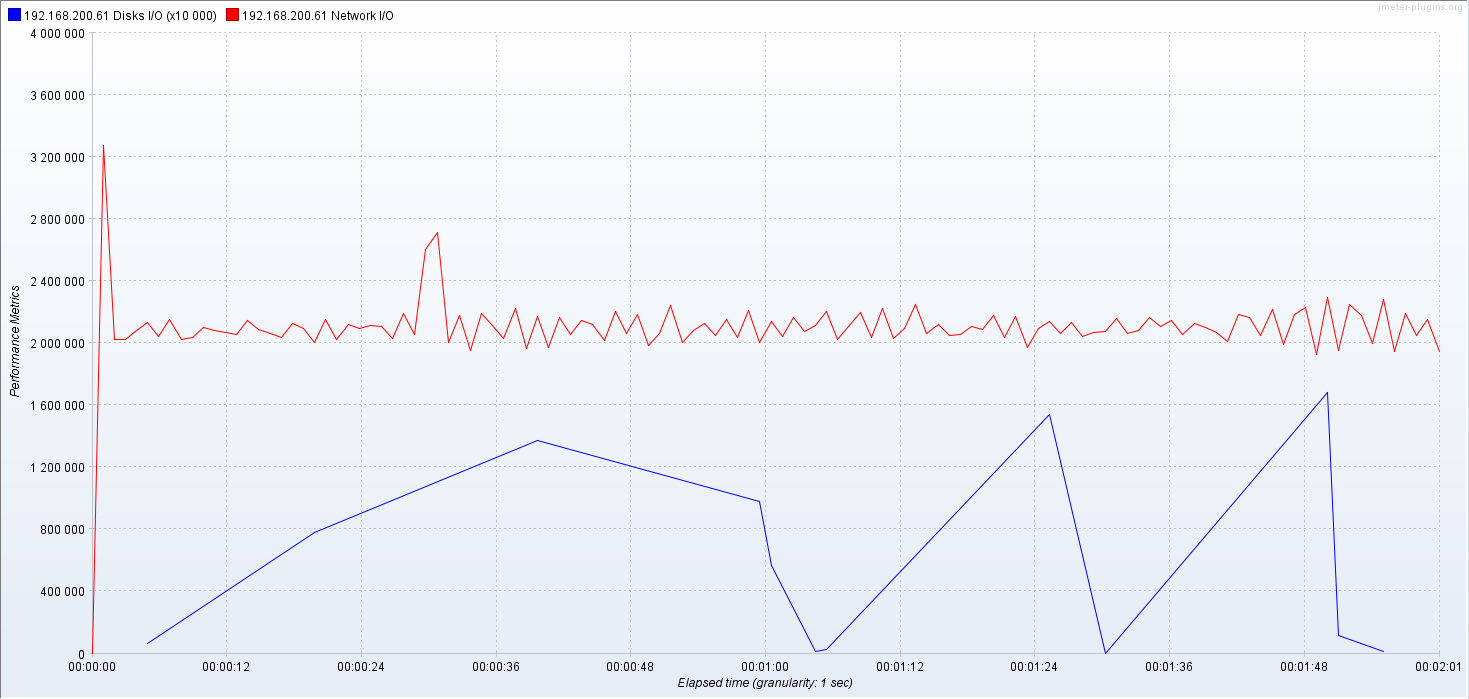
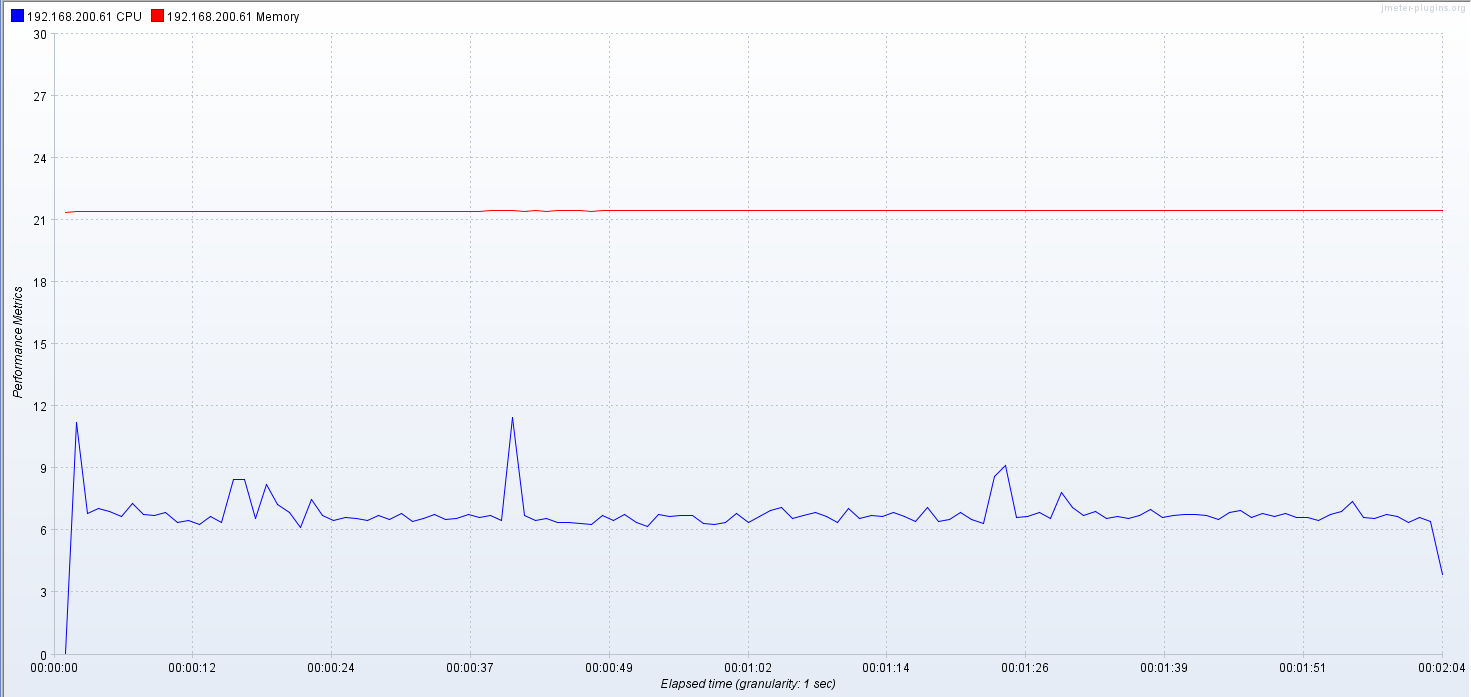


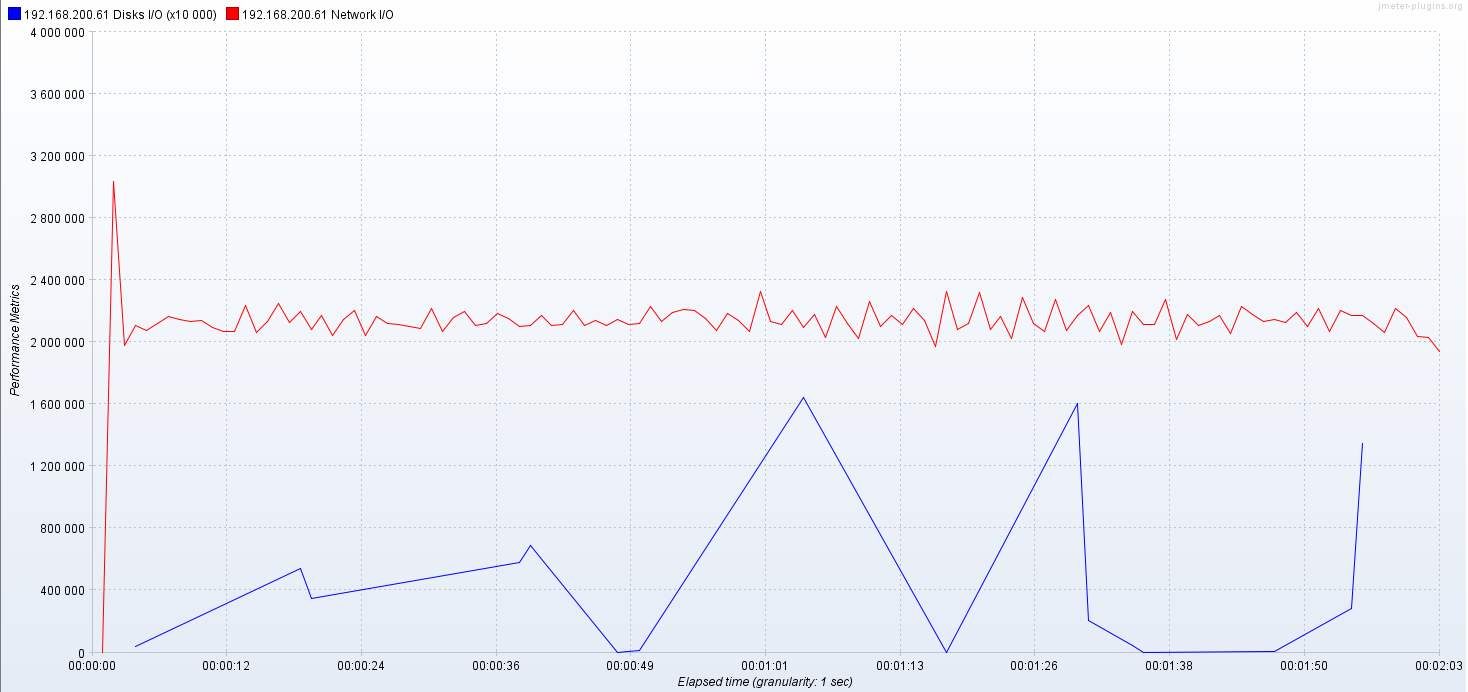
图8：P7签名接口【1000并发2分钟】



服务器CPU、内存监测情况



服务器硬盘I/O、网络I/O监测情况



## 低配置服务器性能结果截图

图1：P1签名接口【100并发2分钟】



图2：P1签名接口【200并发2分钟】



图3：P1签名接口【500并发2分钟】



图4：P1签名接口【1000并发2分钟】



图5：P7签名接口【100并发2分钟】



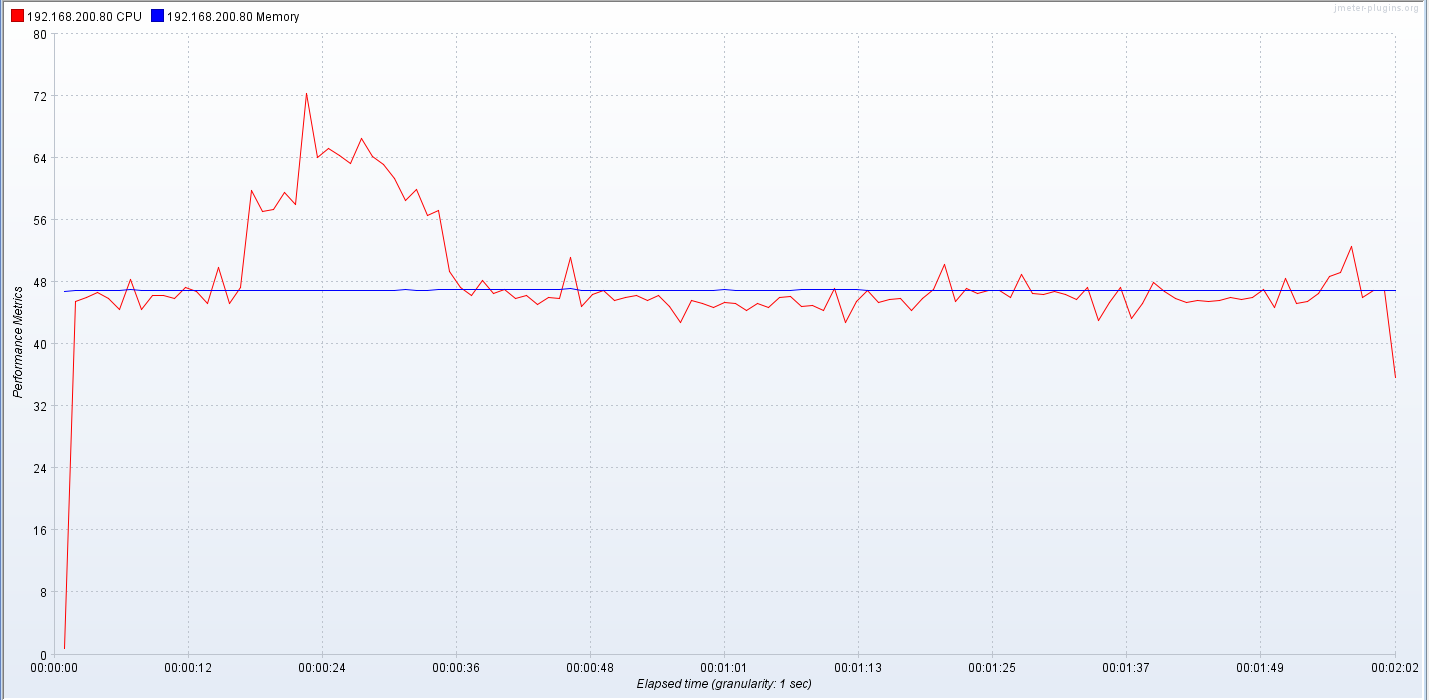
图6：P7签名接口【200并发2分钟】



图7：P7签名接口【500并发2分钟】



服务器CPU、内存监测情况



服务器硬盘I/O、网络I/O监测情况

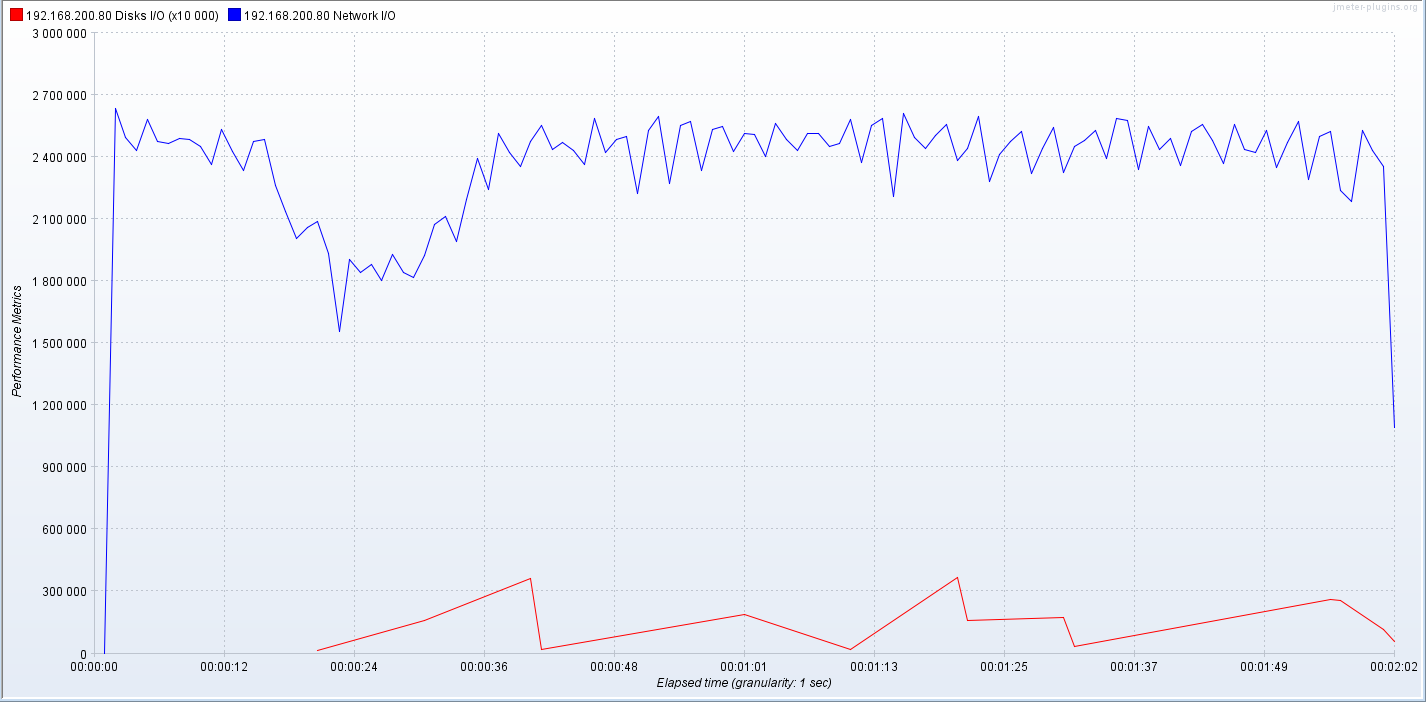
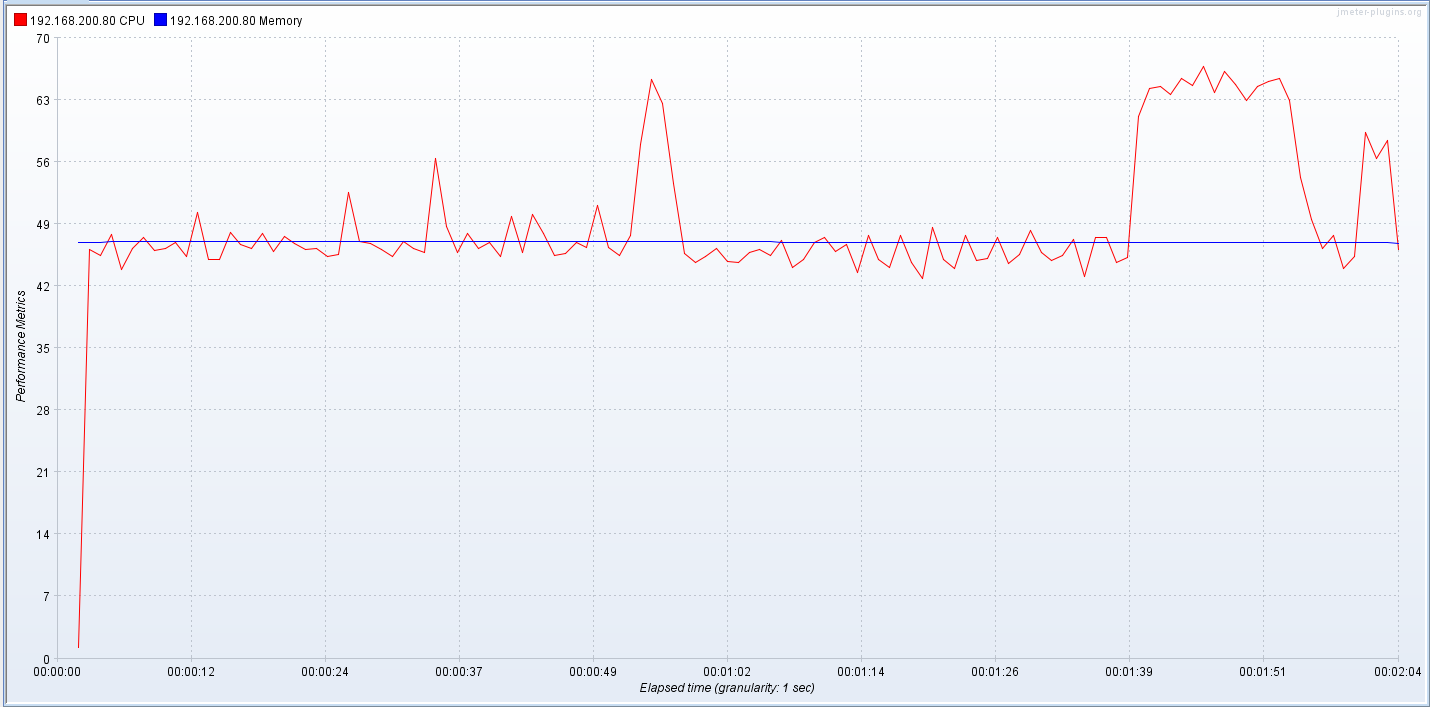


图8：P7签名接口【1000并发2分钟】



服务器CPU、内存监测情况



服务器硬盘I/O、网络I/O监测情况

