**JAVA版TOMCAT服务器时间戳服务V3.2.0测试报告**

**广东省电子商务认证有限公司**

**2018**

目录

[1 升级原因 3](#_Toc509479275)

[2 测试结论 3](#_Toc509479276)

[3 限制条件 4](#_Toc509479277)

[4 测试策略 4](#_Toc509479278)

[5 测试环境 5](#_Toc509479279)

[5.1 服务器环境（虚拟机） 5](#_Toc509479280)

[5.2 客户端测试环境 5](#_Toc509479281)

[6 测试结果 7](#_Toc509479282)

[7 性能测试 7](#_Toc509479283)

[7.1 场景 7](#_Toc509479284)

[7.2 结果统计 8](#_Toc509479285)

[8 问题列表 9](#_Toc509479286)

# 升级原因

为支持时间戳服务系统在具体项目中的应用，本次升级JAVA版时间戳服务系统到V3.2.0，与旧版本V3.1.2相比，升级内容包括：

（1）增加对SM2时间戳证书的支持，包括：加密机、PFX格式软证书。；

（2）完善“网页版-时间戳测试例程”，支持获取返回的时间戳证书。

参考资料：

1. 开发提交的测试申请单：http://192.168.0.123:8080/browse/RODT-710
2. 升级说明： http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCASERVER/NETCATimeStampServer/Java版/NETCA-TSA3.0实施文件/CentOS版本/部署与维护/部署与升级/时间戳服务V3.2.0升级说明.docx

# 测试结论

本次测试是Test Case First Pass（简称TCFP），共执行用例64个，Pass 64个用例，通过率为100 %。就提测的内容，评估为**测试通过**。

RMsis测试集统计结果如下图：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| 003\_时间戳服务V3.2测试（功能测试） | V3.2.0 | win7x86/IE11 | 8 Mar 2018 | 14 Mar 2018 | 60 passed | V3.2.0 |
| 004\_时间戳服务V3.2测试（性能测试） | V3.2.0 | win7x86/IE11 | 12 Mar 2018 | 20 Mar 2018 | 4 passed | V3.2.0 |

测试总结：

证书算法（RSA2048）+ 数据库（MySQL、Oracle、无数据库）+签名方式（JKS、PFX软证书、加密机）随机组合共9种组合下，时间戳服务均正常，测试4个用例获取时间戳通过；

证书算法（SM2 256）+ 数据库（MySQL、Oracle、无数据库）+签名方式（PFX软证书、加密机）随机组合共6种组合下，时间戳服务均正常，测试4个用例获取时间戳通过；

时间戳服务器证书为RSA算法时配置的是RSA新体系T2下的证书，时间戳服务正常，测试通过；

时间戳服务器证书为SM2算法配置为NETCA SM2 TEST01 and Evaluation CA01下的证书，时间戳服务正常，测试通过；

性能测试仅测试了SM2时间戳证书下的连加密机签名方式下性能，由于是虚拟机，并发数控制在100并发以内，各项服务正常，成功率99.99以上，平均响应时间均小于0.5S，测试通过，详细见第七章。

# 限制条件

* + - 1. （新）由于本次部署的时间戳是虚拟机环境，不适合做大并发量的性能测试，性能测试只测试了100个并发，作为参考，如后续有项目需要更大并发量需评估重新启动详细的性能测试。

# 测试策略

由于需要反复更改配置来测试时间戳服务是否正常，所以依次采用如下配置部署：

1. 配置RSA时间戳证书，采用JKS软证书签名方式，分别配置orcal、mysql数据库和不配置数据库，3种组合。
2. 配置RSA时间戳证书，采用PFX软证书签名方式，分别配置orcal、mysql数据库和不配置数据库，3种组合。
3. 配置RSA时间戳证书，采用连加密机证书签名方式，分别配置orcal、mysql数据库和不配置数据库，3种组合。
4. 配置SM2 256算法时间戳证书，采用PFX软证书签名方式，分别配置orcal、mysql数据库和不配置数据库，3种组合。
5. 配置SM2 256时间戳证书，采用连加密机证书签名方式，分别配置orcal、mysql数据库和不配置数据库，3种组合。
6. 对于配置SM2 256时间戳证书，采用连加密机证书签名方式，分别配置orcal、mysql数据库测试10~100并发性能情况。

# 测试环境

## 服务器环境（虚拟机）

|  |  |
| --- | --- |
| **操作系统** | CentOS 6.7 x64 |
| **JDK** | jdk-8u121 |
| **WEB服务器** | apache-tomcat-9.0.0.M17 |
| **数据库系统** | MySQL 5.7.12（本地配置）  Oracle 10g（192.168.0.96） |
| **时间服务器** | 192.168.0.96 |
| **连接的加密机** | 江南天安加密机 |
| **安全中间件** | Java - Linux64位，V5.0.0 |

## 客户端测试环境

|  |  |  |
| --- | --- | --- |
| **测试对象** | 时间戳服务系统 V3.2.0 | |
| **客户端硬件** | Win7 32：Intel(R) Core(TM) i7-6700 CPU @3.10GHz 3.10GHz 8G内存 | |
| **时间戳服务器证书的制证平台&证书模板** | 业务平台：<https://192.168.0.59/certbpms>  证书模板：   1. RSA 2048，证书的密钥用法带不可否认项：【12系统T2体系（测试用）】项目下的服务器模板【RSALx时间戳服务证书模板（带不可否认）】 2. SM2 256证书：在【开发支持时间戳证书测试用】项目下的服务器模板【时间戳证书模板SM2】 | |
| **测试工具** | Adobe Reader 11 | \\192.168.0.8\software\办公软件\Adobe\_Acrobat\_Reader\Reader 11 |
| 时间戳获取程序（NETCA\_GMTDEMO.exe） | http://192.168.0.11:8081/svn/rdrelease/测试文档/03\_测试工具/NETCA\_GMTDEMO.exe |
| 时间戳测试Demo（页面） | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCASERVER/NETCATimeStampServer/应用例程/时间戳应用解析DEMO/NETCA\_CRYPTO数字证书应用(时间戳应用含解析出毫秒)DEMO - 毫秒时间.rar |
| 新版页面测试DEMO | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCASERVER/NETCATimeStampServer/Java版/NETCA-TSA3.0实施文件/CentOS版本/部署与维护/其他/时间戳客户端测试工具/TSATestTool |
| CryptoTestTool | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool.exe（用于产生P10） |
| **标准版客户端** | [http://192.168.0.11:8081/svn/rdrelease/软件发布/统一介质管理工具/install/测试版/标准版/V2.0/网证通安全客户端.exe](http://192.168.0.11:8081/svn/rdrelease/软件发布/统一介质管理工具/install/测试版/标准版/V3.0/网证通安全客户端.exe)（V3.5.0.3） | |
| **测试网址** | 时间戳服务地址：<http://192.168.0.96/NETCATimeStampServer/TSAServer.jsp>  压力测试：  <http://192.168.10.114/TSATESTWEB/NETCA_CRYPTO_TIMESTAMP_NEW.html> | |
| **部署文档** | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCASERVER/NETCATimeStampServer/Java版/NETCA-TSA3.0实施文件/CentOS版本/部署与维护/部署与升级/NETCA-TSA网证通时间戳实施手册.doc Revision: 31160  <http://192.168.0.11:8081/svn/rdrelease/>软件发布/NETCASERVER/NETCATimeStampServer/Java版/NETCA-TSA3.0实施文件/CentOS版本/部署与维护/部署与升级/时间戳服务V3.2.0升级说明.docx | |
| **测试人员** | 叶利乔 苏思婷 | |
| **测试时间** | 2018-03-08至2017-03-20 | |

# 测试结果

本次测试是Test Case First Pass（简称TCFP），共执行用例64个，passed 64个,通过率为100%。测试结果文件格式如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Run Name**  **测试集名称** | **Test Case ID**  **测试用例编号** | **Test Case Name**  **测试用例名称** | **Test Case Status**  **用例结果** | **Artifact ID**  **缺陷编号** | **Artifact Summary**  **缺陷主题** | **Artifact Priority**  **缺陷优先级** |



# 性能测试

由于本次的时间戳服务器是虚拟机，性能不高，故性能测试仅测试SM2算法的时间戳服务连接加密机使用orcal或mysql数据库下的性能情况。

## 场景

|  |  |
| --- | --- |
| 场景1 | Orcal数据库下10个并发 |
| 每2秒增加2个 运行10分钟后每2秒减少2个。 | |
| 场景2 | Orcal数据库下20并发 |
| 每2秒增加5个 运行10分钟后每2秒减少5个。 | |
| 场景3 | Orcal数据库下30并发 |
| 每2秒增加5个 运行10分钟后每2秒减少5个。 | |
| 场景4 | Orcal数据库下40并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景5 | Orcal数据库下50并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景6 | Orcal数据库下80并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景7 | Orcal数据库下100并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景8 | Orcal数据库下10个并 |
| 每2秒增加2个 运行10分钟后每2秒减少2个。 | |
| 场景9 | Orcal数据库下20并发 |
| 每2秒增加5个 运行10分钟后每2秒减少5个。 | |
| 场景10 | Orcal数据库下30并发 |
| 每2秒增加5个 运行10分钟后每2秒减少5个。 | |
| 场景11 | Orcal数据库下40并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景12 | Orcal数据库下50并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景13 | Orcal数据库下80并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |
| 场景14 | Orcal数据库下100并发 |
| 每2秒增加10个 运行10分钟后每2秒减少10个。 | |

## 结果统计

根据7.1场景要求执行结果如下：



统计数据结果如下表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 场景 | 并发量 | 执行总数 | 成功 | 成功率 | 平均响应时间 | 最大响应时间 | 最小响应时间 |
| 1 | 10 | 270430 | 270430 | 100.00% | 0.017 | 3.034 | 0.005 |
| 2 | 20 | 201958 | 201956 | 100.00% | 0.052 | 4.097 | 0.005 |
| 3 | 30 | 266957 | 266957 | 100.00% | 0.061 | 9.517 | 0.005 |
| 4 | 40 | 82892 | 82873 | 99.98% | 0.283 | 4.132 | 0.007 |
| 5 | 50 | 97545 | 97536 | 99.99% | 0.302 | 4.314 | 0.006 |
| 6 | 80 | 268281 | 268281 | 100.00% | 0.175 | 4.406 | 0.006 |
| 7 | 100 | 184075 | 184067 | 100.00% | 0.327 | 3.981 | 0.006 |
| 8 | 10 | 251919 | 251919 | 100.00% | 0.019 | 0.095 | 0.005 |
| 9 | 20 | 150808 | 150808 | 100.00% | 0.073 | 0.333 | 0.007 |
| 10 | 30 | 85329 | 85324 | 99.99% | 0.206 | 1.26 | 0.008 |
| 11 | 40 | 101936 | 101927 | 99.99% | 0.23 | 1.481 | 0.007 |
| 12 | 50 | 87964 | 87954 | 99.99% | 0.337 | 2.064 | 0.008 |
| 13 | 80 | 265551 | 265551 | 100.00% | 0.177 | 1.073 | 0.006 |
| 14 | 100 | 216891 | 216891 | 100.00% | 0.277 | 1.967 | 0.006 |

总结：各项服务正常，100并发内，成功率99.99以上，平均响应时间均小于0.5S。

# 问题列表

无