|  |  |
| --- | --- |
|  | 密级：秘密  文件编号：OnlinePay\_MHB \_V1.0  文件类别：开发文档 |

吉高在线支付系统

维护手册说明书V1.0

**吉高（天津）网络技术科技有限公司**

**2012年7月20日**

文档修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 2012-07-20 | V1.0 | 创建 | XXX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

评审记录

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **内容** | **结果** | **评审人** |
| 2012-07-26 | V1.0评审 | 评审通过 | XXX |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 引言 5](#_Toc366249076)

[1.1 编写目的 5](#_Toc366249077)

[1.2 前景 5](#_Toc366249078)

[1.3 定义 5](#_Toc366249079)

[1.4 参考资料 5](#_Toc366249080)

[2 软件征述 6](#_Toc366249081)

[2.1 软件的结构 6](#_Toc366249082)

[2.2 程序表 6](#_Toc366249083)

[2.3 文卷表 6](#_Toc366249084)

[3 安装与初始化 7](#_Toc366249085)

[4 运行说明 7](#_Toc366249086)

[4.1 运行表 7](#_Toc366249087)

[4.2 运行步骤 8](#_Toc366249088)

[4.3 运行1（标识符）说明 8](#_Toc366249089)

[4.3.1 运行控制 8](#_Toc366249090)

[4.3.2 操作信息 8](#_Toc366249091)

[4.3.3 输入一输出文卷 8](#_Toc366249092)

[4.3.4 输出文段 9](#_Toc366249093)

[4.3.5 输出文段的复制 9](#_Toc366249094)

[4.3.6 恢复过程 9](#_Toc366249095)

[4.4 运行2（标识符）说明 10](#_Toc366249096)

[5 非常规过程 10](#_Toc366249097)

[二级安全事件 11](#_Toc366249098)

[三级安全事件 11](#_Toc366249099)

[6 远程操作 11](#_Toc366249100)

# 引言

## 编写目的

本手册目的是为系统维护人员提供项目部署安装及日常维护的方案。

预期读者：实施部、运维部

## 前景

描述：吉高在线支付系统，通过系统可以达到商户在线充值、转账、支付、退款、分润、退分润等功能业务，并以报表的形式将交易结果呈现给客户，除此之外还包括系统的一些信息管理。为商户提供方便快捷的服务。

项目提出：市场部、产品部

开发：IT技术部

用户：电商平台

## 定义

列出本文件中用到的专门术语的定义和外文首字母组词的原词组。

## 参考资料

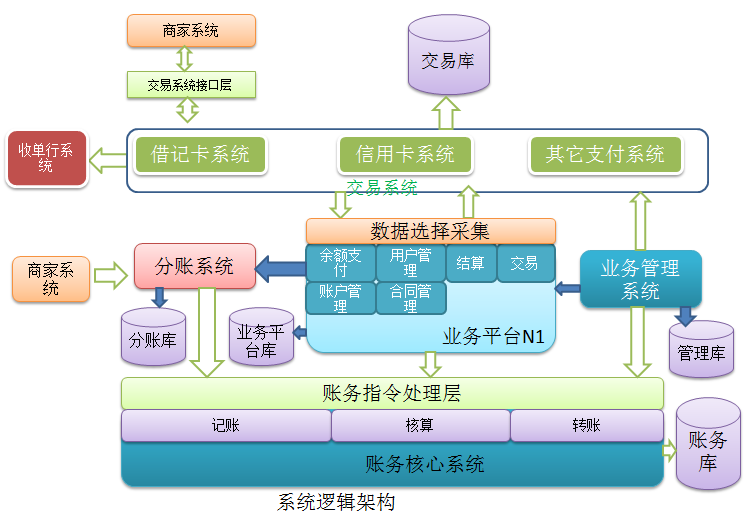
《操作手册编写规范》

《吉高在线支付系统部署方案》

《吉高在线支付系统应急手册》

# 软件征述

## 软件的结构



## 程序表

网关收银平台应用 cashier 版本V1.0

综合业务平台应用 easypay 版本V1.0

业务管理后台应用 boss 版本V1.0

## 文卷表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号 | 助记名 | 标识符 | 存储媒体 | 存储要求 | 存储时效 |
| 1 | Cashier\_log | Cashier.log | 文件 | 定期转储 | 保留18个月 |
| 2 | Cashier\_stdout | Stdout\_payment\_00.log | 文件 | 定期转储 | 保留18个月 |
| 3 | Easypay\_log | Catalina.log | 文件 | 定期转储 | 保留18个月 |
| 4 | Boss\_log | Catalina.log | 文件 | 定期转储 | 保留18个月 |

# 安装与初始化

安装JDK1.6.0\_35到/home/env 目录

1. 使用ROOT用户建立部署用户online，建立用户的环境变量，切换到online用户进行部署操作
2. 建立/home/production根目录，在此目录下建立子目录

bin 用来放置执行和启动脚本

conf 用来放置启动配置文件

apps 用来放置应用的二进制代码

logs 用来输出应用日志

resource 用来放置应用所需的访问资源，包括证书和安全性较高的文件

3. 在apps目录下建立各个系统目录，包括

cashier 收银平台

mapi 商户API调用系统

ismp 商户平台

boss 系统后台

ismsapp 业务平台辅助系统

4. 修改conf目录下配置文件，在bin目录下执行脚本启动各个系统应用

# 运行说明

## 运行表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 主机 | 目录 | 脚本名 | 执行程序 | 运行目的 | 运行编号 |  |
| app | /home/production/bin | Restart00\_cashier.sh  Restart01\_cashier.sh | cashier | 启动cashier应用 | 1 |  |
| App | /home/production/apps/boss/bin | Start.sh/restart.sh | boss | 启动boss | 2 |  |
| App | /home/production/apps/boss/bin | Shutdown.sh | boss | 停止boss | 3 |  |
| App | /home/production/apps/ismp/bin | Start.sh/restart.sh | easypay | 启动easypay | 4 |  |
| www | /usr/local/nginx/ | Restartnginx.sh | nginx | 重启nginx | 5 |  |
|  |  |  |  |  |  |  |

## 运行步骤

* 确认数据库服务正常运行；telnet dbserver 22 正常
* 登录app应用，启动各个应用系统cashier,boss,easypay,和应用服务器
* 登录www应用，启动nginx

4. 检查各系统日志文件没有异常输出

## 运行1（标识符）说明

1. 登录系统，切换用户online，命令sudo - online
2. 进入目录执行脚本 cd ~/bin/
3. 依次执行启动脚本 ./restart00\_cashier.sh
4. 执行./restart01\_cashier.sh
5. 查询运行日志 tail –f ../logs/cashier.log ,确保应用正确执行
6. 切换到www应用执行nginx做负载均衡
7. 打开浏览器访问应用cashier，确认页面访问正常

### 运行控制

通过www的nginx负载均衡各请求到相应的app应用

### 操作信息

执行脚本的目的是启动各应用系统，操作过程请切换到online用户进行操作；

各应用正常启动时间3-5秒

### 输入一输出文卷

日志文件存放路径~/production/logs目录和

cashier.log

jvm-default.log

stderr\_payment\_00.log

easypay应用的log在~/production/apps/ismp/logs/catalina.log

boss应用的log在~/production/apps/boss/logs/catalina.log

对cashier.log和easypay，boss应用log每周做一次转储，存放到日志服务器上，压缩存储，以供将来查询，日志至少保持18个月

### 输出文段

在各自应用log下输出文件内容

### 输出文段的复制

需要复制的文档主要报表发布的版本的备份，在各自目录下建立bak目录进行应用备份

### 恢复过程

#### 系统日志记录查看

* 系统错误日志：${SERVER\_LOG\_ROOT}/SystemErr.log 其中${SERVER\_LOG\_ROOT}为TOMCAT默认路径，可以在TOMCAT中自行配置
* 系统日常日志：${SERVER\_LOG\_ROOT}/SystemLog.log

#### 数据库日常备份与维护

* 数据库文件备份

定期备份数据库数据。

#### 日常维护

为保证服务器和网络设备的正常运行，及时发现、处理故障，现制定如下方案：

* 设备监控：系统管理员和网络管理员应每天定时检查服务器的运行状况，如发现异常情况，应及时与信息安全部联系，并作详细记录。
* 重要数据备份：对于交易系统数据库、电子邮件服务器中的用户信息，域名服务器中的域名信息，ftp服务器中的重要文件应进行及时备份，邮件系统的信息应天天更新备份，每周一次完全备份，备份信息应保存不少于18个月。域名信息每次有更新后进行备份；ftp服务器内容根据重要性的不同进行备份。
* 定期巡检：对于服务器和网络设备应每月去机房巡检，如遇到安全问题应立即升级。
* 故障登记：客服或相关人员对用户反映的问题应进行登记，并根据现象能进行初步判断问题所在，如判断为非用户问题，应及时通知维护人员。
* 故障响应与反馈：维护人员在接到维护通知后，应及时进行维护，同时填写反馈单，对于网络问题及时通知网管。对于因病毒或其他原因造成的网络重大故障，网管和维护人员应及时通报，并与其他部门合作，查找原因，力争尽快解决问题，并由网管人员形成处理过程的报告。

系统故障可以单独停止某个应用，然后重启应用；

## 运行2（标识符）说明

1 登录系统，切换用户online，命令sudo - online

1. 进入目录执行脚本 cd ~/apps/boss/bin

进入server bin目录启动脚本 ./restart.sh

1. 查询运行日志 tail –f ../logs/catalina.log ,确保应用正确执行
2. 切换到www应用执行nginx做负载均衡
3. 打开浏览器访问应用boss，确认页面访问正常

# 非常规过程

按事件的分类：

一级安全事件，应该进行抑制和监控；抑制和监控行为包括

* 如果可能的话，记录使用的用户名，IP地址及入侵者网域。
* 利用许可的技术控制手段，临时或永久地阻止入侵者访问。
* 保持警惕，阻止该用户或来自该IP地址的进一步攻击。

### 二级安全事件

对于二级安全事件，应该进行抑制、监控和警告；具体措施应包括：

* 收集并保护与该入侵有关的信息
* 利用许可的技术控制手段，临时或永久地阻止入侵者访问
* 分析攻击源。
* 联系ISP获取有关该入侵和入侵者的更多信息。
* 研究有关入侵方法可能带来潜在的风险，重新评估较高级别的安全事件及其抑制、消除以及恢复的措施和手段。
* 根据调查如果发现员工是一个不友好的用户，必须通过警告来防止此类事情再度发生。该雇员的管理者应该和人事部门共同依据可接受使用策略来处理该类事件。

### 三级安全事件

对于三级安全事件，应该抑制、消除、恢复并进行事件原因分析。具体措施应该包括：

1. 如果事件涉及持卡人数据，必须通知收单行和相关的信用卡组织机构。有关详细信息，请参阅下一节 -- 信用卡信息泄露特别响应。
2. 遏制入侵并决定采取何种措施。首先可以考虑拔掉网线、应用更严格的ACL、关闭/隔离交换机端口、停用该用户 ID、终止该用户的会话/更改口令等。
3. 通过离线方法收集和保护与入侵有关的信息。如果要求进行法律调查，应急响应组需要和法律和管理部门合作确定合适的法律专家。
4. 将有关情况通知管理层，并汇报每个后续步骤的进展情况。
5. 消除入侵者的访问途径以及任何相关的漏洞/弱点。
6. 研究攻击发起源。
7. 与 ISP 联系获取有关入侵尝试和入侵者的更多信息，提醒他们有责任在这方面提供协助。
8. 研究与所用入侵方法有关的潜在风险及可能导致的损害。总结事件发生的原因并据此修订安全策略，如有必要可修订应急响应流程。

# 远程操作

运行和监控可以通过公司内网或者VPN方式登录到MONO机器上，然后用应用建立的用户登录到app和www服务器上做本地操作；

**你好**