日志存储规范

文件编号	
文件版本	
编　　制	
批　　准	
负 责 人	
读　　者	
保密级别	Internal

修订记录

版本号	修订日期	修订概述	修订人	审核人	批准人	备注
Beta1.0	2011.3.18	建立初稿	张欧			
Beta1.1	2011.6.23	讨论后修订	张欧			
Beta1.2	2011.7.15	SQPG讨论后修订	张欧			
Beta1.3	2011.8.3	征集系统owner反馈后修订	张欧			
v1.0	2012.6.3	与ASA、SQPG讨论后修订	张欧			
v1.0	2012.6.25	参考ASA的建议进行命名规则修订	张欧			

分发/访问列表

姓名	角色	访问类型 (只读/编辑)

目录

1 目的

确保支付宝运维部管辖范围内所有的设备、系统和应用产生的日志信息能够进行有效存储与管理，满足合规需求、日志安全需求、日志查询与分析需求。

2 范围

本规范适用于支付宝生产环境所有的设备、系统和应用产生的日志信息。

3 人员职责划分

3.1 系统管理员

- 根据设备/系统/应用的特点，制定与维护日志存储计划 ；
- 确保各类日志的存储满足日志存储计划；
- 评估特殊日志存储的需求，并建立适当的特殊存储计划。

3.2 应用系统 owner

- 根据应用日志的内容，确定日志的存储期限；
- 对于默认存储计划不能满足的日志存储需求，提出特殊存储申请；
- 设置应用日志的文件名，以符合本规范中的日志命名规则；
- 提供需要备份的日志列表给系统管理员，避免备份无任何意义的日志。

3.3 安全管理员

- 通过日志进行安全审计
- 安全事件的分析

4 要求和操作

4.1 日志的产生和收集

各类设备/系统/应用的运行过程中都会产生日志，系统管理员须确保各类日志发送到日志统一存储系统。

应用系统 owner 须确保应用系统日志符合日志存储计划和日志命名规则，并提供需要备份的日志列表给系统管理员，避免备份无任何意义的日志。

4.2 日志的存储计划

4.2.1 原始日志存储

原始日志在产生日志设备默认保存 14 天，在磁盘空间不足的情况下，系统管理员根据日志生成时间的先后，删除较早的日志。

4.2.2 日志统一存储

系统管理员需要把原始日志收集到日志统一存储系统，进行集中管理。

日志统一存储的形式有两种：

- 在线存储，可以立即查询与分析，适用于访问频率高的日志。
- 离线存储，查询与分析的需要较长的准备时间（磁带存储），适用于访问频率较低的日志。

日志存储时间的配置规则有两种：默认存储计划和特殊存储计划。

- 特殊存储计划中有规定的日志，按照特殊存储计划保存；
- 特殊存储计划中对同一日志存储时间要求不同时，以存储时间长的为准。
- 其他的日志按默认存储计划进行保存。

4.2.2.1 默认存储计划

1） 应用日志

应用日志的保存时间由其包含的业务数据决定。如果一个日志文件中包括多种业务数据，保存时间以时间要求较高的为准。应用日志的保存计划见表 1。应用日志的保存时间将在日志名中体现。

表 1 应用日志保存计划

应用日志业务类型	在线保存时间	总保存时间
支付清算日志	1 年	5 年
客户身份验证日志	1 年	5 年
交易日志	1 年	3 年
关键数据修改日志	1 年	3 年
错误日志	1 年	3 年
信用卡业务日志	1 年	1 年
其他日志	3 月	3 月

- **支付清算日志**，日志中包含用户支付指令，支付宝向银行发出的支付清算指令等数据。
- **客户身份验证日志**，日志中包含用户身份验证、商户身份验证、登录密码验证、支付密码验证、数据签名验证、手机验证码验证等数据。
- **交易日志**，日志中包含交易创建、交易付款等交易过程中各个阶段产生的数据。
- **关键数据修改日志**，日志中包含客户身份信息、联系方式、安全认证信息、资产信息等数据的修改操作。
- **信用卡业务日志**，日志中包含信用卡还款、信用卡快捷、信用卡绑定等信用卡相关业务数据。
- **错误日志**，日志中包含应用或业务的错误信息。

2） 操作系统及组件日志

操作系统及组件日志存储计划见表 2。

表 2 操作系统及组件日志存储计划

日志分类	在线保存时间	总保存时间
系统日志	1 年	1 年
Apache 日志	3 月	3 月
Jboss 日志	3 月	3 月

4.2.2.2 特殊存储计划

对于默认存储计划不能满足的日志存储需求，可以建立特殊存储计划，系统管理员须维护特殊存储计划表，并根据存储计划进行日志的管理。

特殊存储计划至少应该包含以下的要素：

- 计划名称
- 需求的提出部门
- 建立计划的依据
- 日志的类型
- 目标设备与系统
- 日志保存时间
- 失效日期

特殊存储计划可以进行添加，修改与删除。特殊存储计划的变更须需求方提出申请，系统管理员评估通过，则添加新的特殊存储计划。计划失效后，须删除该计划。

日志特殊存储需求的申请流程：

- 需求方填写日志特殊存储需求申请表（见表 3）；
- 系统管理员评估；
- 建立特殊存储计划。

表 3 日志特殊存储需求申请表

提出部门	需求依据	日志名	目标设备与系统	日志量/天	在线保存时间/总保存	特殊计划失效日期

					时间	

4.3 日志的命名规则

1) 应用日志命名规则

文件名格式：{日志原名}.{原始日志保存时间}.{在线保存时间}.{总保存时间} .{日志业务类型标识}.log.{日期}

- 原始日志保存时间格式：{Num}dt
  - 代表原始日志在生产集群上保存的时间。
  - Num 是数字，d 表示天。
  - 缺省则按原始日志默认计划最多保存 14 天。
- 在线保存时间格式：{Num}{(d/m/y)}o
  - 代表日志集中在线存储的时间。
  - Num 是数字，d 表示天，m 表示月，y 表示年。
  - 缺省则按照该日志业务类型的默认保存时间保存。
- 总保存时间格式：{Num}{(d/m/y)}e
  - Num 是数字，d 表示天，m 表示月，y 表示年。
  - 缺省则按照该日志业务类型的默认保存时间保存。
- 日志业务类型是日志保存时间的依据。如果一个日志文件中包括多种业务数据，保存时间以时间要求高的为准。日志业务类型标识参考表 4。
  - 缺省则默认为其他日志。
- 日期：yyyy-mm-dd

表 4 日志业务类型标识

应用日志分类	日志类型标识
支付清算日志	p
客户身份验证日志	v
交易日志	t
关键数据修改日志	a

错误日志	e
信用卡相关日志	c
其他日志	d(可选项)

示例：

trade.14dt.1yo.3ye.t.log 表示这个日志是交易业务日志，总保存时间为 3 年，在线保存 1 年，原始日志在生产集群上保存 14 天。

trade.t.log 表示这个日志是交易日志，保存时间按照交易业务日志保存，原始日志在生产集群上保存 14 天。

cache-common.log 表示这个日志按照默认保存时间保存。

2）其他日志命名规则

日志分类	命名规则
系统日志	系统默认
Apache 日志	文件名格式：{日期}-{日志原名}.log ■ 日期：yyyy-mm-dd 举例： 2011-03-30-access.log
Jboss 日志	文件名格式：{日志原名}.log.{日期} ■ 日期：yyyymmdd 举例： stdout.log.20110323