文章编号：1005-8451（2015）12-0035-04

铁路货票系统Winhp3.0安全体系设计与应用

郑庆华
（哈尔滨铁路局　信息技术所，哈尔滨　150006）

摘　要：本文简述货票系统安全保障的重要性，从网络、主机系统、应用、运用管理几个方面横向分析货票系统的安全性保障，并结合哈尔滨铁路局Winhp3.0系统运行情况，结合货票系统实施中具体操作，从铁路局端到车站端纵向剖析系统运行中安全保障的措施，最大限度地保证系统安全运行。

关键词：货票系统；Winhp3.0；Radware；Weblogic；安全策略；负载均衡
中图分类号：U294.1：TP39　**文献标识码：**A

Security system of Winhp3.0 Freight Invoice System

ZHANG Qinghua
(Institute of Information Technology, Haerbin Railway Administration, Haerbin　150006, China)

Abstract: This article briefly described the security importance of the Freight Invoice System, analyzed the security guarantee of the System from the network, the host system, the application management. Combined with the running conditions of Winhp3.0 System in Haerbin Railway Administration and concrete operation in the Freight Invoice System, from the railway administration to the station, the article analyzed the security measures of the System to ensure the safe operation in detail.

Key words: Freight Invoice System; Winhp3.0; Radware; Weblogic; security policy; load balancing

铁路货票是铁路运营的主要票据之一，随着铁路信息化建设推进，目前，货票系统已升级为3.0版本，即Winhp3。货票系统能够正常运行的关键是安全保障。

货票系统的安全建设目标，是依据国家有关标准和规范，建立完整的安全保障体系，有效地保障货票相关业务的正常开展，保护核算收费依据和收费结果数据等敏感数据信息的安全。货票系统安全性能达到GB/T22239-2008《信息系统安全等级保护基本要求》的第3级。

1　Winhp3.0安全体系设计

货票系统主要由网络系统、主机系统、应用系统（重要的中间件服务器及Web应用服务器）及存储等的高可用性构成。网络系统核心设备和关键链路采用双链路冗余连接保障网络联通的高可用性。主机采用集群或负载均衡方式实现高可用性。

1.1　网络安全设计

网络安全设计遵照“铁道总公司计算机网络安全总体方案”，采用符合国家法规与业界标准的网络访问控制技术、用户身份强认证/授权技术、内容过滤技术和日志审计技术，实现多层次的纵深防御，遏制网络病毒和攻击，提升网络的可靠性。

安全保障方案在设计上，基于铁路信息系统的纵深防御框架，使用铁路安全生产网统一传输平台进行数据交换，出现异常时启动专用FTP软件作为备用传输。

通过对网络通信的主体、客体进行综合的认证，确保通信安全可靠，从而实现在保证网络相互隔离的基础上进行适度的、可靠的数据交换。

对于系统提交的访问请求进行身份鉴别，只有合法请求才能访问相关信息。

1.2　主机系统安全设计

（1）用户身份列表：包括所有可以在该服务器使用的用户信息；（2）访问控制策略：设定为管理人员的权限，确保管理人员只能执行权限范围内的行为；（3）审计策略：设定系统在一定时间段内，需要对什么样的时间进行审计；（4）根据不同工作角色：

收稿日期：2015-04-22
作者简介：郑庆华，工程师。

赋予不同权限，这个系统中主要的客体是数据报文、数据处理结果和表单处理；(5) 数据备份与恢复：为了保障数据存储安全性，采用 FC SAN 存储架构的存储系统对数据进行存储；(6) 高可用性与可靠性：数据库和存储采用双机、双存储，SAN 结构冗余配置。应用服务器等重点设备现场保留备件，硬件故障做到快速修改。

2 Winhp3.0应用安全设计

应用安全设计包括应用基础平台、应用访问控制和安全连接 3 部分。应用访问控制主要针对部、局级系统的访问控制，对权限、角色进行授权管理。(1) 用户身份鉴别：保证操作系统和数据库中不存在重复用户身份标识，身份鉴别信息不易被冒用；并且应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；(2) 访问控制：系统要求严格限制非法人员的使用，保证只有经过授权的人员可以访问应用系统；(3) 强化口令管理：在每次用户登录系统时，采用强化管理的口令进行用户身份鉴别；(4) 业务数据完整性和保密性保护：对数据的存储、传输进行加密，预防数据泄露，对共享的数据按照共享格式通过安全渠道进行共享；(5) 对用户输入的数据，系统要进行严格的数据校验；(6) 系统模拟与仿真：建立仿真系统，可对修改内容进行回归模拟，保证软件的强壮性、正确性；(7) 日志跟踪。

3 Winhp3.0安全运用管理

3.1 安全管理制度

(1) 日常管理制度；(2) 物理环境与设施管理制度（环境与安全设施管理制度，机房及设备间管理制度）；(3) 设备与介质管理制度（信息系统设备管理制度，介质管理制度）；(4) 运行与开发管理制度（运行开发安全管理制度，办公人员使用 IT 设备管理制度，授权与访问控制及口令管理制度，计算机病毒防治管理制度，监控与审计管理制度）；(5) 应急响应管理制度。

3.2 安全运维

实行铁路总公司、铁路局、货运站 3 级管理模式，按照专业管理、分工负责的原则，逐级做好货票系统的建设、应用管理、技术维护等工作。信息部门指定专人负责系统运行维护管理。确保应用软件根据需要按照铁路总公司的部署进行统一发布和更新。

3.2.1 数据资料安全管理

制定完善的数据资料保密管理办法，明确存取权限、存取方式和审批手续；不擅自向其他系统提供信息，也不得利用系统的软件、数据等从事其他活动。

3.2.2 服务器安全管理

建立完整的服务器运行日志、操作记录及其它与安全有关的资料，专人负责保管；定期检查服务器运行状态，确保其处于正常工作状态；建立并严格执行服务器安全管理制度，无关人员未经安全责任人批准严禁登录系统服务器、安装与货票系统无关的软件。

3.2.3 操作安全管理

采取严密的安全措施防止无关用户进入系统；服务器操作系统口令、数据库管理系统的口令必须由专人掌管，并定期更换；各岗位操作权限要严格按岗位职责设置，并定期检查操作员的权限；及时清除不安全隐患。

3.2.4 计算机病毒防范

指定专人负责计算机病毒防范工作，定期进行病毒检测，发现病毒立即处理并报告；系统安装使用的介质在使用前应进行病毒例行检测，禁止运行未经病毒检测的软件和文件；采用铁路总公司信息主管部门许可的正版防病毒软件并及时更新软件版本。

3.2.5 应急管理

对系统可能发生的突发事件要制定应急处理预案；对执行应急预案的全体人员应进行专项培训，定期进行检查、测试和演练；根据测试和演练结果，不断完善应急预案。

4 哈尔滨铁路局Winhp3.0安全保障实践

哈尔滨铁路局（简称：哈局）维护组在货票系统实施中增加运行环境监控职责，货票系统应用服务器、数据库、网络和信息安全等纳入铁路统一的监控管理体系，由各级生产运维单位负责系统环境的运维。

作为哈局维护组认真做好货票系统运营工作，结合哈局实际运行情况，对货票系统日常安全保障从路局端到车站端细化安全维护任务。

4.1 哈局端维护

哈局端 Winhp3.0 系统构架主要分为 3 个部分：负载均衡，应用服务器，Weblogic 中间件。

4.1.1 负载均衡

负载均衡主要是将货票客户端的业务数据链接分配到相对应的应用服务器上。负载均衡采用 2 台 Radware 双机热备。当其中 1 台出现故障时不会影响系统运行，会自动切换到另 1 台正常的 Radware 上。当 2 台同时出现故障时，可以将备份的负载均衡配置文件载入到其他系统 Radware 负载均衡上。

4.1.2 应用服务器

应用服务器采用 Weblogic 中间件提供相应的应用服务，当某台应用服务器出现故障时，可在短时间内实现重新部署上线。

4.1.2.1 负载均衡关闭及启动流程

Winhp3.0 系统各应用部署时，为防止车站在升级期间登录程序进行制票，首先应将负载均衡从网络上断开，部署完成后在将负载均衡连接到网络上。

4.1.2.2 系统应用部署方法

所有部署前必须申请停机维护天窗，将负载均衡网线拔出。顺序为先拔备，后拔主。接着将对应的服务停止，并做好备份工作。查看服务状态是否为活动，健康状态是否显示 OK。部署完成后，将负载均衡网线插回，顺序为先主后备。

TRANSPORT：登录时的参数传输，各类数据库字典更新都需要修改重启 TRANSPORT 服务更新前要查看更新包内是否有数据库配置文件。如果有要将数据库文件删除后再覆盖。修改数据库配置文件后需要删除重新部署。

JCSJ：基础数据网页发布程序。

HPTAX：增值税数据传输服务。

HPPIZ：联机制票服务器（暂未上线）。

HPEPAY：电子支付服务器。

HPAPP：货票应用服务器。

后台数据库建立在机房的大存储中，是双机热备，其中一台出现故障不影响使用。

4.1.3 Weblogic中间件

应用服务器采用 Weblogic 中间件提供相应的应用服务，当某台应用服务器出现故障时，可在短时间内实现重新部署上线。Weblogic 集群部署分布在 10.16.6. *49、10.16.6. *50 和 10.16.6. *66 这 3 台机器上。负载均衡健康检查：在 Health Monitoring 中的 Check Table 中查看所有 server 的状态 。

4.2 车站端维护

4.2.1 终端授权管理功能

对铁路营业厅制票机、信息采集点、信息应用点、监控终端等进行序列号、制票卡、访问地址等进行登记和授权。

4.2.1.1 序列号管理

制票软件序列号生成、登记、发放、销毁，只有有效的序列号才能联入货票系统进行货票、杂费票据填制，以及采集上报信息。

4.2.1.2 制票卡管理

制票卡申领、发放、维护、报废登记等生命周期管理，每台制票机、信息采集机配置一块制票卡，配合软件序列号进行生产授权。

4.2.1.3 地址管理

对铁路总公司货票系统数据服务相联的下级服务器的 IP、应用用户 Web 访问的 IP 地址进行登记，根据用途进行不同的授权。

4.2.2 各种问题流程闭环

对故障进行分类：软件问题、使用系统问题、更新升级问题、硬件问题、货规与货票不符问题、打印故障、传输故障、增值税问题。对不同类有不同处理流程，对应不同的处理方法，并核实是否解决问题，确保制票过程畅通。

5 结束语

以上针对 Winhp3.0 从上层安全性设计部署，安全保障的体系建立，到铁路局层具体应用的实施。安全保障措施的应用具有检测、发现、报警、记录入侵行为的能力；对安全事件进行快速响应处置，并能够追踪安全责任的能力；在系统遭到损害后，能够较快恢复正常运行状态的能力；对系统资源、用户、安全机制等进行集中控管的能力。最大限度保证货

票系统安全正常的运行，保证货运运输不在货票的环节正常、准确运营。

参考文献：

[1] 朱　彤 . 浅论货票信息管理系统的优势 [J]. 管理研究，2009 (7) .
[2] 铁路信息技术中心货票维护组 . 货票系统升级初步方案 [Z]. 北京：铁路信息技术中心货票维护组，2013.
[3] 哈尔滨铁路局信息所货票维护组 . 哈局货票系统应急预案及操作手册 [S]. 哈尔滨：哈尔滨铁路局信息所货票维护组，2014.

责任编辑　徐侃春

（上接 P34）

对应两个节点）。这就需要用到数据库同义词，即别名。例如，上海动车段和虹桥运用所的前、后台程序共用一个服务器，即共用一个 IP 地址，通过 JWMQ 从铁路总公司往该 IP 地址的文件要么发给上海动车段，要么发给虹桥运用所，不可兼得。因而需给虹桥运用所数据库和上海动车段数据库表取同义词，即别名。虹桥运用所数据库的表别名指向它自己。但上海动车段数据库的表别名却指向虹桥运用所数据库的同名表。所以，发给上海动车段的文件实际上是先发给虹桥运用所，然后再通过别名，将这些文件从虹桥运用所转发给上海动车段，如图 3 所示。

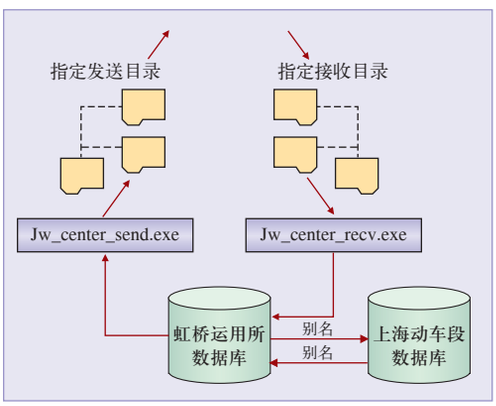

图3　有转发机制的动车组管理信息系统JWMQ架构图

2.4　防死锁机制

由于动车组管理信息系统的业务的量的增长和质的复杂，各数据库的压力越来越大。因此，很多的传输丢失实际上是因为数据库存在死锁对象。很多时候，某些数据库对象被死锁是因为在等待数据的成功传输，但同时数据库对象被死锁反过来又可能进一步恶化数据的传输，形成恶性循环。严重时可能还会造成传输中断。还需防死锁机制，一旦发现数据库存在死锁对象，立刻处理，迅速恢复 JWMQ 传输，然后再分析造成死锁的原因。

2.5　实时传输机制

JWMQ 毕竟是一种基于队列须排队轮候的传输方式。实时性不能完全得到保证，还需补充实时传输机制，通过触发器和 Database Link 将须实时传输的数据优先、快速传输出去。

2.6　垃圾文件清除机制

JWMQ 是一种基于文件的传输，文件是要传输的数据的载体。当数据通过文件这个载体传输成功后，文件仍保留。这种保留相当于是一种备份，时间一长，这些文件成了垃圾文件。日积月累，垃圾文件会越积越多，严重占用资源，所以设有垃圾文件清除机制。通过定期清除过时的垃圾文件，释放资源，保障 JWMQ 传输的正常运行。

3　结束语

经过改进的 JWMQ 传输平台已成功应用于动车组管理信息系统。该平台实用、高效、可信赖，在传输环境复杂的情况下，为动车组管理信息系统的长期稳定可靠运行提供了强有力的技术支撑，是动车组管理信息系统的关键技术之一。

参考文献：

[1] 王　辉，张惟皎，王　治 . 动车段动车组管理信息系统架构设计与关键技术分析 [J]. 铁路计算机应用，2013，22（1）.
[2] 史天运，孙　鹏 . 动车组管理信息系统的建设与发展 [J]. 铁路计算机应用，2013，22（1）.
[3] 张莉艳，崔丽新，张惟皎 . 动车组管理信息系统信息安全体系研究 [J]. 铁路计算机应用，2013，22（1）.
[4] G.Wiederhold, Mediators in the Architect of Future Information Systems[J]. IEEE Computer C-25,1992,(1).
[5] 王石生，李　平，王英杰，史　宏 . 铁路应急平台中数据传输机制研究与实现 [J]. 铁路计算机应用，2010，19（1）.

责任编辑　徐侃春