

基于云服务的智能电网调度管理系统灾备方案及安全加固设计

随着智能电网的飞速发展，电力调度业务需求不断增加，调度管理系统已成为调度控制生产管理工作重要的手段。面对承载业务和访问用户的迅猛增长，通过采用省地两级三级应用的云架构部署方式，设计应用基于DM数据库守护进程的灾备方案，并使用基于数字证书的SSL双向认证方式以及多种防SQL注入手段，有效支撑省、地和县三级调度用户安全、可靠且高效应用调度管理系统。

徐征¹ 刘红军¹ 李胜² 马强¹ 管冀¹ 辛刚^{1/1}. 山东电力调度控制中心
2. 江西南昌泰豪软件股份有限公司

0 引言

为适应智能电网发展和电力体制改革对调度管理工作提出的更集约、更扁平及更专业的要求，山东电网进行了省地县一体化调度管理系统（Operation Management System, OMS）建设，实现了调度内部跨专业的高效流程管理和省调、地调、县调垂直一体化专业管理。随着业务的不断拓展和延伸，OMS并发用户数量和使用频率出现爆发式增长，给OMS数据处理和存储造成很大压力，同时对数据安全和系统安全也提出了更高要求。为解决上述问题，OMS采用云平台硬件结构完善、主备即时同步和安全性能加固等措施，实现OMS资源的统一管理，保障系统数据和信息的共享和传输安全。

1 整体云架构设计

本系统硬件建设在已有的OMS基础上，充分利用云计算的虚拟化、分布式存储与分布式计算等各项关键技术，将OMS及相关应用架构到云计算体系

上，提高资源利用率、系统可靠性和安全性，极大地加快了数据处理及分析速度，为调度人员提供更优的决策依据。重新架构的系统增强了调控人员驾驭不断扩大、日益复杂的电网能力，满足了加强智能电网发展战略要求。OMS云平台硬件架构设计如图1所示。

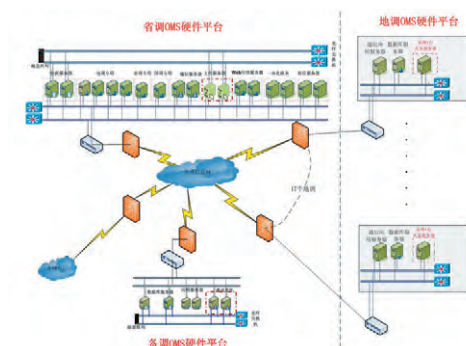


图1 OMS云平台硬件架构设计

基于云计算的OMS系统硬件部署方案，引入虚拟化平台将各地市的服务器整合为2套热备冗余的虚拟集群，满足《智能电网调度控制系统调度管理应用（OMS2.0）》省地两级部署三级应用的分布式部署推荐方案。

利用虚拟化技术，在不改变部署的情况下，实现对现有OMS系统资源的集中管理、监控和统一调配，做到按需快速分配，使安装配置及故障排除自动化，将停机时间从小时级降低至分钟级。

采用分布式存储，提高数据的存储能力、可靠性和可用性，通过并发工作模式，提高吞吐量、降低延迟。采用并行处理模式解决计算瓶颈问题，提高计算速度，确保分析结果的时效性和准确



徐征/工程师

关键词/Keywords

调度管理系统 ·
OMS ·
安全加固 ·
云架构 ·
灾备设计 ·

性。满足未来海量数据的搜索、业务分析及智能决策需要。

图2和图3为用户登陆时间压力测试结果图。在2 000用户在线的前提下，压力测试用户的登录时间，通过两图对比，明显看出采用云服务架构后的系统响应时间波动在170 S峰值之下，较集中式部署270 S的波动区间有很大提升。

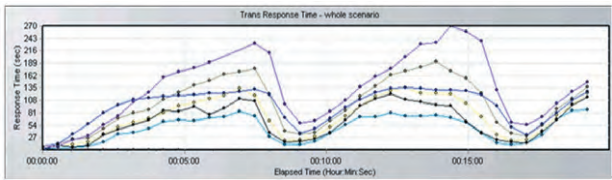


图2 服务器集中式部署响应时间图

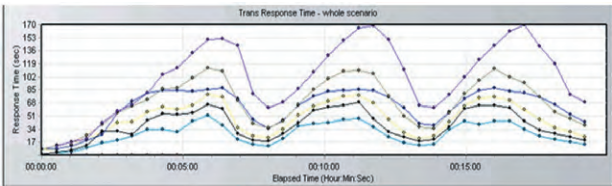


图3 云服务系统登录时间性能对比图

2 系统灾备设计方案

为解决由于硬件故障、自然灾害等原因导致的数据库服务长时间中断问题，满足用户不间断提供数据库服务的要求，OMS创新采用一种基于数据库守护进程的数据守护方案，实现将主机上的REDO日志通过MAL系统发送到异地备机上，备机将接收到的REDO日志重做，实现主备机数据一致。在主机出现运行故障后，数据守护通过数据库模式的切换实现主数据库和备数据角色的互换，从而保证了OMS的不间断工作。主备服务器切换关系图如图4所示。

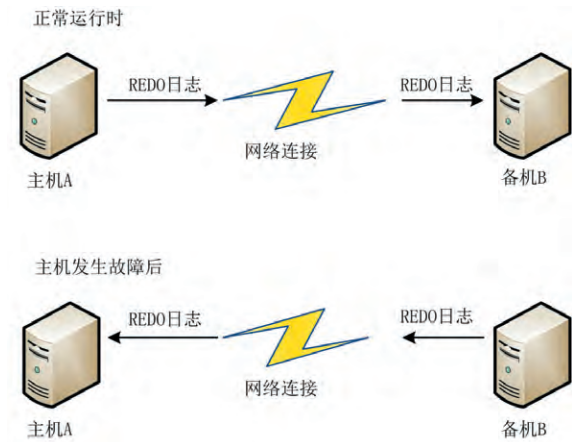


图4 主备服务器切换关系图

2.1 主备信息传递

数据守护方案的核心是信息的传递，信息以TCP和UDP相结合的方式，在主备数据库、守护进程和监视器之间相互传递，并最终达到状态监测、控制和角色转换等目的。数据守护方案信息流转图如图5所示。

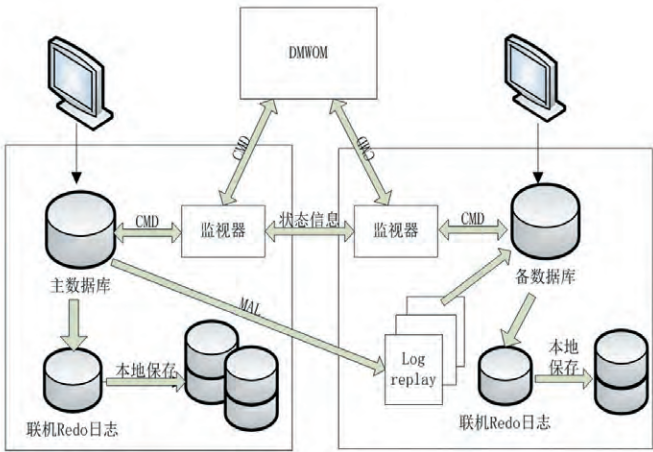


图5 数据守护方案信息流转图

核心的信息流转包括：

(1) 主数据库与备数据库

主数据库通过基于TCP协议实现的MAL系统，发送REDO日志到备数据库，REDO日志包括运行产生的实时归档日志和恢复时的本地归档日志。

(2) 守护进程与数据库

守护进程定时以UDP消息的方式，通知其监控的数据库，守护进程本身是活动的。当满足切换条件时，发送模式切换、状态转换和发送归档日志等消息给数据库。数据库只接收本地守护进程的UDP消息，不接收远程守护进程的UDP消息，也不接收监视器的UDP消息。

(3) 监视器与守护进程

监视器也通过广播UDP消息，向守护进程传递启动监控、停止监控和切换主备数据库等命令。

借助DM7的REDO日志归档机制，将主数据库产生的REDO日志，通过网络传递到备数据库，备数据库的REDO日志重做服务解析并重做REDO日志，在对应数据页的对应偏移上写入最新数据；从而，实现了备数据库与主数据库之间的数据同步。这种同步是纯粹物理层面的同步，可以

严格保证主、备数据库之间数据是完全一致的。

2.2 备机设计与实现

由于OMS系统数据库数据规模较大，同时在线的用户有数千人，且还在增长，若只有一台实时备机，数据处理性能会受到影响。为此采用实时备机和异步备机共存的设计方案：实时备机会在主机发生故障时，自动切换为主机；异步备机不支持主机故障时的实时切换，但是会定时实现跟主机的数据同步。

2.2.1 备机同步原理

整个同步系统由安装在主机和备机上的Agent进程组成，主机的Agent进程对DM的日志进行监控，主机端的数据发生任何数据操作，操作命令都会在Redo log中保存，RealSync Agent通过对获取的Log文件进行分析，或得本次操作的SQL交易命令和交易数据。确认发生数据变化后，将SQL命令和交易数据转为xf1格式文件，通过网络传送给备机端。备机端的RealSync Agent接受到数据包后，进行校验，确认数据包的数据完整后重新执行交易，此时便完成了一次数据同步。异步备机的实现原理就是为同步工作设置了时钟触发，根据数据的更新频率，来设置触发周期。

2.2.2 主机的配置

需要修改的配置有：dm.ini、dmmal.ini、dmarch.ini、dmwatch.ini和设置数据库OGUID值。因为增加异步备机，需特殊配置dmtimer.ini，定时触发主机发送归档日志到异步备机：

```
FREQ_MONTH_WEEK_INTERVAL = 1
FREQ_MINUTE_INTERVAL = 0
START_TIME = 00:00:00
END_TIME = 00:00:00.1047296
DURING_START_DATE = 2014-09-11 17:36:09
DURING_END_DATE = 9999-12-31 23:59:59
```

2.2.3 异步备机的配置

异步备数据库配置文件dm.ini、dmmal.ini和

dmarch.ini同主机配置。另需修改dmwatch.ini配置守护进程：DW_BRO_ADDR根据dmmal.ini中的MAL_HOST配置项计算得出，DW_UDP_PORT配置项与dm.ini的DW_UDP_PORT配置项保持一致，INST_UDP_PORT配置项与dm.ini的INST_UDP_PORT配置项保持一致，INST_OGUID与主机守护进程配置保持一致，DW_MODE配置为2，表示该守护进程守护的是异步备机。山东OMS异步备机采用具体配置如下：

```
DW_BRO_ADDR = 10.37.255.255
DW_UDP_PORT = 5243
DW_MODE = 2
INST_OGUID = 82379
INST_SERVICE_IP = 10.37.*.* #实例对外服务IP
INST_UDP_PORT = 5253
INST_STARTUP_MODE = 1 #0: 服务方式启动； 1: 控制台方式启动
```

2.3 主备机切换

主机、实时备机和同步备机配置好后，网络状态一旦变化，守护进程会对数据库的模式进行切换，从而完成数据库主备模式的切换。同时数据库的超级管理员可手动实现主备之间的切换。

3 安全性能加固方案

OMS的安全防火墙在网络传输层采用HTTPS和基于数字证书的双向认证方式进行HTTP请求传输；在系统层采用硬件防火墙或Linux操作系统防火墙，屏蔽不允许外部访问的端口；在代理层采用HTTP代理服务器的基于规则定义的方式，屏蔽应用层的非法用户请求，同时可以定义用户的并发请求数；在应用服务器层对用户的输入数据合法性、安全性、完整性进行校验；二期安全加固方案主要针对数据完整性、保密性和防止SQL注入进行了重新设计。OMS安全总体架构如图6所示。

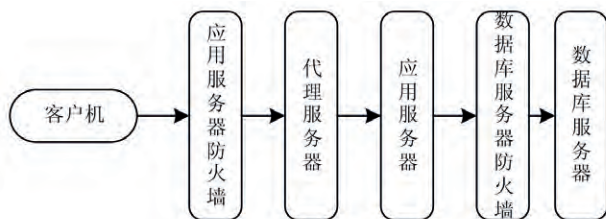


图6 OMS安全总体架构

3.1 数据完整性、保密性设计

系统采用了基于数字证书的SSL双向认证方式对传输内容进行加密。相比于单向认证，双向认证增加了客户端认证的流程，其核心思想就是私用密钥签名，证明证书的确为客户端所有，而中间人无法得知客户端的私钥，有效防止了篡改握手消息的攻击性操作。

数据加密算法：客户端和服务端在传输数据之前，会协商传输过程的加密算法，系统的核心、敏感数据，采用MD5非可逆加密，或DES对称加密方式对数据进行加密处理。

数据完整性校验：系统会根据数据签名的算法不同，采用不同的校验方式，如MD5。

预防重放攻击登陆：每次SSL握手过程中，都会分配一个唯一随机数标记此次握手，有效防止攻击者获取登陆数据后，不经解密直接重传登陆数据包进行攻击的行为。

3.2 防止SQL注入设计

增强OMS数据库抵御恶意攻击能力是OMS安全加固工作的核心内容。为彻底防止SQL注入，OMS设计出三层防注入方案：在代理服务器层，通过Nginx配置文件对注入的可疑URL进行拦截；在应用服务器层，对可疑的SQL注入URL进行拦截；同时可以对表单Post的表单元素数据进行过滤和拦截。

4 结束语

基于云计算的OMS硬件部署方案，引入虚拟化平台将各地市的服务器整合为2套热备冗余的虚拟集群，满足《智能电网调度控制系统调度管理应用（OMS2.0）》要求，增大了系统用户的负载能力。创新设计出基于DM数据库守护进程的灾

备方案，满足了用户不间断提供数据库服务的要求。系统采用了基于数字证书的SSL双向认证方式对传输内容进行加密，综合使用多种防SQL注入手段使系统安全得以加固。综上设计满足了OMS安全加固、提高业务拓展承载力及加强系统可靠性等智能电网调度管理需求。

参考文献

- [1] 塞巴斯塔. Web 程序设计[M]. 北京：清华大学出版社，2011.
- [2] 屈志毅，苏文洲. 一种基于信息分散算法的分布式数据存储方案[J]. 计算机应用，2006，26(5)：1102-1105.
- [3] 黄晓磊，李化. SQL 注入攻击与防御[M]. 北京：清华大学出版社，2010.
- [4] 武仁杰. Web 程序设计[M]. 北京：中国铁道出版社，2009.
- [5] Rescorla E. 崔凯译. SSL 与TLS Designing and Building Secure Systems. 北京：中国电力出版社，2002.
- [6] 康志平，向宏. 特洛伊木马隐藏技术研究及实践[J]. 计算机工程与应用，2006，42(9)：103-105.
- [7] Thimbleby H, Anderson S, Cairns P. A framework for modelling trojans and computer virus infection [J]. Computer Journal, 1998, 41(7): 444-458.

(收稿日期：2015-05-26) EA

作者简介

徐征（1983-）男，硕士，工程师，主要研究方向为电力系统及自动化、调度信息管理。

刘红军（1964-），男，本科，高级工程师，主要研究方向为电力系统及自动化、调度控制管理。