航天测控系统远程数据容灾方案设计与验证

韩伟杰,阎 慧,王 宇
(装备学院 信息装备系,北京 101416)

摘 要:航天测控系统中的重要资产数据对航天任务的成败有重要影响,必须建立数据容灾系统以保障关键数据的安全。分析了当前航天测控系统关键资产数据采用的备份方式及容灾的要求,基于 Oracle 数据库的远程复制功能研究了航天测控系统远程数据容灾技术,设计了航天测控系统远程数据容灾方案,并搭建模拟实验环境对方案进行了实验测试。实验结果表明,容灾方案能够达到第五级的容灾级别,满足可恢复性、可靠性和实时性指标要求,实现对航天测控系统关键资产数据的远程容灾。

关键词:航天测控系统;远程数据容灾;数据库容灾;Oracle DataGuard;Oracle GoldenGate
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2014)02-0136-04
doi:10.3969/j.issn.1673-629X.2014.02.033

Design and Verification of Remote Data Disaster Recovery Plan of Space TT&C System

HAN Wei-jie, YAN Hui, WANG Yu
(Department of Information Equipment, Academy of Equipment, Beijing 101416, China)

Abstract: The critical asset data of the Space TT&C system plays an important role on the space launching missions. Data disaster recovery system must be established to protect the safety of critical data. Analyze the current storage methods and disaster recovery requirements of the data, the remote data disaster recovery method is studied based on the remote replication capability of the Oracle database, and the Space TT&C system remote data disaster recovery plan is designed. The experiment results based on the simulated experimental environment show that the plan can reach the fifth level of the disaster recovery level and satisfy the requirements of the following three performance indicators such as recoverability, reliability and real-time, therefore realizing remote disaster recovery of the critical asset data of the Space TT&C system.

Key words: Space TT&C system; remote data disaster recovery; database disaster recovery; Oracle DataGuard; Oracle GoldenGate

0 引 言

航天测控系统是航天通信、测控和指挥的纽带,其安全性和可靠性直接关系着航天任务的成败[1]。在航天任务执行过程中,会产生一些重要的数据信息,这些信息对于航天发射任务起着决定性作用。如果因为灾难而导致这些关键数据丢失,将会严重影响航天任务的正常执行[2]。

因此,针对航天测控系统的关键业务数据研究远程容灾技术,对于保障航天测控系统的安全可靠具有重要意义。

1 航天测控系统关键数据备份现状及容灾要求

在航天测控系统中,与航天任务相关的技术方案、软件设计开发文档、软件代码产品、软件配置状态以及任务原始数据和处理结果等资料数据都是重要的容灾对象。

目前,各类资料数据的存储管理方式差异性比较大,各类业务数据基本上处于分散管理的状态。

根据航天测控系统对关键资产数据的容灾要求,参照国际上通用的 Share78 标准[3-4],航天测控系统关键数据应达到的容灾等级要求如表 1 所示。

收稿日期:2013-05-02 **修回日期**:2013-08-08 **网络出版时间**:2013-11-29
基金项目:总装备部基金项目(2008SY4108004)
作者简介:韩伟杰(1980-),男,讲师,硕士,CCF 会员,研究方向为信息安全;阎 慧,副教授,博士,研究方向为软件装备;王 宇,副教授,博士,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131129.0857.018.html

表 1　资料数据存储备份现状及容灾要求

序号	数据名称	存储备份现状	容灾等级要求
1	外部输入文件/任务技术方案/任务实施流程/任务故障处理对策	纸制品/磁盘文件	第 5 级 RTO<10 min RPO<5 min
2	软件设计开发文档	配置库管理	
3	软件代码产品	配置库管理	
4	软件配置状态	配置库管理/配置文件/数据库配置	
5	任务原始数据/实时处理结果/事后分析结果	磁盘文件/数据库存储	

2　航天测控系统远程数据容灾方案设计

当前,航天测控系统中的关键资产数据主要采用 Oracle 数据库存储,因此可基于 Oracle 数据库的远程复制技术设计航天测控系统远程数据容灾方案,满足航天测控系统的数据容灾要求。

2.1　基于数据库的远程容灾技术

(1) Oracle DataGuard。

Oracle DataGuard[5-6] 的主要功能是容灾、数据保护、故障恢复等,可分为物理容灾和逻辑容灾两类。二者的最大区别在于,物理容灾应用的是主库的归档日志或在线日志,而逻辑容灾应用的是主库归档或在线日志中提取的 SQL 语句。物理容灾无论是逻辑结构还是物理结构都和主库保持一致,而逻辑容灾只需保证逻辑结构一致,且逻辑容灾在应用 SQL 语句的时候,数据库处于打开的状态,但逻辑容灾方式不支持 LOB 字段。数据的复制通过 Oracle 的日志写入进程或归档进程完成。

(2) Oracle GoldenGate。

GoldenGate[7-8] 是一种基于日志的结构化数据复制软件,它通过解析源数据库在线日志或归档日志获得数据的增删改变化,再将这些变化应用到目标数据库,实现源数据库与目标数据库的同步。GoldenGate 可以在异构的 IT 基础结构之间实现大量的数据亚秒级的实时复制,从而可以在应急系统、数据同步、容灾、数据库升级、双业务中心等多个场景中应用。

2.2　基于数据库的航天测控系统远程数据容灾方案

基于数据库的航天测控系统远程数据容灾方案将数据复制引擎嵌入到生产系统的数据库中,即位于数据库层面,通过数据库管理系统对数据更新操作的交易管理来实现,如图 1 所示。数据库的更新分为两种,即:元数据的更新和用户数据的更新。元数据的更新即数据库结构的改变,如数据库表空间的扩展等;用户数据的更新包括用户数据库表中记录的改变等操作[9]。

在该方案中,基于数据库的数据容灾主要是将生产中心的相关数据库操作目录日志传输到容灾中心,在容灾中心对日志进行相关操作来保证两个中心之间的数据同步。数据库方式由于只是复制归档日志,可在长距离下避免复制联机日志而对生产数据库产生的影响。同时,对磁盘系统和操作系统透明,因此可以直接利用现有设备,无需对现有系统做大的调整。因为要执行数据库监控和复制操作,因此这种容灾方式可能会对系统资源产生一些负载消耗[10]。

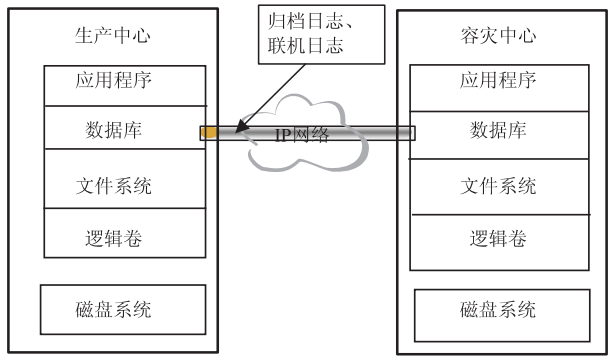

图 1　基于数据库的航天测控系统远程数据容灾方案

3　容灾方案实验验证

为评估以上设计的远程数据容灾方案的性能,搭建模拟的实验环境,分别对基于 Oracle DataGuard 和 Oracle GoldenGate 的容灾方案进行测试。测试主要针对关键容灾性能指标可恢复性、可靠性和实时性进行测试,并评估容灾系统对原系统性能产生的影响。

3.1　测试环境

3.1.1　硬件组成

测试环境主要由以下硬件设备组成:

(1)2 台 Sun Fire V890 服务器(各为 4 CPU);

(2)1 台 Brocade SW200E (16 口) 4 Gb 光纤通道交换机;

(3)2 台操作终端;

(4)两台服务器通过两个千兆以太网口与对方连接。

3.1.2　软件组成

包括的软件有:

(1)2 套 Oracle 10g 数据库软件(自带 DataGuard 工具),配置如下:

源端:IP 为 11.10.10.1;ORACLE_SID = db1

目的端:IP 为 11.10.10.2;ORACLE_SID = db2

(2)1 套 Oracle GoldenGate 软件(需另行安装)。

服务器上安装 Solaris 10 操作系统、Oracle 10g 数据库管理系统,提供数据存储、管理和备份服务。

3.2　实验环境配置

2 台待测服务器上的数据库内容在测试前须保持一致,且主库为归档方式。

3.2.1　Oracle DataGuard 配置

1)源端。

(1)修改源库的初始化参数。

alter system set log_charchiive_config='dg_config=(db1,standby)' scope=both;

alter system set db_unique_name='db' scope=both;

(2)生成目的库的控制文件。

alter database create standby controlfile as'/oracle/rmanback/ctontrl01.ctl';

(3)配置 tnsnames.ora。

```
db1 =
   (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)
(HOST =11.10.10.1)(PORT=1521)))
      (CONNECT_DATA =
         (SERVICE_NAME = db1)))
standby=
   (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)
(HOST =11.10.10.2)(PORT = 1521)))
      (CONNECT_DATA =
      (SERVICE_NAME = db2)))
```

2)备库。

(1)建立参数文件。

其中:

```
fal_server ='db1'
fal_client ='db2'
log_archive_dest_2 ='SERVICE=db1 REOPEN=300'
log_archive_dest_stat_2 ='ENABLE'
```

(2)拷贝控制文件到目的库。

(3)利用拷贝的控制文件,启动目的库成 mount 状态。

(4)配置 tnsnames.ora 与源端相同。

3.2.2 Oracle GoldenGate 配置

源端。

1)配置 mgr 进程。

GGSCI>edit param mgr

输入:PORT 7809

2)增加捕获进程 ext1。

GGSCI>add extract ext1,tranlog,begin now,threads 2

3)配置捕获进程。

GGSCI>edit param ext1

输入

```
extract ext1
userid ggtest,password ggtest
rmthost11.10.10.2, mgrport 7809
rmttrail /ggs
```

3.3 测试输入

实验测试数据包括:

(1)存储在数据库中的软件产品和航天器遥外测数据;

(2)软件代码;

(3)任务装订参数;

(4)技术方案;

(5)航天器原始数据;

(6)航天器处理结果数据。

3.4 测试过程

3.4.1 可恢复性测试

可恢复性测试过程及测试结果如表 2 所示。

表 2 可恢复性测试过程及测试结果

测试内容/方法/步骤	测试结果	
	DataGuard	GoldenGate(需配置双活)
按神舟上升段计划启动仿真、遥测处理、数据入库等进程,10 分钟后关闭主库,并手动实现 redo 日志组切换	备库需要手动打开,存在数据丢失现象,切换延迟<4 分钟	实时切换主备系统,数据不会丢失,切换延迟<1 分钟
按神舟上升段计划启动仿真、遥测处理、数据入库等进程,10 分钟后关闭主库,转运行段 1 小时后重新打开主库,同时停止数据库,并手动实现 redo 日志组切换	可实现完全恢复,恢复时间<4 分钟	可实现完全恢复,恢复时间<1 分钟
备注	由于 DataGuard 主备库需要在 mount 与 open 两种状态之间切换,因此会存在数据丢失的问题,丢失数据量的大小由状态切换的时间决定。同时,由于 DataGuard 的同步机制与 redo 文件组的切换相关,主库写入数据不一定能实时提交,所以在查询时会出现主备库不一致的情况。为防止出现这种情况,测试时手动切换 redo 日志组	

实验结果表明,主备库状态会因为数据量的原因有所不同,但均可实现完全恢复。其中,DataGuard 恢

复时间慢主要因为 redo 文件组的手动切换需要将当前未归档的数据归档。

3.4.2　可靠性测试

可靠性测试过程及测试结果如表 3 所示。

表 3　可靠性测试过程及测试结果

测试内容/方法/步骤	测试结果	
	DataGuard	GoldenGate
按天宫运行段计划启动仿真、遥测处理、数据入库等进程,10 小时后关闭主库,10 小时后切回主库,同时停止数据入库,并手动实现 redo 日志组切换	数据库入库情况正常、切换正常	数据库入库情况正常、切换正常
备注	由于 DataGuard 主备库切换需要在 mount 与 open 两种状态之间切换,所以会存在数据丢失的问题,丢失数据量的大小由状态切换的时间决定	

3.4.3　实时性测试

实时性测试过程及测试结果如表 4 所示。

表 4　实时性测试过程及测试结果

测试内容/方法/步骤	测试结果	
	DataGuard	GoldenGate
启动数据入库进程,发送 100 条遥控指令,并手动实现 redo 日志组切换	备库中可立即查到	备库中可立即查到
启动数据入库进程,发送 10 万条遥测结果数据,每 10 000 条提交一次,并手动实现 redo 日志组切换	备库 2 分 50 秒后可全部查到 备库 2 分 46 秒后可全部查到 备库 2 分 48 秒后可全部查到	备库 10 秒后可全部查到 备库 9 秒后可全部查到 备库 11 秒后可全部查到
启动数据入库进程,发送 50 万条遥测结果数据,每 10 000 条提交一次,并手动实现 redo 日志组切换	备库 3 分 47 秒后可全部查到 备库 3 分 49 秒后可全部查到 备库 3 分 52 秒后可全部查到	备库 11 秒后可全部查到 备库 10 秒后可全部查到 备库 11 秒后可全部查到
备注	备库处于 mount 状态,需要切换到 open 状态,中间过程消耗一些时间	

3.5　容灾系统对原系统性能影响的测试

该测试主要评估容灾系统部署后对原系统的影响,测试指标包括:网络带宽、I/O 吞吐量及 CPU 利用率等,测试内容及测试结果如表 5 所示。

表 5　容灾系统对原系统性能影响测试

测试内容 (使用容灾系统对原系统的影响)	使用前 (峰值)	测试结果	
		DataGuard(峰值)	GoldenGate(峰值)
网络带宽	1 000 M	1 004 M	1 002 M
I/O 吞吐量(主备库建表,含 1 个 timstamp 字段,999 个 float 字段,写入 10 万条,记录写入时间(重复 5 次))	2 分 45 秒 63	2 分 46 秒 52	2 分 47 秒 21
	2 分 48 秒 02	2 分 47 秒 10	2 分 45 秒 34
	2 分 47 秒 12	2 分 48 秒 23	2 分 46 秒 23
	2 分 46 秒 56	2 分 45 秒 76	2 分 48 秒 12
	2 分 47 秒 33	2 分 46 秒 23	2 分 47 秒 63
CPU 利用率(执行启动仿真、遥测处理、数据入库等操作(重复 5 次))	35.8%	36.1%	38.8%
	34.2%	37.3%	39.2%
	37.5%	34.3%	39.9%
	36.8%	35.7%	40.2%
	34.9%	35.2%	38.9%

因为 GoldenGate 运行时为系统进程,DataGuard 为 Oracle 进程,所以 GoldenGate 比 DataGuard 要多占用 5% ~7% 的 CPU(单 CPU 情况下)。网络带宽由于复制机制的不同,DataGuard 存在间歇性带宽占用增大的现象。

3.6　测试结果分析

实验结果表明,利用 DataGuard 和 GoldenGate 均可满足关键数据容灾能力 RTO<10 min、RPO<5 min 的要求,可达到第 5 级的容灾标准。其中,GoldenGate 在带宽占用、实时数据同步及备库状态等方面相比 DataGuard 具有优势,如果不考虑价格因素(DataGuard 内置在 Oracle 中免费使用,GoldenGate 作为可选组件,价格昂贵),GoldenGate 是更好的选择。

(下转第 144 页)

(2)录入者角色:数据库 db_datawriter 权限,除查询和统计外,还可对数据进行添加、修改及删除操作。

(3)管理员角色:dbcreaters 或 sysadmin 权限,除上述两项权利外,还可对数据进行备份、恢复,增加、删除操作人员,为操作人员设置、更改口令等系统管理操作,并且能够创建系统数据库。

软件运行时会出现一个登录窗口,在此输入操作员的名称及口令,若操作员合法且口令正确则进入软件主窗体,主窗体上的菜单根据操作员的角色而不同。

b)进行数据保密性测试。

打开存储密码的文件 MIMA. dat,密码不是显示明文,而是经过加密保存。对 MIMA. dat 文件中的密码内容删除后,输入明文密码,将文件保存,并以明文密码登录,数据库系统提示密码错误。

4 结束语

文中对数据库系统安全性测试技术进行具体分析和研究,将数据库安全性测试分为数据完整性测试、健壮性及防范攻击性测试、备份与恢复测试、安全性访问控制测试,并分别介绍四个测试项在某政务信息系统中的应用,为数据库安全性测试提供了策略和依据。

参考文献:

[1] 郑雷雷,宋丽华,郭 锐,等. B/S 架构软件的安全性测试研究[J]. 计算机技术与发展,2012,22(1):211-224.

[2] 张 岩. 数据库安全性测试研究[J]. 计算机安全,2012(11):33-36.

[3] 周伟明. 软件测试实践[M]. 北京:电子工业出版社,2008.

[4] 何 鑫,郑 军,刘 畅. 软件安全性测试研究综述[J]. 计算机测量与控制,2011,19(3):493-496.

[5] 魏祖宽. 数据库系统及应用[M]. 北京:电子工业出版社,2008.

[6] 贺 红,徐宝文,袁胜忠. 对应用软件进行安全测试的对手模式及其应用[J]. 计算机科学,2006,33(9):266-269.

[7] 张 敏,徐 霞,冯登国. 数据库安全[M]. 北京:科学出版社,2005.

[8] 王爱平. 软件测试[M]. 北京:清华大学出版社,2008.

[9] Huang Y W,Huang S K,Lin T P,et al. Web application security assessment by fault injection and behavior monitoring[C]//Proceedings of the twelfth international world wide web conference. Budapest,Hungary:[s. n.],2003:21-25.

[10] 施寅生,邓世伟,谷天阳. Web 服务安全性测试技术研究[J]. 计算机工程与科学,2007,29(10):11-13.

[11] Microsoft Developer Network. The trustworthy computing security development lifecycle[EB/OL]. 2005-05-23. http://msdn. microsoft. com/en-au/library/ms995349. aspx.

[12] Wikipedia. Software testing[EB/OL]. 2008-11-28. http://en. wikipedia. org/wiki/Software_testing.

[13] 荀 珂. 数据库系统安全性浅析[J]. 电脑知识与技术,2011,7(18):4286-4288.

(上接第 139 页)

4 结束语

针对航天测控系统关键数据存储备份的现状,研究了远程数据容灾技术,并基于 Oracle 数据库的远程数据复制技术设计了容灾方案。为验证容灾方案的有效性,搭建了实验验证环境。实验测试结果表明,设计的容灾方案可以实现 RTO<10 min 及 RPO<5 min 的容灾能力,达到第 5 级的容灾要求。在未来的工作中,将进一步评估航天测控系统数据容灾的可行性,建设航天测控数据容灾系统,实现对航天测控关键数据的持续数据保护[11-12]。

参考文献:

[1] 于志坚. 我国航天测控系统的现状与发展[J]. 中国工程科学,2006,8(10):42-46.

[2] 黄瑜华,周 彬. 容灾技术在军事航天指控中心设计中的应用[J]. 测控技术,2007,26(6):23-24.

[3] Fallara P. Disaster recovery planning[J]. IEEE potentials,2004,22(5):42-44.

[4] Damoulakis J. Continuousprotections[J]. Storage,2004,3(4):33-39.

[5] 蒋秀凤,何凤英. Oracle 9i 数据库管理教程[M]. 北京:清华大学出版社,2005.

[6] 王 靖,刘丽洁. Oracle DataGuard 容灾监控方案探讨[J]. 信息通信,2012(6):201-203.

[7] 徐西波. Oracle GoldenGate 技术在港口的应用浅介[J]. 山东通信技术,2012(3):42-47.

[8] 张云帆. Oracle 数据库备份与恢复策略[J]. 计算机工程,2009,35(15):85-87.

[9] 李 峰,刘晓洁,林翰翮. 基于 Oracle 数据库的容灾系统[J]. 计算机工程与设计,2011,32(11):3573-3577.

[10] 厉 剑,廉国斌,黄 栋. 数据容灾系统与 CDP 技术[J]. 计算机技术与发展,2009,19(1):168-171.

[11] 叶嘉酩,胡晓勤,王 喆. 多数据库容灾系统的设计与实现[J]. 计算机工程与设计,2012,33(12):4541-4545.

[12] Han Hoonglin, Li Lin,Zhu Dehai. Research and implementation on remote disaster recovery system[C]//Proceedings of 2012 international conference on computer science and service system. [s. l.]:IEEE Press,2012:875-879.

航天测控系统远程数据容灾方案设计与验证

作者： 韩伟杰， 阎慧， 王宇， HAN Wei-jie， YAN Hui， WANG Yu
作者单位： 装备学院 信息装备系,北京,101416

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(2)