IT 巡检工具方法

目　　录

1. 概述

1.1 范围定义

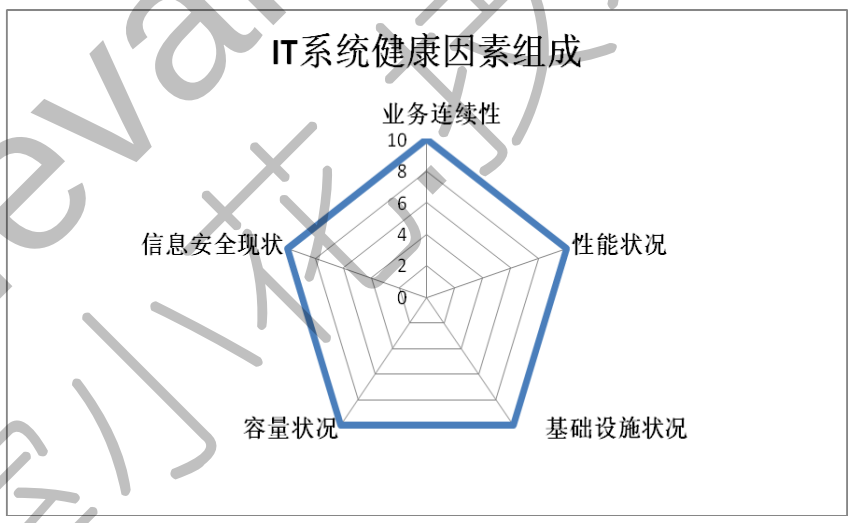
对 IT 系统巡检的逻辑组成，通过对范围定义的与 IT 系统相关的维度的评估，定位当前 IT 系统的健康状况，指导建立改进方案与方针。

1.2 内容说明

对 IT 系统巡检的具体评估指标，用于支持对范围所定义的维度评估结论，提供具体的数据支持；用于给客户提供巡检类报告的数据提供数据支持。

2. 巡检维度

对 IT 系统巡检的评估维度主要包括以下五个方面：



一个完备的 IT 系统建设应该包括上述所有相关解决方案，而客户应用系统中在这几方面体现了不同的完备程度。由于用户行业与业务特点，对这些范围的侧重程度不同，因此我们在评估特定行业用户的 IT 系统之初，要充分考虑这种行业因素，所得出的结论也是对特点行业用户有指导意义的评估结果。

2.1 基础设施状况

IT 基础设施包括系统软件平台和硬件基础设平台。

系统软件平台主要包括操作系统、数据库、中间件。

硬件基础设平台主要包括网络通讯平台和服务器系统平台以及存储系统平台。

对基础设施状况的评估内容包括：

- ✧ IT 系统运维环境状况
- ✧ IT 系统硬件运行状况
- ✧ IT 系统软件平台运行状况
- ✧ IT 系统链路状况

2.2 容量状况

由于 IT 系统的业务和服务需求可能每天都在发生变化,信息系统有时会遇到带宽和存储能力不足的问题。要与 IT 系统当前和将来的业务需求相符意味着必须经常地测定容量。容量规划是一种性能价格比很高的手段，可以根据以往的性能统计数字预知潜在的资源短缺情况。

正确的对当前 IT 系统的容量状况做出评估,是掌握和预测系统当前和未来可用程度的一个重要标志之一，进而也以此为依据做出合理的容量规划。

对容量状况的评估主要包括：

- ✧ 网络带宽负载状况
- ✧ 存储的容量状况

✧ 主机系统负载情况

✧ 业务系统所能承载的吞吐量

软件平台参数配置适用度。

2.3 性能状况

IT 系统所提供的业务的性能，是当前业界评价 IT 系统实施成功与否的主要标准之一。

通常对 IT 系统性能状况评估的对象为具体的业务功能模块,但并不是针对所有的业务功能模块，对这些模块的选取一般遵循以下原则：

✧ 系统日常运行中，使用频率高的功能模块；

✧ 系统日常运行中，业务容易产生相对大并发量的功能模块；

✧ 涉及到的大数据量表操作的功能模块；

✧ 用户反映性能问题突出的模块。

通过选取具有代表性的功能模块，进行性能评测，得出当前系统的性能状况，而这种巡检的环境需要接近真实环境才具有说服力。而本 IT 系统预防性巡检活动通常是在真实的生产环境下完成，因此需要采取适合现场环境的性能评估手段来完成。

对 IT 业务系统的性能评估主要包括以下三个方面：

✧ 业务系统的响应性能状况

✧ 业务系统的稳定性性能状况

✧ 业务容量性能状况

业务系统的响应性能指的是在正常业务并发负载下，以响应时间为主要关注点

的业务模块操作的执行时间，通常单位为秒；

业务系统的稳定性性能的主要关注点则是在长时间较大负载压力下，业务系统能够正常完成业务操作的程度；

业务容量性能状况指的是当前业务系统负载承受能力，目的是了解系统的业务压力可承受的范围，以便在峰值到来之前做出应对措施，通常关注的性能指标为并发量和业务的吞吐量。

2.4 信息安全

这里把信息安全定义为信息系统数据不会被非法用户在未经授权的情况下取得或破坏。信息安全所涉及的技术与业务层面很广，以下是对其简要分类：

1.物理安全

保护信息系统的机房环境、设备、设施、媒体和信息免遭自然灾害、环境事故、人为物理操作失误、各种以物理手段进行的违法犯罪行为导致的破坏、丢失。

2.网络系统安全

网络防护安全是数中心据安全的重要组成部分。网络安全模式要求数据中心首先分析自己的网络系统，并从中找出不同业务、数据和安全策略的分界线，在这些分界线上构建 IT 系统安全等级不同的安全域。

在安全域划分的基础上，通过采用入侵检测、漏洞扫描、病毒防治、防火墙、网络隔离、安全虚拟专网（VPN）等成熟技术，利用物理环境保护、边界保护、系统加固、节点数据保护、数据传输保护等手段，通过对网络和系统安全防护的统一设计和统一配置，实现 IT 系统全系统高效、可靠的网络安全防护。

3.操作系统安全

操作系统提供若干种基本的机制和能力来支持信息系统和应用程序安全，如身份鉴别、访问控制、审计等等。目前主流的商用操作系统主要有 UNIX、LINUX 和 Windows 平台。由于商用的普遍性特点，这些系统都存在许多安全弱点，甚至包括结构上的安全隐患，比如超级管理员/系统管理员的不受控制的权限、缓冲区溢出攻击、病毒感染等。

操作系统的安全是上层应用安全的基础。提高操作系统本身的安全等级尤为关键，除了及时打 Patch 外，还要采用如下的加强措施：

- ✧ 身份鉴别机制：实施强认证方法，比如口令、数字证书等；
- ✧ 访问控制机制：实施细粒度的用户访问控制、细化访问权限等；
- ✧ 数据保密性：对关键信息、数据要严加保密；
- ✧ 完整性：防止数据系统被恶意代码比如病毒破坏，对关键信息进行数字签名技术保护；

✧ 系统的可用性：不能访问的数据等于不存在，不能工作的业务进程也毫无用处。因此操作系统要加强应对攻击的能力，比如防病毒、防缓冲区溢出攻击等；

✧ 审计：审计是一种有效的保护措施，它可以在一定程度上阻止对信息系统的威胁，并对系统检测、故障恢复方面发挥重要作用。

4.数据库安全

数据库安全性问题应包括两个部分：一、数据库数据的安全。它应能确保当数据库系统 DownTime 时，当数据库数据存储媒体被破坏时以及当数据库用户误操作时，数据库数据信息不至于丢失；二、数据库系统不被非法用户侵入。它应尽可能地堵住潜在的各种漏洞，防止非法用户利用它们侵入数据库系统。

5.数据的传输安全

为保证业务数据在传输过程的真实可靠，需要有一种机制来验证活动中各方的真实身份。安全认证是维持业务信息传输正常进行的保证，它涉及到安全管理、加密处理、PKI 及认证管理等重要问题。应用安全认证系统采用国际通用的 PKI 技术、X.509 证书标准和 X.500 信息发布标准等技术标准可以安全发放证书，进行安全认证。当然，认证机制还需要法律法规支持。安全认证需要的法律问题包括信用立法、电子签名法、电子交易法、认证管理法律等。

6.应用身份鉴定

由于传统的身份认证多采用静态的用户名/口令身份认证机制，客户端发起认证请求，由服务器端进行认证并响应认证结果。用户名/口令这种身份认证机制的优点是使用简单方便，但是由于没有全面的安全性方面的考虑，所以这种机制

存在诸多的安全隐患。可以采用：双因子认证和CA认证两种解决方案。

7.应用授权管理

权限管理系统是IT系统信息安全基础设施的重要组成部分，是ICDC信息系统授权管理体系的核心。它将授权管理和访问控制决策机制从具体的应用系统中剥离出来，采用基于角色的访问控制（RBAC，Role Based Access Controls）技术，通过分级的、自上而下的权限管理职能的划分和委派，建立统一的特权管理基础设施（PMI，Privilege Management Infrastructure），在统一的授权管理策略的指导下实现分布式的权限管理。

权限管理系统能够按照统一的策略实现层次化的信息资源结构和关系的描述和管理，提供统一的、基于角色和用户组的授权管理，对授权管理和访问控制决策策略进行统一的描述、管理和实施，提供基于属性证书和LDAP的策略和授权信息发布功能，构建高效的决策信息库和决策信息库的更新、同步机制，面向各类应用系统提供统一的访问控制决策计算和决策服务。建立统一的权限管理系统，不仅能够解决面向单独业务系统或软件平台设计的权限管理机制带来的权限定义和划分不统一、各访问控制点安全策略不一致、管理操作冗余、管理复杂等问题，还能够提高授权的可管理性，降低授权管理的复杂度和管理成本，方便应用系统的开发，提高整个系统的安全性和可用性。

8.应用访问控制

访问控制是IT系统安全防范和保护的主要核心策略,它的主要任务是保证信息资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施，也是计算机系统最重要和最基础的安全机制。

根据控制手段和具体目的的不同,数据中心的访问控制技术包括以下几个方面：入网访问控制、网络权限控制、目录级安全控制、属性安全控制等，只有各种安全策略相互配合才能真正起到保护作用。

9.应用审计追踪

IT系统的安全审计提供对用户访问系统过程中所执行操作进行记录的功能，将用户在系统中发生的相关操作（如：系统登陆/退出、系统操作）记录到数据库中，以确保在需要的时候，对用户历史访问系统的操作进行追溯。

通常审计跟踪与日志恢复可结合起来使用，日记恢复处理可以很容易地为审计

跟踪提供审计信息。如果将审计功能与告警功能结合起来，就可以在违反安全规则的事件发生时，或在威胁安全的重要操作进行时，及时向安检员发出告警信息，以便迅速采取相应对策，避免损失扩大。审计记录应包括以下信息：事件发生的时间和地点；引发事件的用户；事件的类型；事件成功与否。

在 IT 系统中，审计可以是独立工作的不相关的组件的集合，也可以是相互关联运作的组件的集合。审计范围包括操作系统和各种应用程序。

10. 安全管理与策略

IT 系统安全管理系统应包括管理策略、管理组织保障、管理法规制度以及管理技术保障等内容。

IT 系统安全是一个动态不断调整的过程，它随着 IT 系统业务应用和基础设施的不断发展而不断改变，例如 IT 系统信息系统各个信息网络、信息安全部件的具体设置规则，包括特定系统（设备）的口令管理策略、特定防火墙的过滤规则、特定认证系统中的认证规则、特定访问控制系统中的主体访问控制表、安全标签等。为了保证 IT 系统信息安全，及时进行安全策略调整是必要。

管理组织保障，实现对人员、系统、安全设备、物理环境和系统运行的安全管理。另外，IT 系统安全策略应遵照相关行业的法律、规定。

管理技术保障是 IT 系统安全运行管理的技术保证。

2.5 业务连续性

连续性是指一个数据中心类应用为了维持其生存，一旦发生突发事件或灾难后，在其所规定的时间内必须恢复关键业务功能的强制性要求，这就需要预先发现可能会影响企业关键业务能力和过程的所有事件，采取相应的预防和处理策略，以保证企业在事件发生时业务不被中断。通过业务连续性计划保证数据中心业务的不间断能力，即在灾难、意外发生的情况下，无论是数据中心组织结构、业务操作和 IT 系统，都可以以适当的备用方式继续业务运作。

严格的说，业务持续计划的建立和实施过程，实际上是涉及数据中心运营，因此也涉及到项目管理的方方面面。通过多年的实践，根据自身实践经验并参照国际灾难恢复协会（DRI）与业务连续性协会（BCI）的标准，总结出业务持续计划的模型，经过长时间的验证，该业务持续计划模型能够给数据中心带来有效及彻底的业务持续管理。

灾难恢复的技术实现和级别

容灾按级别可分为数据容灾和应用容灾两部分：

数据容灾：在异地建立一个数据拷贝，这个拷贝在本地生产系统的“数据系统”出现不可恢复的“物理故障”时，提供可用的数据。

应用容灾：在异地提供一个完整的应用和数据系统拷贝（不一定要求同当量），这个拷贝在本地生产系统出现不可恢复的“物理故障”时，提供即时可用的生产系统。

1.平台安全性

平台完整性解决 ICDC 内部业务平台和接入平台的高可靠性问题。主要包括服务器、存储和网络层面的技术。

平台完整性涉及的技术主要包括：服务器、存储器、及相应网络连接的部件级可靠性技术；平台的集群技术；Application Server 的高可靠技术；数据库的高可靠技术。

2.备份和恢复完整性

备份和恢复完整性实现 IT 系统内部对业务数据平台的保护。包括服务器和存储层相关技术。

备份完整性涉及的技术主要包括基于磁带、光盘等离线介质的备份技术（或称定点拷贝）；以及基于在线存储介质（磁盘）进行的生产数据快照技术。

实现备份完整性目标，首先需要映射业务种类所需要的数据集。即根据容灾备份系统的需求，明确哪些业务状态数据需要备份，事实上，需要提供最完善备份的是稳定的业务状态数据,而处理流程当中的中间临时数据的备份需求较低。

另外，在备份完整性的实施过程中，应该区分备份数据和存档数据。备份数据是为满足容灾备份的要求，具有较短的时效性，备份数据会根据一定的备份频度被反复覆盖。存档数据则按照业务或法规的要求，有较长的时效性，并具有不断累积的特性。

在绝大多数数据中心应用场合，备份是经常性的工作，恢复是十分偶然的操作，因此，恢复往往是难以经过充分巡检、优化的容灾备份技术---这就更加要求恢

复操作具有明确的可预见性。

3.信息完整性

信息完整性实现对业务数据平台的跨 ICDC 生产中心的保护,实现信息完整性技术是将业务连续性扩展到容灾阶段的一个十分关键的步骤。

信息完整性技术将生产中心的业务状态数据完整地复制到备份中心。

实现信息完整性可以采用同步或异步复制技术。

4.处理完整性

处理完整性即对业务支撑系统平台的完整的、跨越生产中心的保护。

实现处理完整性，需要比较复杂的系统集成工作，包括详细的系统设计和规划。目前的大多数关键业务及其关联子业务系统的容灾的级别要求为处理完整性。

实现处理完整性的关键在于以下三个要素：

✧ 对数据平台的保护－远程数据复制技术（即信息完整性）和对业务平台的保护－服务器、数据库等冗余及切换技术以及应用软件切换技术的集成

✧ 对接入平台的保护和切换－外部接口的冗余和切换

✧ 系统的监控和切换

5.业务连续性管理

业务连续性管理是 IT 信息安全政策的宏观管理文件,该规范清楚说明业务连续性计划对于保障信息安全所采取态度、监管责任以及信念。

业务连续性管理规范包含《灾难恢复预案》、《业务连续性计划》等文件。这些规范从宏观层面，涵盖了灾难备份建设所涉及的内容，其目的是要保护信息安全。根据这些规范，建立业务连续性计划、灾难恢复预案，其中主要包括：灾难应急小组的组织架构和人员职责，应急队伍、联络清单及各类应急处理流程，普及教育及人员培训计划和演习计划等，并报主管部门备案。

主管部门要对各单位灾难恢复预案进行全面审核，评估灾难恢复预案的完整性

和可操作性，配合\建立规范的管理制度和操作文档。

定期进行灾难演习与应急培训。

3. 巡检内容

上一节完成了对 IT 系统巡检的关注方面的分析说明,这一节开始介绍具体体现这些关注方面的指标，在实际检查过程中，可以根据客户的需要选取特定的指标参数，作为评估目标系统的数据支持内容。

3.1 系统整体架构

以下内容作为基本 IT 系统信息被首先调查记录，供分析参考使用。

✧ IT 系统架构拓扑图

✧ 网络设备配置

---设备型号，IOS 版本，模块型号和数量,用途

✧ 存储系统配置

---设备型号，IO 带宽，Cache 容量，磁盘数量，接入模式，存储容量，LUN 配置，所属应用

✧ 主机系统配置

---设备型号，CPU 配置（类型，主频，数量），内存容量，网卡配置（数量，速率），内置硬盘配置（数量，容量，Raid），所属应用

✧ 数据库软件

---产品名称，版本号，所属应用

✧ 中间件软件

---产品名称，版本号，JDK 版本，所属应用

✧ 应用系统

---产品名称，版本号，架构平台，系统架构类型

3.2 机房环境

项目	描述	满足标准
机房功能	服务于何种业务系统	N/A
温度	机房温度范围	摄氏 16-25 度
湿度	机房湿度范围	30%-55%
UPS 保护	稳压继电作用，是否部署	存在 UPS 设备，供电时间根据客户实际情况确定
防雷保护	是否存在	是
接地保护	是否存在	是
防静电保护	是否存在	是
地板承重能力	最大承重	800KG/平方米
防火设施	是否存在	是
防鼠设施	是否存在	是
门禁控制	是否存在	是
监视器	是否存在	是
卫生状况	环境清洁	是

以上的条件可以现场观察和询问用户完成。

3.3 网络系统

网络设备

项目	描述	满足标准
设备外观状况	无破损	是
设备状态灯	是否有告警灯闪亮	无
设备运转状况	功能正常	是
带宽利用率	是否在 80%以内	是
CPU 利用率	是否在 80%以内	是

日志系统是否有错误		无
线路冗余	冗余线路的负载能力要能够满足生产系统负载需求。	是
网络系统监控机制	是否存在	是

防火墙

项目	描述	满足标准
部署情况	是否部署在系统中	是
访问控制策略	是否配置	是
在线访问审计	是否配置	是
保护范围	保护哪些设备	N/A
设备外观状况	无破损	是
设备运转状况	功能正常	是

IPS

项目	描述	满足标准
部署情况	是否部署在系统中	是
在线攻击防御	是否配置	是
在线攻击审计	是否配置	是
保护范围	保护哪些设备	N/A
设备外观状况	无破损	是
设备运转状况	功能正常	是

IDS

项目	描述	满足标准
部署情况	是否部署在系统中	是
旁路访问审计	是否配置	是
旁路攻击审计	是否配置	是
保护范围	保护哪些设备	N/A
设备外观状况	无破损	是
设备运转状况	功能正常	是

VPN

项目	描述	满足标准
部署情况	是否部署在系统中	是
安全策略	配置包过滤规则	是
保护范围	保护哪些设备	N/A
设备外观状况	无破损	是
设备运转状况	功能正常	是

3.4 存储系统

项目	描述	满足标准
设备外观状况	无破损	是
设备运转状况	功能正常	是
RAID 级别	根据业务类型和容错需求判断是否适合	是
Hot Spare	是否配置热备盘	是
硬件冗余配置	硬件是否存在单点故障	否
访问控制	是否配置访问控制	是
可用容量		20%以上
数据增长率	评估可用容量的可用时间	N/A
系统日志	是否有严重报错	无

3.5 主机系统

项目	描述	满足标准
设备外观状况	无破损	是
设备运转状况	功能正常	是
硬件系统日志	是否有严重报错	无
网卡状态	可用	是
IP 地址配置		N/A
路由配置		N/A
网络联通状况	链路是否畅通	N/A
文件系统类型		N/A
分区剩余状况	是否存在即将写满的分区	无

分区合理性	Swap 分区达到物理内存的 2 倍， VAR 分区是否达到 2GB	是
外存储接入设备	设备型号	N/A
外存储接入设备速率	传输速率	N/A
RAID 级别	根据业务类型和容错需求判断是否适合	是
应用数据部署位置		N/A
CPU 负载情况	利用率小于 85%， 运行队列小于 CPU 个数的 4 倍， 阻塞队列小于运行队列， 交换队列为零， 互斥失速小于 CPU 个数的 250 倍。	是
CPU 配置信息	是否多个 CPU 全部用于处理	是
主要负载进程	是否存在再用系统资源过多的进程	否
内存使用情况	使用率低于 90%， 页面调出不持续增加， 不存在页面扫描活动	是
磁盘 IO 状况	是否存在 IO 热点	否
网络负载	平均利用率低于 80%	是
口令管理	密码复杂程度高， 1. 长度超过 8 个字符。 2. 设置为无意义字符组合。 3. 多类型字符组合。 4. 大小写混合组合。 定期修改，强制口令过期。 限制口令重试次数。	是
系统补丁	更新为最新	是

病毒防范措施	安装病毒防火墙	是
系统日志	不存在验证错误警告	是
主机系统监控机制	是否存在	是

3.6 数据库系统

3.6.1 Oracle 数据库

项目	描述	满足标准
运行状态	功能正常	是
表空间使用率	使用率小于 70%	是
大表数据量	用于分析	N/A
数据量增长率	评估可用容量的可用时间	N/A
数据文件存储类型	N/A	N/A
数据文件部署位置	高速存储设备	是
SGA 配置	是否优化配置	是
PGA 配置	是否优化配置	是
Process 配置	是否优化配置	是
Sessions 配置	是否优化配置	是
数据库模式	是否适合应用	是
串行 IO 配置	是否配置	是
分区表使用	在数据表很大的情况下是否部署	是
并行处理使用	大型数据库系统中是否使用	是
错误日志	没有严重错误	是
集群配置	是否部署	是
SGA 命中率	Buffer Nowait%>=99% Redo NoWait%>=99% Buffer Hit %>90% In-memory Sort %>=99% Library Hit %>95% Soft Parse %>95% Execute to	是

	Parse %>90% Latch Hit %>99% Parse CPU to Parse Elapsd %>90%	
首要事件	无非空闲等待事件	是
Top SQL	通常 SQL 执行在秒级以下	是
锁等待	无锁等待	是
队列等待	无队列等待	是
Checkpoint	Oracle 文件中 scn 是否一致	是
用户口令管理	密码复杂程度高， 1.长度超过 8 个字符。 2.设置为无意义字符组合。 3.多类型字符组合。 4.大小写混合组合。 定期修改，强制口令过期。 限制口令重试次数。	是
用户权限配置	无过多权限	是
重做日志配置	是否有同组镜像	是
日志归档配置	是否归档	N/A
数据库系统监控机制	是否存在	是

3.6.2 DB2 数据库

项目	描述	满足标准
运行状态	功能正常	是
Admin Server	N/A	N/A
Instance	N/A	N/A
数据库管理配置（DBM_CFG）	用于分析	N/A
数据库配置文件(DB_CFG)	用于分析	N/A
DB2 进程状态	是否优化配置	是
内存使用情况	是否优化配置	是

缓冲池数量与容量	是否减少直接 I/O，检查 IBMDEFAULTBP	是
表空间与表空间容器	检查表空间的缓冲池和文件系统，系统表空间、临时表空间、用户表空间	是
集群配置	是否部署	是
缓冲池命中率	(1 - ((buffer pool data physical reads + buffer pool index physical reads) /(buffer pool data logical reads + pool index logical reads))) * 100 %	〉95%
锁等待	无锁等待	是
SQL 执行速度	通常 SQL 执行在秒级以下	是
队列等待	无队列等待	是
用户口令管理	密码复杂程度高， 1. 长度超过 8 个字符。 2. 设置为无意义字符组合。 3. 多类型字符组合。 4. 大小写混合组合。 定期修改，强制口令过期。 限制口令重试次数。	是
用户权限配置	无过多权限	是
日志归档配置	是否归档	N/A
数据备份机制	系统级备份 数据库级实时备份 存储级实时备份	建议使用数据库级或存储级实时备份，如果不能实现则需要在系统级备

		份同时是数据库运行在日志归档模式下
数据库系统监控机制	是否存在	是

3.7 中间件系统

项目	描述	满足标准
运行状态	功能是否正常	是
JVM 配置	是否优化配置	是
执行线程配置	是否优化配置	是
执行队列配置	是否优化配置	是
连接池配置	是否优化配置	是
集群配置	是否部署	是
JVM GC 情况	是否正常	是
中间件错误日志	是否有严重错误	否
中间件监控机制	是否存在	是

3.8 应用系统

项目	描述	满足标准
运行状态	功能正常	是
关键业务执行效率	性能相应时间满足客户需求	是
稳定性状况	满足客户需求	是
可承受的最大负载	最大并发用户负载	N/A
口令管理	密码复杂程度高， 1.长度超过 8 个字符。 2.设置为无意义字符组合。 3.多类型字符组合。 4.大小写混合组合。 定期修改，强制口令过期。 限制口令重试次数。	是

用户访问接入形式	广域网，局域网，专线，VPN	局域网，专线，VPN
数据传输形式	是否加密	是
权限控制机制	分级权限控制是否存在，访问应用中任何资源都需要身份验证为前提。	是
版本控制机制	是否存在	是
应用审计机制	是否存在	是

3.9 备份与恢复系统

备份与恢复系统是 IT 系统中重要的容灾措施，IT 系统应该根据自身业务特点选取以下备份与恢复方案。

1. 备份系统

设备系统备份

部件的冗余

---包括网络设备，主机设备，存储设备内部部件的冗余，保证在设备本身避免单点故障。

设备的冗余

---网络层设备冗余包括交换设备的 HA 和线路冗余，交换设备的 HA 可以实现故障发生时自动切换。

---主机层设备冗余可以采用冷备与热备两种方式，热备即主机集群，实现故障发生时自动切换。

---存储层的设备冗余指阵列间的镜像和异地复制方案。

数据系统备份

系统级归档备份

---一般采用磁带备份方式，备份设备可选取磁带机或磁带库

---制定备份策略，可以按一段时间周期，将完全备份、增量备份和差分备份组合使用制定备份策略。

---系统级归档备份的备份数据与在线生产数据存在备份间隔差异,对数据库数据采用这种备份时应将数据库设置为归档模式，来消除这种差异，保证数据的完整性。

存储级数据备份

---本地镜像

---同城容灾镜像

---异地数据传输，分为同步和异步模式。

应用系统备份

应用系统备份基于网络备份，主机系统备份和数据备份的整合，方案中涉及以下因素：

本地应用系统备份，远程应用系统备份

手动应用切换，自动应用切换

应用系统备份是备份方案中级别最高的备份形式，而其中自动应用切换的远程系统备份方案则是最高级备份方案，保证应用的完整性。

2. 恢复系统

备份系统完成 IT 系统的容灾保证的一般工作,恢复的成功与否是衡量备份方案有效的唯一标志。

备份是多次重复工作，而恢复操作则较少发生，这种情况下，验证备份有效性就尤为重要。通过制定以下策略与措施，保证恢复策略的有效性：

制定恢复应急预案

制定恢复流程

定期进行巡检、培训与演习

4. 巡检方法

对照巡检计划的安排，对主机系统进行硬件、操作系统进行功能及性能检查。
注意：系统中所使用的每台主机都要单独列表检查。

4.1 IBM 主机

巡检对象：XX 系统 XX 服务器(HOSTNAME)

巡检目的：检查 XX 系统 XX 服务器的状态

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	主机物理外观检查	主机系统外观正常，没有明显损坏状态		
2	主机加电检查	主机系统正常启动。		
3	登录测试: 从主控制台(console)及用 telnet 命令远程登录到服务器上	正常登录		
4	主机型号巡检 用#prtconf 命令查看	主机型号符合订货要求		
5	检查 CPU 型号与个数 #lsdev -Cc processor #lsattr -El proc0	CPU 型号与个数符合订货要求		
6	检查内存大小 #lsattr -El mem0	内存大小符合订货要求		
7	检查主机的内置硬盘大小 #lspv hdisk0	显示硬盘大小符合订货要求		
8	光驱巡检 在光驱中放入一张光盘,使用 mount	使用 ls 命令可列出光盘内容		

	/cdrom 命令可将光盘挂接				
9	磁带机巡检 将一盘磁带放入磁带机中,使用 tar cvf /dev/rmt0 <filename>将文件拷入磁带机,并使用 tar xvf /dev/rmt0 将文件写回.	文件应可以正常写入和读出			
10	网卡检测 lsdev -Cc adapter	grep en	网卡数量与订货相符		
11	光纤存储卡检测 lsdev -Cc adapter	grep fcs	光纤存储卡与订货相符		
12	附件设备巡检: 用 lsdev -CH 列示附加设备	显示所有设备符合订货要求			
13	检查主机名称 #hostname	显示正确主机名			
14	检查系统时间 #date	与当前时间一致			
15	检查系统时区 #echo "$TZ"	显示东 8 区			
16	检查主机 IP 地址 #netstat -in	显示正确 IP 地址			
17	检查网络连接状态正常 #ping 133.64.7.254	显示连接状态正常			
18	检查操作系统的版本号 #oslevel	显示正确操作系统版本			
19	检查操作系统补丁是否完整 #instfix -l	grep ML	显示现在的系统补丁号		
20	检查系统是否有硬件故障 #diag	显示无硬件故障			
21	主机断电检查 #shutdown -F	主机系统正常关闭。			
	说明： **检测主机的目的是：** **A.确认系统运行正常；** **B.确认系统配置与设计一致；** **C.确认网络状态正常；** **D.确认操作系统安装状态正常。**				

4.2 IBM HACMP Cluster

巡检对象：XX 项目双机系统

巡检目的：XX 系统双机热备功能正常

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	双机软件安装检查 lslpp -l |grep cluster	软件版本与订货合同相符		
2	双机软件启动检测 #smitty clstart	双机系统正常启动		
3	双机状态巡检 #smitty clstat	双机系统运行状态正常		
4	双机软件停止巡检 #smitty clstop	双机系统正常关闭		
5	模拟主机网卡失效巡检 #ifconfig en0 down	用 netstat -in 命令显示 en0 网卡状态为 down，服务地址转到 en1 上		
6	模拟主机网线失效巡检 将 en0 的网线拔出	用 netstat -in 命令显示服务地址转到 en1 上		
7	模拟备机网卡失效巡检 #ifconfig en0 down	用 netstat -in 命令显示 en0 网卡状态为 down，服务地址转到 en1 上		
8	模拟备机网线失效巡检 将 en0 的网线拔出	用 netstat -in 命令显示服务地址转到 en1 上		
9	模拟主机失效巡检 # cat /etc/hosts > /dev/kmem	主机宕掉，LED 显示 888，在所有服务由备机接管		
10	双机系统接管巡检 #smitty clstop，选择 takeover 选项	主机上的所有服务由备机接管		
11	双机数据库服务巡检 #smitty clstop，选择 takeover 选项	数据库服务在主机上停止，并且在备机上启动		
	说明： **检测主机的目的是：** **A.确认双机系统运行正常；** **B.确认双机系统配置与设计一致；**			

	C.在双机互备状态配置下，以上巡检在每台机器上巡检一遍。

4.3 HP 主机

巡检对象：XX 系统 XX 服务器(HOSTNAME)

巡检目的：检查 XX 系统 XX 服务器的状态

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	检查主机及外设的物理完好性	设备完好，		
2	主机加电检查	主机系统正常启动。		
3	登录测试: 从主控制台(console)或 telnet 命令远程登录到服务器上,进行登录	正常登录		
4	主机型号巡检: 用#model 命令查看	主机型号符合订货要求		
5	CPU 数量巡检: 用 ioscan -fnCprocessor 命令查看	CPU 数量符合订货要求,且状态为 CLAIMED		
6	CPU 主频巡检: echo itick_per_usec/D |adb -k /stand/vmunix /dev/kmem	CPU 主频符合订货要求		
7	内存数量测量: 用 dmesg 命令查看 Memory Information 部分	内存条数量及每条的大小符合订货要求		
8	硬盘容量确认: 用 ioscan -fnCdisk 命令列出所有硬盘设备及光驱,用 diskinfo -v /dev/rdsk/cXtYdZ 命令可查看该硬盘的详细信息及大小.	硬盘数量及容量符合订货要求		

9	光驱巡检: 在 DVD-ROM 中放入一张光盘,使用 mount /dev/dsk/cXtYdZ /cdrom 命令可将光盘 mount 到/cdrom 目录下.	使用 ls 命令可列出光盘内容			
10	磁带机巡检: 将一盘磁带放入磁带机中,使用 tar cvf /dev/rmt/0m <filename>将文件拷入磁带机,并使用 tar xvf /dev/rmt/0m 将文件写回.	文件应可以正常写入和读出			
11	网卡功能巡检： 用 lanscan 命令和 ifconfig 命令查看,并观察网卡指示灯的状态.	显示所有网口信息, ifconfig 命令显示网卡状态为 UP,网卡指示灯状态正确.			
12	HBA 卡巡检: 用 ioscan -funC fc	显示 HBA 卡状态为UP,网卡指示灯状态正确.			
13	其他设备巡检: 系统正常启动后,使用 ioscan -fn 命令查看.	显示所有设备应为 CLAIMED 状态.			
14	检查主机名称: #hostname	显示正确主机名			
15	检查主机 IP 地址: #netstat -in 命令查看网络参数。	显示 ip、netmask、gateway 设置正确。			
16	检查网络连接状态: #ping xxx.xxx.xxx.xxx	显示连接状态正常			
17	检查主机系统的时间 #date	系统的时间为当前时间			
18	检查主机系统的时区 #echo $TZ	系统时区为 eat-8			
19	检查操作系统版本号 #uname -v	显示的版本号正确			
20	检查补丁号 #swlist |grep QPK 软件安装检查: 使用 swlist 命令列出所安装的软件	显示的版本号正确 显示结果包含合同中所定的软件.			
21	检查 down 机情况 #shutdown -y 0	主机系统正常关闭。			

	说明： **检测主机的目的是：** **A.确认系统运行正常；** **B.确认系统配置与设计一致；** **C.确认网络状态正常；** **D.确认操作系统安装状态正常。**

4.4 HP MC/ServiceGuard Cluster

巡检对象：XX 项目双机系统

巡检目的：XX 系统双机热备功能正常

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	双机软件安装检查 #swlist | grep MC	软件版本与订货合同相符		
2	双机软件启动检测 #mcruncl -v	双机系统正常启动		
3	双机状态巡检 #mcviewcl -v	双机系统运行状态正常		
4	双机软件停止巡检 #mchaltcl -v	双机系统正常关闭		
5	模拟主机网卡失效巡检 #ifconfig en0 down	用 netstat -in 命令显示 en0 网卡状态为 down，服务地址转到 en1 上		
6	模拟主机网线失效巡检 将 en0 的网线拔出	用 netstat -in 命令显示服务地址转到 en1 上		
7	模拟备机网卡失效巡检 #ifconfig en0 down	用 netstat -in 命令显示 en0 网卡状态为 down，服务地址转到 en1 上		
8	模拟备机网线失效巡检 将 en0 的网线拔出	用 netstat -in 命令显示服务地址转到 en1 上		
9	模拟主机失效巡检 #/sbin/shutdown -r	主机宕掉，所有服务由备机接管		
10	双机系统接管巡检 #mchaltnode -v	主机上的所有服务由备机接管		

11	双机数据库服务巡检 svrmgr>shutdown immediate 关数据库	数据库服务在主机上停止，并且在备机上启动		
	说明： **检测主机的目的是：** **A.确认双机系统运行正常；** **B.确认双机系统配置与设计一致；** **C.在双机互备状态配置下，以上巡检在每台机器上巡检一遍。**			

4.5 SUN 主机

巡检对象：XX 系统 XX 服务器(HOSTNAME)

巡检目的：检查 XX 系统 XX 服务器的状态

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	主机物理外观检查	主机系统外观正常，没有明显损坏状态		
2	主机加电检查	主机系统正常启动。		
3	登录测试:从主控制台(console)及用 telnet 命令远程登录到服务器上	正常登录		
4	项目中中规划的主机名字: hostname	输出是:		
5	主机 ID 号巡检 Hostid: hostid	输出是:		
6	主机型号巡检 用# prtconf -vp |grep banner-name:命令查看	主机型号符合订货要求		
7	检查主机的内置硬盘大小 #iostat -En 命令察看，同时没有 hard error 报错.	显示硬盘大小符合订货要求		
8	cpu 数量巡检： 用命令 psrnfo 命令察看	CPU 数量符合订货要求,且状态为 on-line		

9	内存数量测量:用 prtconf |grep Memory 命令查看	内存数量符合订货要求		
10	光驱巡检:在 DVD-ROM 中放入一张光盘,使用 mount /dev/dsk/cXtYdZ /cdrom 命令可将光盘 mount 到/cdrom 目录下.	使用 ls 命令可列出光盘内容		
11	磁带极巡检:将一盘磁带放入磁带机中,使用 tar cvf /dev/rmt/0m <filename>将文件拷入磁带机,并使用 tar xvf /dev/rmt/0m 将文件写回.	文件应可以正常写入和读出		
12	网卡状态巡检：用 ifconfig -a 命令查看,并且可以看到网卡的地址和网络掩码.	显示所有网卡信息， ifconfig 命令显示网卡状态为 UP,网卡指示灯状态正确. 网卡的地址和规划中一样		
13	网卡是以何种数率运行的：使用 ndd /dev/hme link_speed 来查看；1 代表 100M,而要是 0 就代表 10M.	显示所有的网口的运行数率的信息是否和规划中相符		
14	检查网络情况 $netstat -nr	可以看到正确的路由和网络地址		
15	主机系统中其它硬件各模块是否正常:系统正常启动后,使用 prtdiag -v 命令查看.	显示所有设备应为 ok 状态		
16	软件安装检查:使用 pkginfo 命令列出所安装的软件	显示结果包含合同中所定的软件.		
17	察看系统的补丁的级别 $uname -a	确认是当前比较新的。		
18	系统当前时间、时区 $date	系统当前的时间		
19	察看当前的系统 $uname -s	输出是 SunOS		
20	察看系统当前的 OBP 版本：prtdiag -v |grep OBP	输出系统的 OBP 的版本		
21	察看系统是 64bit 还是 32bit:isainfo -kv	确认当前系统是 64 位的		
22	主机断电检查 #poweroff	主机系统正常关闭。		

	说明： **检测主机的目的是：** **A.确认系统运行正常；** **B.确认系统配置与设计一致；** **C.确认网络状态正常；** **D.确认操作系统安装状态正常。**

4.6 VCS Cluster

巡检对象：XX 系统 XX 服务器(HOSTNAME)

巡检目的：检查 XX 系统 XX 服务器的状态

巡检平台：XX 系统主机，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	双机软件安装检查 #pkginfo | grep VRTS	软件版本与订货合同相符		
2	双机软件启动检测 #hastart -v	双机系统正常启动		
3	双机状态巡检 #hastatus -v	双机系统运行状态正常		
4	双机软件停止巡检 #hastop -v	双机系统正常关闭		
5	主机 Online 测试过程 进入 VCS 的图形界面，选中 hbgsmjf 服务组，点击右键菜单中的 Online 选项，看主机的 Online 过程是否进行正常	正常		
6	主机Offline测试过程 进入VCS的图形界面，选中hbgsmjf服务组，点击右键菜单中的Offline选项，看主机的Offline过程是否进行正常；	正常		

	另，若将处于Online的hbgsmjf服务组offline掉的话，另外一台主机需要手动Online				
7	主机Switch切换过程 进入VCS的图形界面，选中hbgsmjf服务组，点击右键菜单中的Switch选项，看主机的Switch切换过程是否进行正常	正常			
8	数据库测试过程 进入VCS的图形界面，shutdown掉当前处于Online状态的主机数据库，看主机是否进行切换； 注意：如果此步操作进行正常，在做完此步操作后，需要点击hbgsmjf服务组的右键菜单中的Clear Auto选项，使失效的主机恢复正常	正常			
9	主机shutdown测试过程 进入VCS的图形界面，reboot当前处于Online状态的主机，看另外一台主机切换过去是否正常	主机宕掉，所有服务由备机接管			
10	**注意：** VCS要求集群中的两台主机同一时刻必须有一台处于不宕机的状态，若两台主机都宕机后，VCS默认情况下不知道让那一台主机HA启动处于Online状态。 若出现两台主机都宕机的情况，需要进行以下步骤： 在xxgsmjf1上键入 #hastop -all -force #hastart -force 再在xxgsmjf2上键入 #hastart -force				
11					

	说明： 检测主机的目的是： A.确认双机系统运行正常； B.确认双机系统配置与设计一致； C.在双机互备状态配置下，以上巡检在每台机器上巡检一遍。

4.7 网络部分

对照巡检计划的安排，对网络设备进行硬件、操作系统进行功能及性能巡检。
注意：系统中所使用的每台网络设备都要单独列表巡检。

4.7.1 XX 网络设备

巡检对象：XX 系统网络设备(NAME)

巡检目的：XX 系统网络设备的系统状态

巡检平台：XX 系统网络设备，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	网络设备外观检查	网络设备外观正常，没有明显损坏状态		
2	网络设备加电检查	网络设备正常启动。		
3	登录测试: 从主控制台(console)及用 telnet 命令远程登录网络设备上	正常登录		
4	检查版本和硬件配置 >show version （**路由器 ios**） >show module（**交换机 catalyst os**）	显示版本和配置同设计相符。		
5	检查 CPU 利用率 >show processes cpu	显示正常的 CPU 使用率。		
6	检查内存利用率 >show processes memory	显示正常的内存使用率。		
7	检查端口状态 >show ip interface brief 检查正在使用的主要端口的状态 >show interface	显示工作的端口为 UP 状态；Interface 没有冲突等错误信息。		

8	用 PING 扩展命令检查本网络设备到其它设备接点的连通性： #ping Target ip_address: 10.255.254.2 Repeat count:1000 Datagram size [100]:1500 **（多个接点按此项扩展）**	显示“!!!!!”，所发包全部成功			
9	查看路由配置 #show ip route	显示正确的路由，指向正确的路由器			
10	**（10-12 条，根据不同路由协议，填写相关的检查要点和命令）** 检查 ospf neighbor >show ip ospf neighbor	显示 ospf neighbor，（ ）个 neighbor			
11	检查 ospf 数据库信息 >show ip ospf database	显示 ospf 链路状态数据库的信息，其中 Link ID 为路由器的 ID。			
12	检查 ospf 路由表信息 >show ip route summary >show ip route ospf	显示 ospf 路由的条数和 ospf 路由表			
13	检查 HSRP 的状态： #show standby	具有高 priority 值的端口处于 active 的状态，低 priority 值的端口处于 standby 状态。			
14	在具有**高** priority 值的网络设备上 reload 重启动 #reload	在具有**低** priority 值的上网络设备 interface 由 standby 状态转换为 active 状态			
15	从用户 PC ping 通过网关访问其它接点地址： ping -s xxx.xxx.xxx.xxx	切换正常，用户设备到其它设备的连接中断之间小于 5s			
16	**（高端交换机，例如 65 系列）**在引擎上 reset 重启动引擎**（交换机引擎 catalyst os）** #(enable)reset	在具有高 priority 值的网络设备 interface 由 standby 状态转换为 active 状态			
17	从用户 PC ping 通过网关访问其它接点地址： ping -s xxx.xxx.xxx.xxx	切换正常，用户设备到其它设备的连接中断之间小于 5s			

	说明： **检测网络设备的目的是：** **A.确认网络设备运行正常；** **B.确认网络设备配置与设计一致；** **C.确认网络状态正常；** **D.确认网络设备安装状态正常。**

4.7.2 XX 网络设备

巡检对象：XX 系统网络设备(NAME)

巡检目的：XX 系统网络设备的系统状态

巡检平台：XX 系统网络设备，超级用户

前提条件：线路通畅

序号	巡检步骤	正确结果	巡检结果	
			是	否
1	网络设备外观检查	网络设备外观正常，没有明显损坏状态		
2	网络设备加电检查	网络设备正常启动。		
3	登录测试: 从主控制台(console)及用 telnet 命令远程登录网络设备上	正常登录		
4	检查版本和硬件配置 >show version （**路由器 ios**） >show module（**交换机 catalyst os**）	显示版本和配置同设计相符。		
5	检查 CPU 利用率 >show processes cpu	显示正常的 CPU 使用率。		
6	检查内存利用率 >show processes memory	显示正常的内存使用率。		
7	检查端口状态 >show ip interface brief 检查正在使用的主要端口的状态 >show interface	显示工作的端口为 UP 状态；Interface 没有冲突等错误信息。		

8	用 PING 扩展命令检查本网络设备到其它设备接点的连通性： #ping Target ip_address: 10.255.254.2 Repeat count:1000 Datagram size [100]:1500 **（多个接点按此项扩展）**	显示“!!!!!”，所发包全部成功			
9	查看路由配置 #show ip route	显示正确的路由，指向正确的路由器			
10	**（10-12 条，根据不同路由协议，填写相关的检查要点和命令）** 检查 ospf neighbor >show ip ospf neighbor	显示 ospf neighbor，（ ）个 neighbor			
11	检查 ospf 数据库信息 >show ip ospf database	显示 ospf 链路状态数据库的信息，其中 Link ID 为路由器的 ID。			
12	检查 ospf 路由表信息 >show ip route summary >show ip route ospf	显示 ospf 路由的条数和 ospf 路由表			
13	检查 HSRP 的状态： #show standby	具有高 priority 值的端口处于 active 的状态，低 priority 值的端口处于 standby 状态。			
14	在具有**高** priority 值的网络设备上 reload 重启动 #reload	在具有**低** priority 值的上网络设备 interface 由 standby 状态转换为 active 状态			
15	从用户 PC ping 通过网关访问其它接点地址： ping -s xxx.xxx.xxx.xxx	切换正常，用户设备到其它设备的连接中断之间小于 5s			
16	**（高端交换机，例如 65 系列）**在引擎上 reset 重启动引擎**（交换机引擎 catalyst os）** #(enable)reset	在具有高 priority 值的网络设备 interface 由 standby 状态转换为 active 状态			
17	从用户 PC ping 通过网关访问其它接点地址： ping -s xxx.xxx.xxx.xxx	切换正常，用户设备到其它设备的连接中断之间小于 5s			

	说明： 检测网络设备的目的是： A.确认网络设备运行正常； B.确认网络设备配置与设计一致； C.确认网络状态正常； D.确认网络设备安装状态正常。

5. FAQ

5.1 机房环境

对机房的基础设施配备应该按照标准实施，不符合标准的项目应该尽可能整改，添加应有设施。对 UPS 的维护应该定期进行检测，巡检其供电的有效时间，一旦发现电池老化应尽快更换。

5.2 网络系统

网络设备

问题描述	解决方法
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修
带宽利用率过高	检测网络数据流状态，判断是否存在病毒、网络攻击以及设计不合理的应用造成的原因，排除上述因素后考虑升级网络交换设备。
CPU 利用率过高	检测网络数据流状态，判断是否存在病毒、网络攻击以及设计不合理的应用造成的原因，排除上述因素后考虑升级网络交换设备。
不存在网络系统监控机制	建议部署相关产品

Cisco 系统的一些巡检常用命令列表：

总体的信息收集 show tech

查看 ios 版本等信息 show version

查看 log　　show log

查看设备的时钟　　show clock

查看接口状态　　show ip int bri

查看设备路由情况　show ip route

查看 ios 软件包　　show flash (或 show bootflash　/show disk0)

防火墙

问题描述	解决方法
未部署防火墙	建议部署
未配置访问控制	建议配置
未配置在线访问审计	建议配置
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修

IPS

问题描述	解决方法
未部署 IPS	建议部署
是否配置在线攻击防御	建议配置
是否配置在线攻击审计	建议配置
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修

IDS

问题描述	解决方法
未部署 IDS	建议部署
是否配置旁路访问审计	建议配置
是否配置旁路攻击审计	建议配置
设备外观状况存在破损	检测设备可用性，一旦发现功能

	问题及时更换维修
设备运转存在功能问题	更换维修

VPN

问题描述	解决方法
未部署 VPN	建议部署
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修

5.3 存储系统

问题描述	解决方法
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修
RAID 级别不适合应用系统需求	结合业务系统存储需求，在存储资源丰富并且对速度和容错要求较高的需求，建议配置 RAID1 或者 RAID1+0； 在存储资源紧张并且对容错要求较高的需求，建议配置 RAID5； 在存储资源紧张并且对容错需求不大，比较注重速度的需求，建议配置 RAID0。
没有配置 HOT Spare	在存储资源允许的条件下，建议配置 HOTSpare 热备盘。
硬件存在单点故障	在条件允许的情况下，建议实现硬件模块全冗余。
未配置访问控制	建议配置访问控制机制，限制不同主机对数据资源的访问权限。可以采用存储设备自身的访问控制机制，也可以使用 SAN 交换设备的区域划分功能。
可用容量过低	可选方案：

	1. 扩充存储设备； 2. 陈旧数据转移到二级存储或者归档。
系统日志错误	1. 查看设备手册相应的错误代码； 2. 寻求设备厂商支持

Sun T3 阵列的常用命令列表：

系统状态 sys stat

系统配置 sys list

系统部件状态 fru stat

系统部件列表 fru list

卷的列表和状态 vol list，vol stat

SUN StorEdge 3000 系列阵列 cli 命令列表：

显示阵列全部配置 show configuration

查看设备网络状态 show network-parameters

组件状态命令 show battery-status

show enclosure-status

show frus

查看磁盘信息 show disks

查看逻辑设备卷等 show logical-drives

show luns

查看分区状态	show lun-maps
	show partitions
	show logical-volumes
显示 firmware 版本	show ses-devices
	show deses-devices

5.4 主机系统

问题描述	解决方法
设备外观状况存在破损	检测设备可用性，一旦发现功能问题及时更换维修
设备运转存在功能问题	更换维修
系统硬件日志存在错误或警告日志	1.查看设备手册相应的错误代码； 2.寻求设备厂商支持
网卡状态不可用	1. 驱动未加载，参照网卡设备驱动说明加载 2. 网卡设备配置文件未正确配置 3. 网卡设备硬件故障，使用替代方法确认，如果 PING 自身地址正常，可以排除硬件和驱动
网卡链路状态不通	1. 检查网卡状态是否可用，使用 ping 自身地址的方式，如果不正常，则根据网卡状态不可用的解决方法分析解决 2. 检查外部网络是否连通正常，包括网线连接，交换设备状态，防火墙等网络设备状态 3. 自身 IP 配置是否正确，包括掩码 4. 自身静态路由设置是否正确

	5. 检查是否存在 IP 冲突
存在即将写满的分区	1. 清理数据，删除无用数据，归档陈旧数据 2. 扩充分区 3. 移植数据到较大分区 4. 重新定向主要数据量增长文件的输出路径到较大分区 5. 使用文件或目录连接的方法解决
Swap 分区较小不满足需要	1. 对 swap 可以动态增加文件作为 swap 容量 2. 配置新的 swap 分区，将原有的 swap 路径定义为新的 swap 设备路径
RAID 级别不适合应用系统需求	结合业务系统存储需求，在存储资源丰富并且对速度和容错要求较高的需求，建议配置 RAID1 或者 RAID1+0； 在存储资源紧张并且对容错要求较高的需求，建议配置 RAID5； 在存储资源紧张并且对容错需求不大，比较注重速度的需求，建议配置 RAID0。
CPU 负载情况 利用率大于 85%， 运行队列大于 CPU 个数的 4 倍， 阻塞队列大于运行队列， 互斥失速大于 CPU 个数的 250 倍。	1. 检查负载产生的主要进程或应用来源，进行处理或优化 2. 运行队列大于 CPU 个数的 4 倍表明 CPU 数量不满足处理能力需要 3. 阻塞队列大于运行队列需要重点检查优化高 IO 应用系统的性能问题，例如数据库系统 4. 互斥失速大于 CPU 个数的 250 倍说明 CPU 的主频处理能力不足
部分 CPU 未参与处理业务	1. 使用 psrinfo 命令查看是否所有 CPU 的配置为在线使用

	2. 使用 psrset 命令查看是否有进程绑定配置
某些进程占用系统资源过高	1. 清除不必要进程 2. 优化进程相关的应用
内存使用情况 使用率高于 90%， 页面调出率持续增加，进程交换数不为零， 存在页面扫描活动	内存不足，增加内存
磁盘 IO 状况存在 IO 热点	1. 分散 IO 到多个存储设备上 2. 优化高 IO 操作相关的应用系统
网络负载平均利用率持续高于 80%	1. 优化相关应用系统 2. 升级网卡接入带宽 3. 增加网卡接入数量，配置网卡负载均衡
口令管理密码复杂程度低	1.长度超过 8 个字符。 2.设置为无意义字符组合。 3.多类型字符组合。 4.大小写混合组合。
口令未定期修改	制定口令定期修改策略，强制口令过期。
未限制口令重试次数	限制口令重试次数，超过次数后自动锁定用户
未及时更新系统补丁	定期更新
没有病毒防范机制	安装病毒防范产品
硬件存在单点故障	在条件允许的情况下，建议实现硬件模块全冗余。
未部署主机集群环境	对需要均衡负载，需要主机设备冗余需求的建议部署主机集群
存在严重错误警告	1. 查看设备手册相应的错误代码； 2. 寻求设备厂商支持
没有主机系统监控机制	建议部署相关监控机制

5.4.1 sun solaris 主机命令

查看系统运行状况设备运行状况 tform/sun4u/sbin/prtdiag -v

查看系统日志	grep WARN /var/adm/messages*
	grep error /adm/messages*
	grep panic /adm/messages*
查看网络状态路由配置	ifconfig -a
	netstat -rn
磁盘和分区使用情况	df -k
	format
disksuit	metastat,metadb
volume manager	vxprint -ht
CPU	psrinfo
	sar 1 10
vmstat	
prstat	
系统补丁	uname -a
进程情况	ps -ef
磁盘 IO 状况有无错误	iostat -En
	iostat -xn 3

5.4.2 IBM AIX 主机命令

查看系统运行状况设备运行状况	prtconf
	lscfg -pvv
查看系统日志	errpt
	errpt -a|more
	errpt -a -j 日志号
查看网络状态路由配置	ifconfig -a
	netstat -rn
磁盘和分区使用情况	df -k
	lsdev -Ccdisk
	lsvg -o
	lsvg -l 磁盘组
	lsps -a
CPU	lsdev -Ccprocessor
系统补丁	
进程情况	ps -ef
磁盘 IO 状况有无错误	iostat -En
	iostat -xn 3

5.4.3 HP-UX 主机命令

查看系统运行状况设备运行状况	
查看系统日志	vi /var/adm/syslog/syslog.log
列出 I/O 卡的相关信息	ioscan -fn
查看网络状态路由配置	lanscan
	netstat -rn
磁盘和分区使用情况	bdf
	vgdisplay -v vgxx
	lvdisplay -v LVxx
	ioscan -funC disk
	pvdisplay -v /dev/dsk/c*t*d*
CPU	
系统 ID OS 版本	uname -a
进程情况	ps -ef
磁盘 IO 状况有无错误	iostat -En

5.5 数据库系统

5.5.1 Oracle 数据库

问题描述	解决方法

表空间使用率大于 70%	扩充表空间
数据文件没有部署在系统中已存在的高速存储设备	移动数据文件到高速存储设备
SGA 配置未默认配置	根据特定条件进行优化配置
PGA 配置未默认配置	根据特定条件进行优化配置
Process 配置未默认配置	根据特定条件进行优化配置
Sessions 配置未默认配置	根据特定条件进行优化配置
数据库模式不适合	对中间件连接池应用使用专有数据库 对连接数要求达到上千时，使用共享数据库
未配置串行 IO	参照相关文档进行配置
未使用分区表	根据业务和数据量需要判断是否部署
存在错误日志	1. 根据经验解决 2. 参考 Oracle Error 手册解决 3. 寻求厂商支持
没有部署数据库集群	对需要均衡负载，需要中间件冗余需求的建议部署数据库集群
SGA 命中率低	1. 调整 SGA 参数配置 2. 在应用代码中配置变量绑定 3. 尽量减少排序操作
非空闲等待事件占大部分 cpu 时间	参考相关文档，优化应用与配置
存在执行效率低的 SQL	1. 优化索引 2. 优化执行计划 3. 优化 SQL 格式 4. 从业务角度进行优化
较多的锁等待	1. 优化表空间或表参数配置 2. 使用变量绑定 3. 分散数据热点，使用分区表
较多的队列等待	1. 优化表空间或表参数配置 2. 分散数据热点，使用分区表
口令管理密码复杂程度低	1. 长度超过 8 个字符。 2. 设置为无意义字符组合。 3. 多类型字符组合。 4. 大小写混合组合。
口令未定期修改	制定口令定期修改策略，强制口令过期。
未限制口令重试次数	限制口令重试次数，超过次数后自动锁定用户
用户权配置过多权限	仅为用户配置必须的权限

没有重做日志镜像	建议做重做日志镜像，每组重做日志中至少一组镜像。
未启动日志归档	对仅存在系统级备分的系统，建议使用日志归档
数据库备份机制	建议使用数据库级或存储级实时备份，如果不能实现则需要在系统级备份同时是数据库运行在日志归档模式下
没有数据库系统监控机制	建议部署相关监控机制

Oracle 命令列表：

数据库 alert 日志信息——检查日志中是否有错误信息提示。

初始化参数 —— show parameter;

检查控制文件状态—— select * from v$controlfile;

检查联机日志文件状态—— select * from v$logfile;

检查数据文件状态—— select * from v$datafile;

检查表空间使用率——

```
select b.file_id "File ID",b.tablespace_name "TabSP_Name",b.bytes/1024/1024 "Size(M)",
(b.bytes-sum(nvl(a.bytes,0))) "Used",sum(nvl(a.bytes,0)) "Free",
sum(nvl(a.bytes,0))/(b.bytes)*100 "Free Per%"
from dba_free_space a,dba_data_files b
where a.file_id=b.file_id
group by b.tablespace_name,b.file_id,b.bytes
order by b.file_id;
```

检查回滚段使用情况－－

```
SELECT  SEGMENT_NAME,OWNER,TABLESPACE_NAME,SEGMENT_ID,FILE_ID,STATUS
FROM DBA_ROLLBACK_SEGS;
```

检查用户状态－－

```
select
username,account_status,default_tablespace,temporary_tablespace,crea
ted from dba_users;
```

是否存在失效对象－－

```
select owner,  object_name,object_type from dba_objects where status =
‘INVALID’;
```

是否有异常等待事例 －－

```
    select event,sum(decode(wait_Time,0,0,1)) "Prev",
     sum(decode(wait_Time,0,1,0)) "Curr",count(*) "Tot"
from v$session_Wait     group by event order by 4;
```

检测连接数情况 －－

```
SELECT status,count(*) "count" FROM v$session GROUP BY status;
```

用户使用情况 －－ 向客户了解使用过程是否有问题。

5.5.2 DB2 数据库

问题描述	解决方法
表空间使用率大于 90%	扩充表空间
数据文件没有部署在系统中已存在的高速存储设备	移动数据文件到高速存储设备
缓冲池配置未默认配置	根据特定条件进行优化配置
锁机制配置未默认配置	根据特定条件进行优化配置

Process 配置未默认配置	根据特定条件进行优化配置
Sessions 配置未默认配置	根据特定条件进行优化配置
存在错误日志	1. 根据经验解决 2. 参考 DB2 手册解决 3. 寻求厂商支持
没有部署数据库集群	对需要均衡负载，需要中间件冗余需求的建议部署数据库集群
缓冲池命中率 (1 - ((buffer pool data physical reads + buffer pool index physical reads) /(buffer pool data logical reads + pool index logical reads))) * 100%〉95%	1. 增加缓冲池大小 2. 调整数据库配置参数 3. 尽量减少排序操作
SortsPerTransaction = (Total Sorts) / (Commit statements attempted + Rollback statements attempted)〉5 PercentSortOverflow = (Sort overflows * 100) / (Total sorts)〉3%	1. 增加 SORTHEAP 2. 添加正确的索引
存在执行效率低的 SQL	1. 优化索引 2. 优化执行计划 3. 优化 SQL 格式 4. 从业务角度进行优化
较多的锁等待	1. 优化表空间或表参数配置 2. 分散数据热点，使用分区表
口令管理密码复杂程度低	1. 长度超过 8 个字符。 2. 设置为无意义字符组合。 3. 多类型字符组合。 4. 大小写混合组合。
口令未定期修改	制定口令定期修改策略，强制口令过期。
未限制口令重试次数	限制口令重试次数，超过次数后自动锁定用户
用户权配置过多权限	仅为用户配置必须的权限
没有重做日志镜像	建议做重做日志镜像

未启动日志归档	对仅存在系统级备分的系统，建议使用日志归档
数据库备份机制	建议使用数据库级或存储级实时备份，如果不能实现则需要在系统级备份同时是数据库运行在日志归档模式下
没有数据库系统监控机制	建议部署相关监控机制

5.6 中间件系统

问题描述	解决方法
JVM 使用默认配置	根据特定条件进行优化配置
执行线程使用默认配置	根据特定条件进行优化配置
执行队列使用默认配置	根据特定条件进行优化配置
连接池使用默认配置	根据特定条件进行优化配置
未部署集群	对需要均衡负载，需要中间件冗余需求的建议部署中间件集群
JVM GC 不正常	1. 检查 JVM 配置是否合理 2. 检查是否有内存泄漏
日志中有严重错误警告	1. 检查环境参数配置 2. 程序代码错误 3. 参考产品文档 4. 寻求厂商支持
没有中间件系统监控机制	建议部署相关监控机制

5.7 应用系统

问题描述	解决方法
主要应用模块响应时间过长	1. 检查系统负载是否过大，如果无法优化则需要硬件升级 2. 优化应用
在长时间运行中不稳定	1. 检查系统参数配置是否合理 2. 对相关模块优化分析 3. 升级硬件配置
没有采用专网接入形式	建议采用专线，VPN 接入
数据传输未加密	建议使用数据加密与数字证书技术

应用中存在权限控制盲点	修改应用，访问应用中任何资源都需要身份验证为前提
不存在版本控制机制	建立版本控制策略
不存在应用备份	按照应用版本进行备份
没有应用审计机制	建议部署相关审计机制，记录各级用户的操作事件。

6. 附录 1 词汇表

列出本巡检方案中专门术语的定义、英文缩写词的原词组和意义、项目组内达成一致意见的专用词汇，同时要求继承全部的先前过程中定义过的词汇。

词汇名称	词汇含义	备注
软件 software	程序、过程、规则以及任何数据系统操作相关的文档编制。	
硬件 hardware	执行计算机活动和计算机指挥的活动的物理设备。计算机系统的物理组件。	
数据库 database	至少由一个文件组成的事实和说明的集合，它完全能满足给定目的。	
主机 host	（1）通信网络中的主计算机或控制计算机。（2）连接到网络的计算机。	
服务器 server	（1）通常在后台（守护程序）运行且由“系统程序控制器”控制的应用程序。（2）在网络上，包含数据或提供网络上的其他计算机访问的设施的计算机。（3）处理协议、队列、路由以及在计算机系统的设备中传送数据所需的其他任务。（4）在“增强的X-Windows”中提供了基本窗口机制，它处理来自客户机的 IPC 连接，多路分解图形请求到屏幕上，并多路复用输入返回到客户机。（5）在 NCS 中，指向一个或更多对象导出一个或更多接口的进程，可以从远程主机调用其过程。	
工作站 workstation	（1）输入/输出设备的配置，操作员在这些设备上工作。（2）一个终端或微型	

	计算机，通常连接至大型机或网络，用户可在它上面执行应用程序。	
客户机 client	（1）分布式文件系统环境中，一个依赖于服务器为其提供程序或程序访问的系统。(2)“增强的 X-Windows”的应用程序。程序可以成为服务器的客户机，但它实际上就是 IPC 路径本身。协议视具有多个打开到服务器的路径的程序为多客户机。（3）“增强的 X-Windows”中，一个使用应用程序中小窗口或用来组成另一个小窗口的工具箱例程。(4) AIXwindows 中，一个在传统客户机/服务器模型（基于“增强的 X-Windows”和 AIXwindows）中担负客户机角色的软件应用程序。(5)NCS 中一个使用借口创建远程调用（RPC）的程序。	
节点 node	（1）连接到网络的计算机。(2) 链路的结束点，或者连接到网络的节点结点，通常是两个或更多。节点可以是处理器、控制器或工作站，他们可以通过路由和其他功能加以区别。(3) 在系统网络体系结构中，硬件组成部分连同相关的软件部分，实现了七层结构的功能（SNA）。(4) 在树结构中的点，下级数据项从它起源。	
模块 module	（1）一个离散的编程单元，通常执行一个特定的任务或任务集。模块是先被单独汇编然后链接成一个完整程序的子例程和调用程序。(2)在汇编语言中，由过程或数据声明组成同其他这样的构造交互的语言构造。(3) 一个封装的功能性硬件单元，设计用来同其他组件一起使用。	
操作系统 Operating system,OS	控制系统如何工作的程序集。控制程序的运行，提供像资源分配、调度、输入和输出控制以及数据管理的服务。	
超级用户 Superuser	能无限制地访问和修改操作系统的任何部分的人，通常是管理系统的用户。	

(root user)		
超级用户权限 Superuser authority (root user authority)	无限制地访问和修改操作系统的任何部分的能力,通常与管理系统的用户关联。	
登陆 Log in Log on	（1）在一个显示站上开始一个会话。（2）通过在工作站上输入标识和认证信息从而获得对一计算机系统的访问的操作。	
内存 memory	（1）可寻址的程序存储器，通过它指令和其他的数据可被直接装入到寄存器以便后续的程序运行和处理。(2)电子芯片上的存储器。存储器的示例有随机存取存储器，只读存储器，或者寄存器。	
磁盘驱动器 Disk drive	用来读写磁盘上信息的设备	
磁盘 disk	一种存储设备，由一个或多个平面、有磁性表面的圆形盘片组成,可以在上面存储信息。	
软盘驱动器 Diskette drive	用来读写软盘上信息的设备。	
硬盘 Fixed disk Hard disk	（1）平面的、圆形的、不可移动的盘，带有磁性表面层,数据可由磁性记录存储在该层上。在硬盘驱动器中使用的硬磁盘。(2)该磁盘术语也宽松地用于工业上的板和盒,他们包含了模拟硬盘操作的微芯片或磁泡存储器。	
CD-ROM	格式为光学读取光盘的高容量只读存储器。	
适配器 adapter	（1）用于连接两个不同部件或机器的机械装置。(2)一印刷电路卡修改系统元件以允许它以特定方式操作。	
网络 network	通过通信线路连接的数据处理产品的集合，用于在不同位置间进行信息交换。	
局域网（LAN）	（1）通信被限制在合适的地理区域（1	

Local Area Network	到 10km）的一个网络，如：作为单一的办公楼、仓库、或者校园。一个本地网络服务于一个设备，不需要利用公共载体通信公司，尽管他们可能利用普通发送来进行相互连接。一个本地网络依赖于一个适合高数据速率的通信介质（每秒 1 到 20M 字节），而且在操作过程中出错率一直很低。（2）在一个数据网络中的一系列传输用来在数据站之间直接数据通信。	
网络适配器 Network adapter	在网络中允许设备与其他设备通信的电路。	
以太网 Ethernet	一种使用 CSMA/CD（带冲突检测的载波侦听多路访问）的 10M 基带局域网。这种网络允许多个站点随意访问网络介质而无需事先协商，它通过使用载波侦听和延迟来避免争用，并使用冲突检测和传输来解决争用。	
网络地址 Network address	（1）表示特定网络的地址的那部分。一个用于网络上的机器的完整地址，由网络地址和主机地址构成。（2）在 NCS 中，网络或因特网中的特定主机的唯一的标示符（在地质系列内）。网络地址足够用来标识主机内的通信端点。	
IP 地址 IP address	网际协议所采用的网络地址。是一个 32 位整数，通常用点分十进制书写，其中每个连续的八进制被转换成整数和由小数点与其他部分分开。	
路由 Route	为在网络上发送数据而定义的一种路径。	
地址解析协议（ARP） Address Resolution Protocol	TCP/IP 提供的协议之一，在局域网里的因特网地址、基带适配器地址、X.25 地址和令牌环适配器地址之间进行动态映射。	
网络协议 Network protocol	OSI 网络结构的网络层通信协议，例如网际协议（IP）	
防火墙 firewall	一个系统或者机器，它控制在外部网络和专用网间的访问。	
备份	可在发生故障或数据丢失时使用的系	

backup	统、设备、文件或设备。	
归档 archive	（1）存储程序和数据以保管。（2）单个或多个文件的副本或数据库副本，保存该副本以备原始数据损坏或丢失。	
恢复 restore	返回到原始值或原始图像；例如，从磁带恢复库。	

备注中注明该词汇的来源，或有其他更详细的解释的文档位置；以及对该词汇的其他叫法。

7. 附录 2 参考资料

本方案同时查阅了以下 Internet 网址上的技术标准及信息。

IBM e-Server p-Series 信息中心：

http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base

IBM Redbooks 网站：

http://www.redbooks.ibm.com

HP 公司网站：

http://www.hp.com

SUN 公司网站：

http://www.sun.com

CISCO 公司网站：

http://www.cisco.com

EMC2 公司网站：

http://www.emc2.com