4 一体化安全服务

4.4 数据安全规范

数据是平台中最重要的信息，应该在平台正常运行时保持数据的副本一致性、副本容忍性、存储安全、传输安全、备份安全、恢复安全、剩余信息保护等，具体规范如下

（1）数据副本一致性

基本要求：应该支持指定数量副本的数据在任意情况下都是一致的，其他副本最终能够完成数据同步。

增强要求：应该支持所有副本的数据在任意情况下都是一致的。

（2）数据副本容忍性

基本要求：

①支持当少于总数据副本数量的50%的数据副本故障时，仍能正常对外提供服务。

②应该支持当大于等于总数据副本数量的50%的数据副本故障时，通过人工干预或其他技术手段，仍能对外提供服务。

③应该支持副本故障容忍数阈值告警，且告警阈值可设置。

④应该支持设定副本故障容忍数阈值，并在副本故障容忍数阈值范围内，发生网络异常或部分节点故障情况时，保证数据不丢失。

⑤应该支持当故障副本数量恢复到可靠性水平后，分布式事务数据库能自动恢复读写服务。

增强要求：无。

（3）数据存储安全

基本要求：

①应该采用加密技术或其他保护措施实现鉴别信息保密性。

②应该根据国家与行业主管部门相关规定加密存储敏感数据。

③应该支持采用密码算法技术对数据表进行加密。

④应该支持采用密码算法的方式对字段进行加密。

⑤应该支持采用密码算法技术对数据库进行整库加密。

增强要求：无。

（4）数据传输安全

基本要求：

①应该采用技术措施保证敏感数据和个人信息传输的保密性。

②应该能够检测到数据在传输过程中完整性是否受到破坏。

增强要求：无。

（5）数据备份安全

基本要求：

①应该支持数据备份的存储位置可选，包括但不限于本地备份、同城容灾中心、异地容灾中心等。

②应该支持采用密码算法技术，保证备份文件、导出文件的数据完整性与保密性。

增强要求：

①支持多重层级数据备份，包括但不限于库级、表级、集群级、用户级等。

②运维接口应该与外部业务接口、内部集群数据接口进行隔离。

（6）数据恢复安全

基本要求：

①数据恢复时，应该保证恢复到备份时刻状态。

②数据恢复时，应该保证恢复到数据全局一致状态。

③应该支持将数据恢复到具备恢复条件时间段内任意时刻的能力。

增强要求：

①应该支持表级别数据快速恢复的能力。

②应该支持库级别数据快速恢复的能力。

（7）剩余信息保护

基本要求：

①应该支持在集群扩缩容和重分布过程中因物理存储介质变更产生的剩余信息进行自动清理。

②应该支持在数据迁移、数据导入导出过程中，对产生的中间数据进行检查和清理。

增强要求：无。

4.5 应用安全规范

从应用的部署要求、身份验证、会话管理、权限管理等方面规范平台的应用安全，具体如下：

（1）部署要求

①如果Web应用对Internet开放，Web服务器应当置于DMZ区，在Web服务器与Internet之间，Web服务器与内网之间应当有防火墙隔离，并设置合理的策略。

②如果Web应用对Internet开放，Web服务器应该部署在其专用的服务器上，应避免将数据库服务器或其它核心应用与Web服务器部署在同一台主机上。

③Web站点的根目录必须安装在非系统卷中。

（2）身份验证

①对用户的最终认证处理过程必须放到应用服务器进行。

②网页上的登录/认证表单必须加入验证码。

③用户名、密码和验证码必须在同一个请求中提交给服务器，必须先判断验证码是否正确，只有当验证码验证通过后才进行用户名和密码的校验，否则直接提示验证码错误。

④所有登录页面的认证处理模块必须统一。

⑤所有针对其他第三方开放接口的认证处理模块必须统一。

⑥认证处理模块必须对提交的参数进行合法性检查。

⑦认证失败后，不能给用户详细以及明确的错误原因，只能给出一般性的提示。

⑧最终用户入口和管理员入口分离。

⑨禁止在系统中预留任何的后门账号或特殊的访问机制。

⑩对于重要的管理事务或重要的交易事务要进行重新认证，以防范会话劫持和跨站请求伪造给用户带来损失。

（3）会话管理

①使用会话cookie维持会话

②会话过程中不允许修改的信息，必须作为会话状态的一部分在服务器端存储和维护。

③当Web应用跟踪到非法会话，则必须记录日志、清除会话并返回到认证界面。

④禁止使用客户端提交的未经审核的信息来给会话信息赋值。

⑤当用户退出时，必须清除该用户的会话信息。

⑥必须设置会话超时机制，在超时过后必须要清除该会话信息。

⑦在服务器端对业务流程进行必要的流程安全控制，保证流程衔接正确，防止关键鉴别步骤被绕过、重复、乱序。

⑧所有登录后才能访问的页面都必须有明显的“注销（或退出）”的按钮或菜单，如果该按钮或菜单被点击，则必须使对应的会话立即失效。

（4）权限管理

①对于每一个需要授权访问的页面或servlet的请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作。

②授权和用户角色数据必须存放在服务器端，不能存放在客户端，鉴权处理也必须在服务器端完成。

③一个账号只能拥有必需的角色和必需的权限，一个组只能拥有必需的角色和必需的权限，一个角色只能拥有必需的权限。

④对于运行应用程序的操作系统账号，不应使用“root”、“administrator”、“supervisor”等特权账号或高级别权限账号，应该尽可能地使用低级别权限的操纵系统账号。

⑤对于应用程序连接数据库服务器的数据库账号，在满足业务需求的前提下，必须使用最低级别权限的数据库账号。

4.6 异常日志规范

本小节从错误码和日志规约两方面对异常日志的记录规范进行约束，具体如下：

（1）错误码

①错误码的制定原则：快速溯源、沟通标准化。错误码必须能够快速知晓错误来源，可快速判断是谁的问题；错误码必须能够进行清晰地比对；错误码有利于团队快速对错误原因达到一致认知。

②错误码为字符串类型，共5位，分成两个部分：错误产生来源+四位数字编号。错误产生来源分为A/B/C，A表示错误来源于用户，比如参数错误，用户安装版本过低，用户支付超时等问题；B表示错误来源于当前系统，往往是业务逻辑出错，或程序健壮性差等问题；C表示错误来源于第三方服务，比如CDN服务出错，消息投递超时等问题；四位数字编号从0001到9999，大类之间的步长间距预留100。

③错误码使用者应避免随意定义新的错误码，尽可能在原有错误码附表中找到语义相同或者相近的错误码在代码中使用即可。

④错误码不能直接输出给用户作为提示信息使用。

（2）日志规约

①应用中不可直接使用日志系统（Log4j、Logback）中的API，而应依赖使用日志框架 （SLF4J、JCL--Jakarta Commons Logging）中的API，使用门面模式的日志框架，有利于维护和各个类的日志处理方式统一。

②所有日志文件至少保存15天，因为有些异常具备以“周”为频次发生的特点。对于当天日志，以“应用名.log”来保存，保存在/home/admin/应用名/logs/目录下，过往日志格式为: {logname}.log.{保存日期}，日期格式：yyyy-MM-dd。

③根据国家法律，网络运行状态、网络安全事件、个人敏感信息操作等相关记录，留存的日志不少于六个月，并且进行网络多机备份。

④应用中的扩展日志（如打点、临时监控、访问日志等）命名方式：appName\_logType\_logName.log。logType:日志类型，如stats/monitor/access等；logName:日志描述。这种命名的好处：通过文件名就可知道日志文件属于什么应用，什么类型，什么目的，也有利于归类查找。

⑤在日志输出时，字符串变量之间的拼接使用占位符的方式。

⑥避免重复打印日志，浪费磁盘空间，务必在日志配置文件中设置additivity=false。

⑦生产环境禁止直接使用System.out 或System.err 输出日志或使用e.printStackTrace()打印异常堆栈。

⑧异常信息应该包括两类信息：案发现场信息和异常堆栈信息。如果不处理，那么通过关键字throws往上抛出。

⑨日志打印时禁止直接用JSON工具将对象转换成String。如果对象里某些get方法被覆写，存在抛出异常的情况，则可能会因为打印日志而影响正常业务流程的执行。

4.7 容灾备份规范

按照信息系统灾难恢复规范的划分标准，将信息系统的灾难恢复能力划分为6级，如过要达到某个灾难恢复能力等级，应同时满足该等级中7个要素的相应要求。每级对应的灾难恢复资源各要素的具体要求如下：

（1）第1级 基本支持

第1级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第1级—基本支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放。 |
| 备用数据处理系统 | 不作要求 |
| 备用网络系统 | 不作要求 |
| 备用基础设施 | 有符合介质存放条件的场地 |
| 专业技术支持能力 | 不作要求 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |

（2）第2级 备用场地支持

第2级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第2级—备用场地支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放。 |
| 备用数据处理系统 | 配备灾难恢复所需的部分数据处理设备，或灾难发生后能在预定时间内调配所需的数据处理设备到备用场地 |
| 备用网络系统 | 配备部分通信线路和相应的网络设备，或灾难发生后能在预定时间内调配所需的通信线路和网络设备到备用场地 |
| 备用基础设施 | a.有符合介质存放条件的场地；  b.有满足信息系统和关键业务功能恢复运作要求的场地。 |
| 专业技术支持能力 | 不作要求 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证；  c.有备用站点管理制度；  d.与相关厂商有符合灾难恢复时间要求的紧急供货协议；  e.与相关运营商有符合灾难恢复时间要求的备用通信线路协议。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |

（3）第3级 电子传输和部分设备支持

第3级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第3级—电子传输和部分设备支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放；  c. 每天多次利用通信网络将关键数据定时批量传送至备用场地。 |
| 备用数据处理系统 | 配备灾难恢复所需的部分数据处理设备 |
| 备用网络系统 | 配备部分通信线路和相应的网络设备 |
| 备用基础设施 | a.有符合介质存放条件的场地；  b.有满足信息系统和关键业务功能恢复运作要求的场地。 |
| 专业技术支持能力 | 在灾难备份中心有专职的计算机机房运行管理人员 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证；  c.有备用计算机机房管理制度；  d.有备用数据处理设备硬件维护管理制度；  e. 有电子传输数据备份系统运行管理制度。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |

（4）第4级 电子传输及完整设备支持

第4级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第4级—电子传输及完整设备支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放；  c. 每天多次利用通信网络将关键数据定时批量传送至备用场地。 |
| 备用数据处理系统 | 配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态 |
| 备用网络系统 | a.配备灾难恢复所需的通信线路；  b.配备灾难恢复所需的网络设备，并处于就绪状态。 |
| 备用基础设施 | a.有符合介质存放条件的场地；  b.有满足信息系统和关键业务功能恢复运作要求的场地；  c. 有满足关键业务功能恢复运作要求的场地；  d. 以上场地应保持 7x24 小时运作。 |
| 专业技术支持能力 | 在灾难备份中心有：  a.7x24 小时专职计算机机房管理人员；  b.专职数据备份技术支持人员；  c.专职硬件、网络技术支持人员。 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证；  c.有备用计算机机房管理制度；  d.有备用数据处理设备硬件维护管理制度；  e. 有电子传输数据备份系统运行管理制度。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |

（5）第5级 实时数据传输及完整设备支持

第5级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第5级—实时数据传输及完整设备支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放；  c. 采用远程数据复制技术，并利用通信网络将关键数据实时复制到备用场地。 |
| 备用数据处理系统 | 配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态 |
| 备用网络系统 | a.配备灾难恢复所需的通信线路；  b.配备灾难恢复所需的网络设备，并处于就绪状态；  c. 具备通信网络自动或集中切换能力。 |
| 备用基础设施 | a.有符合介质存放条件的场地；  b.有满足信息系统和关键业务功能恢复运作要求的场地；  c. 有满足关键业务功能恢复运作要求的场地；  d. 以上场地应保持 7x24 小时运作。 |
| 专业技术支持能力 | 在灾难备份中心有：  a.7x24 小时专职计算机机房管理人员；  b.专职数据备份技术支持人员；  c.专职硬件、网络技术支持人员。 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证；  c.有备用计算机机房管理制度；  d.有备用数据处理设备硬件维护管理制度；  e. 有电子传输数据备份系统运行管理制度。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |

（6）第6级 数据零丢失和远程集群支持

第6级灾难恢复能力应具有技术和管理支持如表X所示。

表X 第6级—数据零丢失和远程集群支持

|  |  |
| --- | --- |
| 要素 | 要求 |
| 数据备份系统 | a.完全数据备份至少每周一次；  b.备份介质场外存放；  c.远程实时备份，实现数据零丢失。 |
| 备用数据处理系统 | a. 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容；  b.应用软件是“集群的”，可实时无缝切换；  c.具备远程集群系统的实时监控和自动切换能力。 |
| 备用网络系统 | a. 配备与主系统相同等级的通信线路和网络设备；  b.备用网络处于运行状态；  c. 最终用户可通过网络同时接入主、备中心。 |
| 备用基础设施 | a.有符合介质存放条件的场地；  b.有满足信息系统和关键业务功能恢复运作要求的场地；  c. 有满足关键业务功能恢复运作要求的场地；  d. 以上场地应保持 7x24 小时运作。 |
| 专业技术支持能力 | 在灾难备份中心有：  a.7x24 小时专职计算机机房管理人员；  b.专职数据备份技术支持人员；  c.专职硬件、网络技术支持人员；  d.专职操作系统、数据库和应用软件技术支持人员。 |
| 运行维护管理能力 | a.有介质存取、验证和转储管理制度；  b.按介质特性对备份数据进行定期的有效性验证；  c.有备用计算机机房管理制度；  d.有硬件和网络运行管理制度；  e.有实时数据备份系统运行管理制度；  f. 有操作系统、数据库和应用软件运行管理制度。 |
| 灾难恢复预案 | 有相应的经过完整测试和演练的灾难恢复预案 |