# 应急保障响应方案

突发重大紧急情况是指平台环境或者业务应用系统遭遇突发事件，已经或者可能将要给用户造成巨大损失或者不良影响的情况。造成这种突发重大事件的原因可能会与中间件产品或中间件关联产品有关，也可能无关，但无论如何都需要中间件厂商立即立刻给予有力的技术支持，帮助用户迅速解决问题。

中间件厂商协助用户应对突发重大紧急情况的任何保障措施策略，都必须保证以最快的速度解决问题、尽可能的减少用户损失，**这是重要的衡量标准。**

金蝶天燕作为中间件厂商，在应对突发重大紧急情况的保障措施，将充分做好事前有预案、事中有应对、事后有总结等各重要阶段的工作。

事前有准备，是在平时正常状况下，要不断设计演练预案，做好技术预防措施，如各项备份工作、备份节点的巡检等同于生产节点、人员预设安排等等工作。

事中有应对，是指一旦发生突发重大事件，首先要储备足够的人力资源、技术资源，能够迅速响应用户的请求；其次要和生态上下游厂商有良好的沟通机制，发挥协同作用。

事后有总结，突发重大紧急情况一般都是事先无法预料的技术或者业务问题、且一般都会在初期有个黄金挽救时间，做好事后总结归档工作，就是为下一次遇到突发状况能够及时有效的挽回损失做好技术储备，有利于下一次遇到突发状况时，可以及时有效的判明问题原因和问题性质，从而为后续技术资源的投入提供方向性的指导。

## 故障应急服务保障的目标

金蝶天燕在此次项目中的所有服务保障将遵循“一切以客户为中心”的总体目标。在客户的运维过程中，无论遇到任何突发重大紧急情况，我们将第一时间给予响应，并根据实际情况以最快的速度做出相应的安排部署，无论问题是由中间件产生的，还是与中间件产品相关的上下游产品所产生的，都是在我们的紧急响应范围之内。

### 保障的目标对象

金蝶天燕在此次项目中的紧急服务保障的对象目标，将分为用户、业务系统、中间件、总体环境等四个维度聚焦紧急重大服务保障的对象目标。

**其中服务保障的目标用户，**将包括此次项目工程范围所覆盖的全部用户单位，以及所有用到金蝶Apusic应用服务器产品的终端用户、集成商、平台运维厂商，以及中间件产品相关联的上下游厂商。

**其中服务保障的目标业务系统，**将涵盖此次项目中所有部署在金蝶Apusic应用服务器产品上的业务系统，以及在此次项目体系中，与金蝶Apusic应用服务器产品有消息往来、应用接口交互、数据及缓存共享的一切外围应用系统及设备，我们都将承担完全的紧急保障服务或者参与到用户方所组织的综合响应技术团队，并积极主动的发挥金蝶天燕在中间件产品方面的技术保障优势，尽可能的协助终端用户完全解决问题。

**其中中间件产品范围，**将包括此次项目中部署的所有金蝶Apusic应用服务器中间件产品。同时，在此次项目实施过程中，如有准备替代，但尚未来得及实施的替代工作中，有涉及到其它国外或者开源中间件产品出现了重大紧急问题，我们也将根据金蝶天燕自身的技术经验，协助客户完成替代过渡期间发生的其它品牌中间件所产生问题。对于部分经现场技术人员研判，实际问题不大的情况下，我们将给出适当的技术建议，以保障客户过渡期平稳为主，而对于部分重要且一时无法解决的问题，并根据情况，适当调整替代工作计划，采取火线替代的策略，直接完成替代工作。

**其中总体环境方面，**金蝶天燕将积极协助上下游厂商，配合友商及时准确的解决问题。

### 服务效果目标

在实际的实施与运维过程中，不管客户遇到何种紧急重大突发情况，最终的服务目标都是，要在最短的时间内，保障客户的业务系统恢复正常，或者保障客户完成他所需要的、紧急的中间件应用需求，例如疫情期间的，如遇到紧急的业务需求，需要紧急上线某业务系统，而其中涉及到中间件的部署、测试、调优工作等等，这是我们制定突发紧急重大事项保障策略的最终服务目标。

同时，在整个信息化综合IT架构体系中，中间件只是其中重要的一个环节，当最终客户遇到重大紧急问题时，金蝶天燕将根据在往期参与的国家重大安可替代项目经验，来分别提供针对性的服务保障措施。如问题与部署于中间件产品之上的业务系统、金蝶Apusic中间件产品自身以及与金蝶Apusic产品强相关的数据库、操作系统等相关，则金蝶天燕将做为主要负责单位，来确保客户问题及时有效的解决；如遇到网络、硬件、存储等相关的问题，金蝶天燕做为协助单位，将及时给到友商合理、有效的的技术建议，尤其是与中间件产品、应用系统等有关的技术建议。

## 故障应急服务保障的原则

在项目中，遇到重大紧急服务保障需求时，将遵循如下的一些保障原则：

* 1. **坚持防范问题优于解决问题的原则。**强化巡检制度，多做预案，重要业务系统做好备份或应急备用节点，尽量避免发生突发重大紧急情况的发生，把问题消于无形；
  2. **坚持以“以业务和用户为中心”的原则。**无论问题涉及到业务系统、中间件、数据库、操作系统及相关软硬件环境，都要以积极主动的态度解决问题；所投入的人力资源、设备资源，一切都必须以最快速、最优方案来解决用户问题为指导原则。
  3. **服务保障措施应该坚持符合国标和行业规范的原则。**所提供的服务标准与水平，需要符合相应的国标规范，如提供的服务应满足《信息安全技术 云计算服务安全能力要求》（GBT 31168-2014）、《信息安全技术云计算服务安全指南》（GBT 31167-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2015]14号）及国家主管部门发布的其他标准规范要求等等。
  4. **服务保障措施应该符合本地实际情况的原则。**应根据此次项目所覆盖单位的实际情况，进行分类、有针对性的服务。对于部分技术力量强的单位，可以在人员到达现场的同时，公司同时提供在线指导；对于部分技术维护力量教薄弱的单位，则要强调我方技术人员到达现场的时间跨度，以及解决问题的时限等等。
  5. **保障服务需遵循持续反馈总结、防微杜渐的原则。**每次提供技术保障服务，无论问题大小，都要坚持留下详细的过程记录，并制度性的定期反馈总结，从根源上避免小问题累积成大问题。

## 故障应急服务保障的内容

整个项目必须综合开展运行监控、补丁管理、配置管理、故障管理、变更管理、资源管理、信息管理、安全管理、业务开通、故障响应等项工作，才能保证全网的稳定运行及对已承载的业务提供有力支撑。

金蝶天燕在此次项目的紧急服务保障中的技术支持主要包括**业务和生态**两方面内容.

### 对于业务保障服务方面

主要是面向金蝶Apuisc应用服务器中间件承载的业务系统，侧重监视、控制、调度、维护、测试、管理。这个一方面是要依赖产品的各项技术功能来保障，比如监控组件、集群组件等；另一方面要做好合理的服务资源保障，如服务团队、服务流程、服务策略等等方面。

### 对于生态保障服务方面

主要是面向以用户为中心的、全生态链条的综合保障体系，因为一旦出现重大紧急问题，一般不是仅仅某个方面出现问题，而是会需要软件、硬件、网络、安全等方方面面的厂商一起来综合性应对。在面对重大突发问题的情况下，金蝶天燕作为中间件厂商，需要服从总体技术保障团队的安排，为最终问题的解决，贡献中间件层面的技术参考意见及解决办法。

### 服务保障内容清单

服务保障的具体内容，包括如下的方面：

|  |  |
| --- | --- |
| 系统服务 | 突发重大紧急情况技术支持 |
| 服务覆盖范围 |  |
| 此次项目中用到以及即将用到金蝶Apusic应用服务器产品的所有终端用户 | 保护 |
| 金蝶Apusic应用服务器软件所承载的所有业务系统 | 保证 |
| 金蝶Apusic应用服务器软件自身及替代过渡期的待替代的各类中间件 | 保证 |
| 重大紧急情况下的生态综合应急响应支持 | 保证 |
| 服务响应 |  |
| 电话覆盖时间 | 7\*24小时 |
| 电话响应时间 | 立即响应 |
| 能够到达现场的时间 | 7\*24小时 |
| 到达客户现场时间 | 2小时内 |
| 特别重要时刻到达客户现场的紧急时间 | 1小时内 |
| 问题诊断时间 | 1小时内 |
| 从人员到达现场起系统恢复时间（中间件自身的问题、每2小时无法解决问题，则服务响应升级） | 8小时内 |
| 从人员到达现场起给出合理技术建议的时间（上下游生态链的问题） | 4小时内 |
| 服务记录报告及总结报告提交 | 提供 |
| 定期巡检与预防性维护 |  |
| 系统定期巡检维护 | 每季度一次 |
| 健康性检查 | 每月一次 |
| 专家巡检 | 每季度一次 |
| 全面巡检 | 每年一次 |
| 系统检查及服务报告 | 提供 |
| 技术服务 |  |
| 项目现场技术支持 | 提供 |
| 远程并行的专家级技术指导 | 提供 |
| 随时随地响应客户咨询 | 提供 |
| 远程诊断 |  |
| 远程拨入系统分析 | 提供 |
| 远程故障解决 | 提供 |

### 服务内容说明

#### 保修期内服务范围

（1）确保本次保修范围内所有中间件产品及中间件产品之上的业务系统能够正常运行。由此产生的业务及生态问题，都在应急响应服务范围内。

（2）产生重大安全问题或者功能模块需求时，金蝶天燕将及时提供必要的中间件产品升级。比如某些计算机病毒的大规模扩散时，能以最快的速度及时有效的提供临时安全补丁。

（3）确保客户在产生应急业务需求下的快速响应。如疫情阶段，要紧急部署某些业务系统，金蝶天燕将提供中间件层面的紧急技术支持。

#### 服务响应

（1）全天候7×24小时

（2）对于重大问题，如现场技术无法解决，支援的技术专家2小时内到达现场，非常紧急时刻1小时到达现场，如果是中间件产品自身的问题，包含服务响应升级的时间在内，总体保证8小时之内系统恢复正常，问题解决12小时之后，给出服务报告。如果是上下游生态问题且需要中间件协助的问题，则保证4小时内，给出中间件产品层面的技术建议；

（3）非系统崩溃的情况，接到问题报告后0.5小时内提供电话支持服务；

（4）多级别服务支持，技术专家到达现场后，如1小时内无法解决问题，此后则每2小时提升技术响应级别，必要时公司研发总监、CTO直至总经理亲临现场协调解决该重大突发紧急问题；

#### 维护间隔与维护情况汇报

（1）每季度一次的例行巡检即预防性维护并提供巡检分析报告；

（2）每年一次全面巡检，包括运行安全、性能评估、问题总结、资源状况并提供全面巡检报告；

（3）每次故障处理后提供技术处理和备件更换报告；

（4）服务期限内，每月完成并提供当月服务总结报告；

#### 季度定期巡检与预防性维护内容

每季度一次的定期例行巡检和预防性维护，内容包括：

（1）提供巡检报告；

（2）中间件及相关运行环境运行物理状态；

（3）系统性能检查；

（4）系统运行环境健康度诊断；

（5）业务数据安全存储检查；

（6）运维错误报告的分析、记录和清理；

（7）及时提供产品补丁；

（8）重点核心业务系统的备份节点巡检等同于生产节点；

#### 节点备份

预先提请用户对关键业务系统做好备份节点，备份节点也会在预防性巡检阶段被检测到，一旦发生重大紧急、且无法立即排查原因的bug时，将立即启用备份节点。

所有备份节点，可以根据对业务重要程度的区分，分为本地同服务器节点备份、不同服务器节点备份、异地备份等多种不同形式。

#### 应对重大突发紧急事件的演练培训

我们将免费提供应对突发重大紧急情况的专项技术培训和技术交流，通过不定期的演练重大突发情况下的应对预案，来磨合及协同各方共同应对紧急重大突发事件的处理经验。包括：

* **现场培训：**

主要在巡检及项目实施过程中进行，由我公司工程师结合实际情况，对工程产品的安装调试、使用和维护阶段，如何应对预设的各类重大突发情况，并对常规解决方案和应对策略进行详细的讲解，达到客户相关人员能够自主解决常见的突发情况，如网络断线的备份节点如何启用，常规网络病毒攻击的配置防御措施等等。

* **专业技术培训：**

通过培训使相关技术人员能熟悉应对重大突发事项的预案以及所涉及的技术细节。我公司将免费提供培训师资、教材及协助搭建培训软硬件环境。

技术培训也包括如何与上下游产品厂商进行一体化的技术协同配合。如何操作、如何调试、如何技术验证等等方面。

#### 同步远程诊断

在接到重大紧急服务要求时，一方面会指派精干技术人员赶赴现场，另一方面会提请公司专家级的技术资源与客户链接，通过远程诊断，尽量避免重大紧急突发事件向不可预料的方向发展。在安全可靠的前提下，也可以远程拨入系统分析和远程系统监控，以达到对紧急重大故障的远程解决。

远程诊断可以为客户提供最为迅速的技术支持，以最快捷方式保证系统的正常运行。

#### 保修期终止

运维保修期终止前十五日内，将派遣专门组建的综合性工程师团队前往客户现场，对保修产品进行一次全面检查，双方签署《中间件产品维护期届满备忘录》。若有遗留问题，双方另行商定。

服务期结束后，将根据用户需要，按照本服务方案标准及要求继续提供维护服务。

## 应急事件的响应等级及措施

### 应急分级

根据信息安全特点以及应急事件的严重性、影响范围，由紧急程度低到高定义蓝色故障等级、黄色故障等级、橙色故障等级、红色故障等级四个应急等级。启动预警后，第一时间向建设单位项目主管部门报告，如下对各等级进行划分：

1.蓝色故障等级

对生产环境造成影响，不符合规范化操作和管理要求，导致业务存在重大风险隐患的，定义为蓝色故障等级。

2.黄色故障等级

造成生产业务中断，但未造成数据损坏、经济损失，可以通过修改业务系统、调整软硬件配置快速恢复业务的，定义为黄色故障等级。

3.橙色故障等级

造成业务中断，需要对业务系统进行重大升级，业务数据遗失但可以进行紧急恢复或更换核心部件的，定义为橙色故障等级。

4.红色故障等级

对全网业务造成或有可能造成重大影响，重要业务数据丢失难以恢复的，以及信息化主管部门确认的，定义为红色故障等级。

### 应急处置

应急保障负责人接到故障报告，第一时间通知建设单位项目主管部门负责人，启动对应故障等级应急预案，联系相关保障团队人员。

1.蓝色应急预案

首先快速分析风险隐患，定位故障原因；

针对故障原因，提出解决方案；

待应急保障负责人及系统主管确认后，安排专业人员进行排除。

2.黄色故障等级

首先快速分析风险隐患，定位故障原因；

故障相关保障人员1小时内到达现场，防止问题升级；

针对故障原因，提出解决方案；

待应急保障负责人及系统主管确认后，安排专业人员进行排除。

3.橙色故障等级

业务系统保护性关闭，快速分析风险隐患，联系保障团队定位故障原因；

故障相关保障人员1小时内到达现场，防止问题升级；

针对故障原因，提出解决方案；

待应急保障负责人及系统主管确认后，安排专业人员进行排除。

4.红色故障等级

故障业务系统及关联业务系统保护性关闭，快速分析风险隐患，联系保障团队定位故障原因；

故障相关保障人员1小时内到达现场，控制故障影响范围；

我公司高层领导督战，随时协调各种资源；

组建专家团队针对故障原因，提出解决方案；

待应急保障负责人及系统主管确认后，安排专业人员进行排除。

原则上2小时内排除故障，故障排除后，向应急保障负责人提交故障处理报告，组织保障人员认真开会总结，避免此类事件再次发生。

### 主要应急措施

预防和准备性措施是应急措施的重要内容，它可以降低系统的风险和系统发生故障时的破坏性，有利于尽快恢复系统运行，主要有以下三个内容：

1.环境保障

严格按照生产系统环境配置，系统应部署在具备足够安全生产条件的机房。运维人员进行例行检查，确保系统的正常运行。

2.数据备份

系统运行可能会因为自然或人为的原因遭破坏，我公司将在售后运维期间，配合应用开发商或用户单位按照既定的方案实施系统恢复维护。如定期进行数据备份，保证在系统故障的时候能及时恢复。

3.应急响应

当应用系统或服务器出现故障,首先由现场运维工程师配合应用开发商或网络运维人员进行紧急排查，评估后进行紧急修复，或调派后台支持工程师在规定的时间内尽快修复故障并恢复系统正常运行。

如果应用系统或服务器出现紧急故障，无法及时修复的，紧急采用当地的备品备件，我公司需在服务器使用备品恢复后，配合应用开发商完成应用系统的部署和恢复。

## 应急服务保障的资源安排

在遇到积极重大突发事件时，我们优先保障投入精干的技术资源。其次根据事件的紧急程度，技术资源保障的级别逐级迅速提升。

（1）首次派出的技术人员必需至少保障有如下的技术资历：服务工程师都是公司中间件产品的原厂且经过技术认证与评级的维护工程师，在同类项目上的工作年限在三年以上，负责过国内至少三个以上大型信创类项目的实施及运维；

（2）公司每年为每个提供此类重大紧急服务保障的一线技术工程师提供三周以上的专业培训，以保证技术工程师不断吸收新知识及技术水平的不断升级，并能深入掌握公司产品的新功能、新技术，能够全面了解并掌握Apusic应用服务器产品的升级改造情况、以及中间件上下游产品厂商的技术升级情况、了解信创信息化总体背景情况等，以备技术工程师在客户现场应对紧急突发状况时，能够迅速做出有效的技术判断，并立即采取有效可行的解决办法，从而尽可能的避免用户方的损失；

（3）当现场工程师无法立即有效的解决用户问题，在规定时间内做出二级响应的支持工程师，是公司中间件产品的核心研发人员；

（4）如果二级响应的研发工程师仍然无法及时有效是解决问题，则第三级响应的技术资源，将提请公司研发总监、CTO、副总经理级别的技术骨干立即介入支持，并及时上报公司总经理。

（5）如公司三级响应技术支持仍然无法解决问题，则立即报请集团公司，提请科学家级别的技术专家介入解决。

上述响应机制，总体时间不超过2个小时内。如遇特别紧急、影响面特别大、受波及范围特别大的重大事件，则公司产品研发核心骨干将在第一时间直接介入，并给出有效的解决方案。

## 突发故障事件的应急预案

在综合统筹考虑突发重大紧急情况的应对策略时，首先要优先考虑数据安全，做好备份。其次要重点保障对用户业务持续性、稳定性的维持，尽量使得用户不因事件影响停服。从这个核心目标来展开演练预案，主要分为三个阶段来设计应对突发重大事件的处理预案。主要包括事前预防准备工作、事中响应处理流程、事后分析总结

### 事前预防准备工作

突发重大紧急事件往往不可预料，所产生的结果影响也难以预料，因此在平时就需要做好全面的预防准备工作，以避免给用户造成重大损失。主要包括如下的一些工作项：

1. **业务数据备份**

对中间件承载的业务系统进行分类，按不同级别的业务系统进行不同频次的数据备份，做到应备尽备。

1. **应用节点备份**

对于关键业务系统，需要做适当的冗余，做好应用节点的备份，并且需要保持应用节点随时启动的状态，要保证随时可以做节点切换的状态。

1. **预留冗余资源**

为预防某些业务在某些时间段突发高并发访问量，需要在服务端做适当的、机动的资源冗余储备，如网络带宽、存储空间等方面。并且要保持资源随时处于活跃状态，可供随时切换。

1. **技术人员培训**

提供服务的技术人员的配置需要设定一定的资质门槛，同时也要强化技术培训机制，包括产品、现场环境、新技术、当前网络安全危险新动向等方面的内容。

1. **定期生态交流**

用户一旦面临重大突发事故，往往不是某一家产品所导致的，生态厂商之间需要保持定期的沟通，做好技术交叉培训，尤其是基于项目的实际环境和业务场景，各厂商之间定期做好技术交流、技术磨合等方面的工作。

1. **定期巡检（含备份节点）**

要强化定期巡检的机制。巡检不仅仅针对生产环境，针对备份环境也要定期巡检，并且把备份环境等同于生产环境来对待，保证备份环境随时可用。

1. **定期恢复演练**

恢复演练包括备品备件的激活操作，也包括上下游各环节厂商之间的人员协同磨合。尤其是在问题的定位分析、协同策略等方面要做综合性的恢复演练演习工作。

1. **设立预警机制**

要整合个厂商产品自身的监控平台功能，结合总体监控平台，对重大紧急突发事件的指标产生做预防性的指标设计。比如某个关键应用系统的访问量达到了某个数值指标，则需要启动预警机制。或者某个病毒感染、网络攻击在整个应用范围内达到一定的程度，并有扩散的趋势等，都可以设定一定的预警机制和指标。

1. **重点事件预防**

针对部分明显会造成大面积影响的事件，需要进行重点梳理。比如，如果启用中间件的自动版本升级功能，则很可能由于升级包的bug或者不完善，导致一下子覆盖面过大，造成大面积的应用停服；或者网络病毒、或者关键网络断网、底层存储设备损坏等典型的、会涉及大面积影响的事件，需要单独梳理出来，进行针对性的预防和演练。

### 事中应急处理流程

然而，一旦发生突发紧急重大事项时，无论是金蝶天燕还是其他友商，都需要立即启动合理有效的快速响应服务机制，金蝶天燕为此项目初步拟定的重大事项技术服务流程如下：

图 事中紧急处理流程

整个服务流程、事件响应级别升级机制的设计和考虑，首先是要在最短的时间内保障用户的业务安全、数据安全，其次是要把影响控制在最小范围内。

### 事后总结分析优化

在遇到突发紧急重大服务保障情况下，优先解决客户的实际问题，并会在问题解决完毕之后，做好过程记录并归档。

金蝶天燕公司将为此项目指定专职的管理团队，定期收集用户对服务质量的评估，尤其是突发情况下的技术服务水平，以客户满意度来考核服务质量及服务承诺，从中发现不足，并积极地予以改正和补救。

在公司内部进行了科学合理的评估之后，我方将与客户方就具体的突发紧急事件的服务过程、服务流程、服务质量等关键性的问题，与客户会商，并认真仔细听取客户意见，双方商讨服务过程与结果的亮点与不足，并提出整改措施，相关讨论过程将归档并留存会议纪要。

## 关于建立重大事项联防联控机制的建议

从当前金融行业信创国产化替代工程的背景来看，此次的信创替代工程是全面性的，中间件产品作为其中的一个环节，需要积极的联合上下游产业链的技术力量，凝聚成一个强大的技术团队共同为用户服务，防范和应对解决突发重大紧急事故。

从技术自身的角度来看待所面对的突发重大事故风险，问题往往不止牵涉到某一两家厂商，尤其是分析定位问题阶段，需要上下游各厂商通力合作，才能迅速有效的为用户提供解决方案。在解决问题阶段，也离不开各家厂商是协同配合。

保障最终用户运行环境的总体平稳，是我们所有各家参与厂商的共同目标，因此，金蝶天燕如果中标本项目，将建议**由用户牵头，召集本次信创工程中参与的所有国产厂商，共同制定专门应对重大突发事项的联防联控机制。**只要出现这类问题，各家厂商，都必须按照这个机制、提供本单位最适合的技术力量、迅速组成技术攻坚团队。同时，在预防阶段，也需要做好相关的技术资源调配、参与预防演练等工作。

我们建议，联防联控机制的核心内容包括如下的一些方面：

* 1. **各家厂商需指定专门技术联系人。**在整个技术团队中，应该至少涵盖这些岗位：中间件工程师、中间件高级工程师、数据库工程师、数据库高级DBA、网络工程师、运维开发工程师、云平台工程师、云平台大数据工程师、云平台基础工程师、安全态势感知运维工程师、机房硬件工程师等等。如遇到上述岗位技术人员无法解决的问题，各家厂商要承诺迅速做出响应升级行动，派出各家单位更高级别的技术骨干参与到技术攻坚团队中来。
  2. **定期举行联合预防演练：**主要是加强各单位技术人员之间的技术与流程的磨合。每次演练可以预设演练主题，比如安全主题、网络主题、性能主题、自动化版本升级主题，也可以按业务需求来分设主题，比如两会期间、年底年初服务等等方面。
  3. **定期举行交叉技术培训：**使每家厂商的技术人员都能熟悉与自家产品相关联的上下游产品的产品情况。并部分解决技术人员流动，造成的技工作交接错位的情况。
  4. **制定一系列的联合应急响应流程：**在联合运维的流程设计上，要参照金融信息化运维支撑体系规范要求，并结合本项目运维实际需求，实现服务流程与服务内容紧密结合。每一项服务内容都可被运维流程所调用并记录，实现运维服务和管理流程的相互交融，全面提升服务质量。流程主要包括：服务台流程、值班流程、抢修流程、巡检流程、事件管理流程、故障管理流程、请求管理流程、问题管理流程、变更管理流程、配置管理流程、发布管理流程、服务报告管理流程、连续性管理流程等等。
  5. **运维资料共享机制：**一旦发生重大紧急情况，资料的综合调阅往往是一个非常重要的措施。由于平时各家单位都是以自家的产品运维为主要工作，因此在应对紧急重大事项时，查找运维资料、定位问题原因，对解决问题的时间和效率往往发挥着至关重要的作用。因此建议加强运维资料的定期共享，我们初步建议的资料包括如下的一些：

|  |  |
| --- | --- |
| **资料类型** | **资料名称** |
| **巡检类** | 巡检计划 |
| 巡检报告 |
| 巡检遗留问题跟踪表 |
| **工单类** | 工单电子件 |
| 工单报告 |
| **报表类** | 网络性能报表 |
| 网络故障&问题报表 |
| 运维耗材&备件使用登记表 |
| **报告类** | 故障报告 |
| 故障汇总月报 |
| 网络性能报告 |
| KPI/SLA报告 |
| 日常维护活动总结报告 |
| 专题方案及总结报告（如重大节日安全保障方案及总结） |
| 维护月报 |
| 年度复盘总结报告 |

上述建议，在实际实施阶段，仍需要不断细化细则，金蝶天燕如果中标，将积极推动此项工作的落实。

## Apusic应用服务器通用应急预案

##### 应急处置原则与工作流程

本次中间件应急预案以“先抢通、后抢修”为处理原则，首先恢复业务应用，保存相关日志，后期再根据日志进行详细分析和故障定位。

Apusic应用服务器是应用程序的发布平台，相对比较稳定。业务应用均通过Apusic应用服务器进行发布，通过Apusic应用服务器的JDBC等配置，实现前端应用和后台数据库之间的交互。因此不管是程序代码问题、硬件问题、数据库问题均有可能体现在Apusic应用服务器节点异常；并且由于程序代码效率低下、参数配置不当，也会导致Apusic应用服务器节点异常。这种情况下，重启异常Apusic节点，释放资源，是最快的恢复业务的应急手段。具体原因可以通过备份日志，事后进行分析排查。

本应急预案中涉及到的程序包路径，均是根据具体项目中Apusic应用服务器安装规范中指定的路径。如果未按照规范安装的中间件，请电话咨询对应系统专责协助处理。

##### Apusic应用服务器故障应急场景

故障应急处理步骤6步：

1. 使用web浏览器访问节点应用确认节点可用性。
2. 登陆Apusic应用服务器控制台确认节点状态。
3. 收集故障点日志，备份节点日志。
4. 查看节点日志，根据报错信息确定故障原因。
5. 根据故障原因，执行应急操作。
6. 组织人员进行具体原因分析并整改。

**三、故障场景**

Apusic应用服务器日志文件中常见错误如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 错误信息 | 原因 | 出现时机 | 执行步骤 |
| 1 | java.lang.OutOfMemoryError | 内存溢出 | 节点运行过程中 | 1、2、3、4、5 |
|  | java.lang.OutOfMemoryError | 内存溢出 | 节点启动过程中 | 4、5、6 |
| 2 | more than the configured time (StuckThreadMaxTime) of "600" seconds | 线程阻塞 | 节点运行过程中 | 1、2、3、4、5 |
| 3 | error occured:Apusic.jdbc.extensions.PoolLimitSQLException: Apusic.common.resourcepool.ResourceLimitException: No resources currently available in pool dgNonPool to allocate to applications, please increase the size of the pool and retry.. | JDBC连接池满 | 节点启动过程中 | 4、5、6 |
| 4 | server-000627 Reachedmaximum capacity of pool “JDB-HQGL” make 0 new resource instances  <server-000628> <Created "1" resources for pool "JDBC Data Source-0", out of which "0" are available and "1" are unavailable. | JDBC连接池满 | 节点运行过程中 | 1、2、3、4、5 |
| 5 | Too many open files | 打开文件超过系统限制 | 节点运行过程中 | 1、2、3、4、5 |
| 6 | <server-000386> <Server subsystem failed. Reason: apusic.security.SecurityInitializationException: Authentication for user Apusicdenied  Apusic.security.SecurityInitializationException: Authentication for user Apusicdenied | aas密码错误 | 节点启动过程中 | 4、5、6 |
| 7 | /home/Middleware/aas/bin/startserv: line 180: 64034 Killed                  ${JAVA\_HOME}/bin/java ${JAVA\_VM} ${MEM\_ARGS} | 人为停止节点 | 节点运行过程中 | 1、2、3、4、5 |
| 8 | <Aug 10, 2014 1:41:37 AM CST> <Error> <EmbeddedLDAP> <srver-000000> <Error opening the Transaction Log: /home/Middleware/domains/test\_domain/config/server.policy Permission denied)> | 权限问题 | 节点启动过程中 | 4、5、6 |
| 9 | <Aug 10, 2014 3:15:07 AM CST> <Error> <JDBC> <server-001112> <Test "SELECT 1 FROM DUAL" set up for pool "JDBC Data Source-0" failed with exception: "java.sql.SQLRecoverableException: No more data to read from socket".>  <Aug 10, 2014 3:15:07 AM CST> <Warning> <JDBC> <server-001129> <Received exception while creating connection for pool "JDBC Data Source-0": IO Error: The Network Adapter could not establish the connection.> | 数据库单节点异常，RAC无法全部正常对外提供服务 | 节点运行过程中 | 1、2、3、4、5 |
| 10 | The JRE was not found in directory /usr/java/1.8.0\_232. (JAVA\_HOME) Please edit your environment and set the JAVA\_HOME variable to point to the root directory of your Java installation. | Java环境变量配置不正确 | 节点启动过程中 | 4、5、6 |
| 11 | <server-002621> <Connection rejected, the server license allows connections from only 5 unique IP addresses.> | 版本license未授权 | 节点运行过程中 | 1、2、3、4、5 |
| 12 | VM Version 1.8.0\_232 from Sun Microsystems Inc.>  <2014-8-11 下午04时50分58秒 CST> <Critical> <ApusicServer> <server-000362> <Server failed. Reason:  There are 1 nested errors:  Apusic.management.ManagementException: Unable to obtain lock on /home/middleware/domains/test\_domain/servers/AdminServer/tmp/AdminServer.lok. Server may already be running | 节点未正常停止 | 节点启动过程中 | 4、5、6 |
| 13 | 因硬件或者系统故障，应用服务器全部无法启动 |  |  | 6 |

##### 应急处理步骤

1. 使用web浏览器登陆访问对应故障节点应用地址，验证故障现象，防止误告警出现。
2. 登录Apusic应用服务器控制台，确认故障节点名称。
3. 使用web浏览器，访问Apusic应用服务器控制台<http://IP>:端口，根据异常端口号确认异常节点名称，如下图。



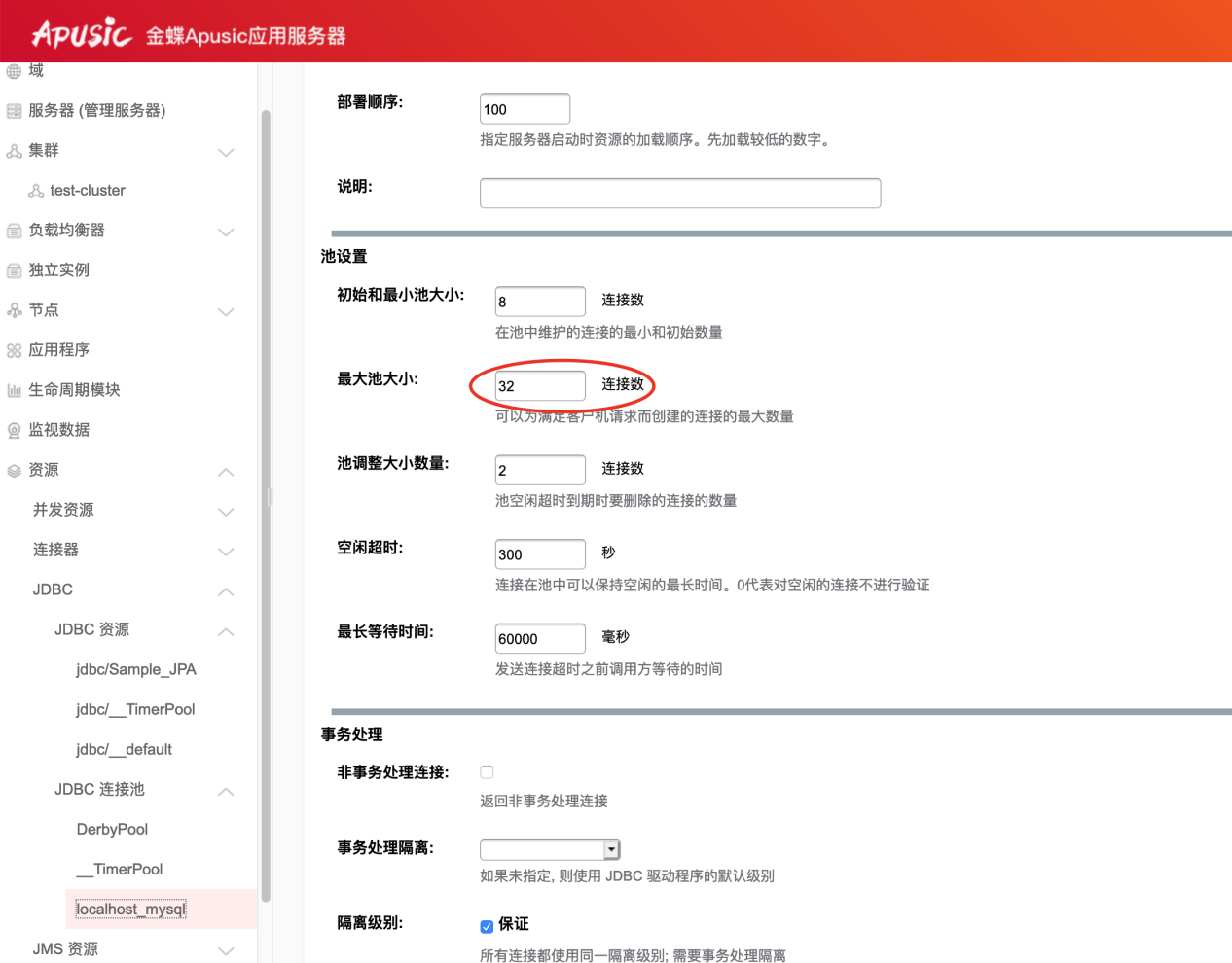
1. 使用Apusic用户登陆操作系统。
2. 备份对应节点日志。

|  |
| --- |
| $cd /middleware/aas/domains/mydomain/logs/server.log ---进入对应日志目录  $ cp –r server.log 20200808server1.log -----按照日期备份节点日志 |

1. 查看节点进程状态。

|  |
| --- |
| $ ps –ef|grep server(server1为节点名称)  如果返回值为空，如下，则执行步骤12：  server 59086 2803 0 22:12 pts/1 00:00:00 grep server  如果返回值不为空，如下，则执行步骤11： |

1. 增加JDBC连接池上限
2. 登陆Apusic应用服务器控制台，进入JDBC配置页面，修改增加JDBC配置。主要调整初始和最小池大小及最大池大小两个参数，其中初始和最小池大小表示初始建立的连接数，最大池大小表示最大的连接数，主要调整增大最大池大小参数，再原有基础上增加20。（具体要根据对应数据库的process上限，要求Apusic应用服务器节点数\*最大池大小值< 数据库process数的80%）如下图所示：



1. 如果无法进入JDBC控制界面，可以通过重启应用节点，释放数据库连接资源，达到抢通业务的目标。
2. 调整操作系统用户打开文件数量上限

|  |
| --- |
| 使用root用户登录系统  # vi /etc/security/limits.Conf  Apusic - nofile 10240 ----新增该内容，或者调整该值上限。  # su – Apusic ---切换到Apusic用户  $ ulimit –Hn ---验证配置是否生效，如下表示生效  10240 |

1. 修改Apusic应用服务器后台启动密码问题

|  |
| --- |
| 使用Apusic用户登录系统,进入服务器目录,修改后台启动密码文件。  方法1：如果某个管理员如admin密码忘记了，但是其他用户密码知道，就可以拷贝安装路径下mydomain/config/ admin-keyfile中的其他用户的密码，替换admin用户的密码,需要重启系统才生效。  方法2：修改mydomain/config/admin-keyfile文件里面对应的用户的密码，使用如下密码替换 “{SSHA256}iU4Ef2uGWYh3V+BQjpW5f8BTbgGWzKp7pfrNU020Nu2l9YLEwCWOpA==”，重置为空密码，重启系统，需要重新设置密码。  方法3：系统管理员admin登陆控制台，切换到配置->server-config->安全性->安全域->  admin-realm页面，点击【管理用户】按钮进入用户管理界面，点击用户名称编辑用户，可以修改用户密码。。 |

1. 调整JVM参数设置

|  |
| --- |
| 使用Apusic用户登录系统  登录Apusic应用服务器控制台，点击配置,点击server-config，如图所示，根据需要调整内存大小。具体要根据服务器的物理内存确定，原则上该服务器上运行的java进程内存总和，不得超过物理内存的80%。 |

1. 修改文件权限

|  |
| --- |
| 使用root用户登录操作系统  # chown –R Apusic:Apusic /middleware/ ----修改程序包的权限  #chown –R /middleware/domains/  对应domain名称 ------修改Apusic应用服务器相关文件权限  #chown –R /middleware/ domains/mydomain/logs/server.log ------修改启动日志文件权限 |

1. 停止异常节点进程

|  |
| --- |
| Apusic@test] $ kill -961658 ----停止异常节点进程 |

1. 启动异常节点

|  |
| --- |
| Apusic@test]$ cd /middleware/aas/bin --进入启动脚本路径  [Apusic@test]$ ls  [Apusic@test]$ ./startserv ---启动节点 |

1. 修改JDBC连接串

|  |
| --- |
| 如果在数据库单节点或者VIP等集群服务异常时，导致数据库节点无法全部正常对外提供服务时，修改JDBC连接串，让应用节点连接到可用的数据库地址上。  登陆Apusic应用服务器控制台，进入JDBC配置页面，根据数据库专责提供的可用连接串，修改JDBC连接串地址。 |

1. JAVA环境变量错误

|  |
| --- |
| Apusic用户登录系统  $ java –version --------查询Apusic用户下jdk信息 java version "1.8.0\_251"  Java(TM) SE Runtime Environment (build 1.8.0\_251-b08)  Java HotSpot(TM) 64-Bit Server VM (build 25.251-b08, mixed mode) $ which java ---查询jdk安装路径 /usr/bin/java  $ cd /middleware/aas/bin  $ vi startserv ---按照上面查询的路径结果修改Apusic脚本中的JDK配置  JAVA\_HOME="/usr/bin/java" export JAVA\_HOME |

1. 更换Apusic应用服务器license

|  |
| --- |
| Apusic用户登录系统  使用FTP工具上传授权license至/middleware/aas/目录下 |

1. 因硬件或者系统故障，节点均无法启动

|  |
| --- |
| 临时调配应用服务器，重新安装Apusic应用服务器，利用备份文件，进行重新发布配置。建议保留原故障环境。 |