运维管理规范

版 本 历 史

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **版本** | **说明** | **作者** |
| 2017-5-27 | 0.1 | 新建 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[**1.** **总则** 3](#_Toc490492053)

[**2.** **范围** 3](#_Toc490492054)

[**3.** **运维规范** 3](#_Toc490492055)

[**3.1.** **系统账号管理制度** 3](#_Toc490492056)

[3.1.1. 账号密码设置 3](#_Toc490492057)

[3.1.2. 账号密码使用 3](#_Toc490492058)

[3.1.3. 内部管理帐号的删除 3](#_Toc490492059)

[3.1.4. 内部管理帐号权限的变更 3](#_Toc490492060)

[**3.2.** **服务器运维管理制度** 4](#_Toc490492061)

[3.2.1. 工作内容概述 4](#_Toc490492062)

[3.2.2. 服务器安全守则 4](#_Toc490492063)

[3.2.3. 运维文档管理 4](#_Toc490492064)

[3.2.4. 服务器集群管理 5](#_Toc490492065)

[3.2.5. 系统监控管理 5](#_Toc490492066)

1. **总则**

为了更好的确保公司产品安全稳定运行，提高公司产品的服务质量，特制订本管理制度，作为公司系统运维的依据。

1. **范围**

此规范适用于公司系统运维工作人员，也供开发人员参阅。

系统运维工作包含但不限于对服务器日常维护、监控与灾备，操作系统的安装与维护，各产品应用的负载均衡配置，数据库的安装、备份及日常维护、网络安全监控等。

1. **运维规范**
   1. **系统账号管理制度**
      1. 账号密码设置

* 所有在线服务器，均禁止root用户登录，并且密码设置必须是12-18位的强密码（包含数字、大小写英文和字符）。
* 服务器密码应该定期更新，最多不超过3个月需要更换一遍密码。
* 公司内部管理服务器，例如SVN服务器与GitLab服务器，密码统一由运维设置。
  + 1. 账号密码使用

新入职员工或系统初始使用者，知会运维，默认开通内部服务器账号；

系统服务器账号，如须使用，需向其部门分管领导提出账号密码申请，经产品负责人>技术负责人>系统运维核准后，授权使用。

* + 1. 内部管理帐号的删除

员工如果因岗位变动而不再需要访问公司信息资源时，账号管理专员在收到HR通知后，删除该员工相应的内部管理帐号。

员工离职后，账号管理专员在接到离职手续后，删除该员工所有的员工帐号。

* + 1. 内部管理帐号权限的变更

如果员工因岗位变动或其他工作原因需要修改信息系统访问权限，其部门分管领导需要通知运维人员修改权限。 

账号管理专员需要依照“最小需要知道”原则对员工权限分配情况进行定期检查，如有必要，将修改员工权限，并通知该员工和其部门分管领导。

* 1. **服务器运维管理制度**
     1. 工作内容概述

服务器作为公司产品的核心支撑设备，建立起有效的备份与容灾体系，在发生各类灾难时快速响应、全力保证业务连续性，将成为保证企业运营持续稳定的关键。

公司在线产品运行支撑的服务器，均使用的阿里云服务器，硬件安全方面已经比较稳定，主要的运维任务，在于备份与容灾体系，可自动建立定时定期自动备份计划、双机热备份、系统恢复、灾难恢复、异地容灾、报警机制、安全查杀、攻击防御等，无论应用服务器发生任何意外，例如，恶意的程序破坏、文件损毁、人为误删误改、操作系统宕机、硬件故障，甚至整个机房毁于意外，都可以完整保护整个信息系统，保障最大程度的使数据丢失最少，业务中断时间最短，恢复能力最强。

服务器管理的运维人员有权对公司的所有服务器进行操作并查看。同时，其负有对所有服务器信息保密的义务。

* + 1. 服务器安全守则

1、所有线上服务器，应禁止root用户登录；

2、所有线上服务器应该修改默认的SSH端口；

3、不同的游戏服务器，绝不添加到同一个安全组中；

4、不同的游戏，绝不同用一台服务器；

5、除测试服，所有线上服务器都要使用云版mysql，memcached，redis

6、mysql，memcached，redis绝对不能在不同的游戏里共享；

7、测试用的mysql，memcached，redis绝对不能监控外网IP，并且只允许在安全组内访问；

8、服务端服务器，禁止使用PHPMYADMIN，测试服必须改PHPMYADMIN的默认目录和密码。

* + 1. 运维文档管理

1. 运维需要对服务器管理相关文档整理备案，更新的文档需及时归档，服务器方面管理文档包括：

* 内部开发服务器配置详细说明
* 内部服务器安全管理说明
* 线上服务器配置详细说明，需保密
* 线上服务器安全管理账号，需保密
* 线上服务器与内部开发服务器数据通说明
* SVN服务账号、版本及配置说明，账号密码信息需保密
* 服务器交互配置详细说明
* 服务器安装程序列表

1. 研发人员对服务器的操作权限由运维进行分配，并对服务器操作权限、研发人员的使用情况、操作安全等负责。
   * 1. 服务器集群管理

公司游戏产品均是互联网产品，用户量比较大，对服务器的要求比较高，因此需要做Linux服务器集群，并实现负载均衡。

* + 1. 系统监控管理

1. 监控内容

为保证认证各游戏产品7\*24的可靠稳定运行，需采用网管软件或其他监控工具对整个系统进行全方位的监控，主要包含网络状态、硬件运行状态及系统服务状态等多个方面。

网络状态：主要监控网络的运行情况，如网络进出流量，当前线路质量，检测各种安全事件（入侵、探测、攻击）等等；

硬件设备状态：主要监控系统内所有硬件设备的运行状态，对主要服务器的硬件资源使用情况进行监控，如硬盘空间、CPU使用率、内存占用情况等等，对网络设备如路由器、交换机、负载均衡设备的运行状态进行监控；

系统服务状态：对系统的所有服务进程的状态进行监控，可使用监控工具或脚本工具对服务的端口进行检测，也可通过定时运行模拟业务过程的检测程序对整个系统服务状态进行监测；

1. 每日需对服务器运行情况进行监控、检查、分析、记录等工作，形成《服务器运维日报表》，每日提交归档。
2. 每周需对服务器进行杀毒、清理垃圾文件、升级补丁，保持服务器环境安全，形成《服务器安全周报表》,每周提交归档。
3. 若有突发异常事故，运维需第一时间向总经理汇报并协调跟进解决，以保证损失降至最低。