PDF 文件，便于资产二维码打印。

1.6.1.3.资产资源一图管控

基于遥感影像和基础地理信息数据，叠加国土三调、宅基地调查和国土空间规划图层，采用一张图的方式展示武进区所有的农用地、养殖水面、厂房、宅基地等全要素资产资源情况，图上地块与农村集体资产监管业务数据一对一关联，实现图上资产资源全生命周期管理，包括资产资源编号、权属情况、合同情况等信息管理。可根据规划用途进行多维度的比对分析，全区层面一目了然地统览到各类型资产资源的分布、占比情况。主要功能如下：

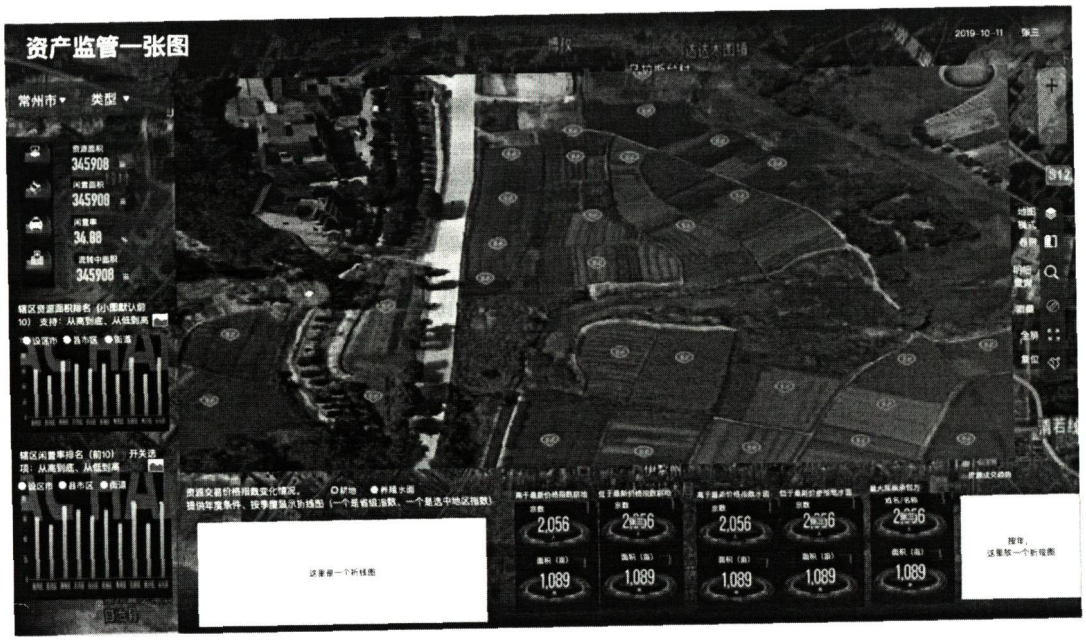
1、 将资产、资源等业务数据与地理信息数据进行关联，实现业务数据的可视化展示。

2、 依托电子地图，展示资源相关统计信息。主界面以地图为背景，通过查询条件及统计项，实现地图与业务数据联动展示。

3、 支持图上查询，查询条件支持按地区、资源类型进行检索。更改查询条件，显示统计信息将实时联动，同时地图将自动定位到所选地区，并在地图中标识出满足查询条件的资源对象。

4、 点击地图中资源对象，显示该资源详情。资源详情包括卡片信息、交易信息、合同信息，点击页签切换显示相应内容。扫描卡片二维码，可在移动端查看卡片信息。

5、 图上支持统计展示资源面积、闲置面积、闲置率、流转中面积、交易价格指数等指标信息，可以从宏观层面了解全区资源概况。



1.6.1.4.集体资产发包“一键推送”

支持“一张图”上资产资源电子档案调阅。点击具体某一个村集体的一笔资产，可调阅到该资产的基本信息、面积类型、权属信息、交易信息、合同信息、预警分析等电子档案数据，可直接在图上发起“进场交易”操作，流转进江苏省农村产权交易平台的项目登记，实现农村各类型资产资源与农村产权交易平台的无缝对接，方便各级领导快速处置到期、逾期或闲置的耕地，实现集体资产资源交易应进必进，项目发包“一键推送”。

集体资产资源发包后，系统支持资产资源关联交易记录，允许关联多条交易信息，主要关联：项目编号信息、标段编号信息、交易信息、合同信息等。

1.6.1.5.资产全生命周期管控

引入地理信息技术和二维码技术，实行资产全生命周期“一图（码）动态监管”，通过自动整合汇总、监测分析，实现资产存量、结构、变动、交易、合同签订、收付款等全生命周期数据沉淀，包括资产日常所有管理相关功能：

1、 建卡：资产初始化后的资产新增；

2、 变更：变更申请单形式发起申请，审批通过后生效；

3、 处置：处置方式包括出售、转让、报废、清理、其他减少等，通过处置单的形式发起申请，审批通过后可进行处置，如出售，则推送产权交易平台；

4、 盘点：发起盘点，系统根据资产情况，生成系统盘点单，由用户根据线下资产清点情况与系统盘点结果进行比对，支持录入盘点结果。

1.6.2.“一户三权”融合管理

以集体经济组织成员为主体，以监管平台“一户三权”融合管理为手段，摸清股东成员、承包地、宅基地三项权益的关系，形成三权之间的交叉验证机制。聚焦群众反映问题较为突出的地区，汇聚相关信息构建权利、资金关系网，运用大数据预警分析技术，穿透式发现存在的遗留问题，有效保障集体经济组织成员合法权益。

1.6.2.1.集体经济组织成员资格认定

运用大数据技术，梳理三权在基层工作中存在的问题，落实研究成员资格认定、权益享受以及土地承包经营、宅基地取得、农村土地征收、基本公共服务、返乡落户配套改革等基层核心监管需求。建立集体经济组织成员认定体系，完善集体经济组织成员库，为“一户三权”融合管理筑牢数据基座。

1.6.2.2.“一户三权”台账管理

以组织成员为主体，明晰股权权属关系，记录股权分红历史信息，有效保障组织成员合法权益，推进股权有序流转。

与土地确权颁证系统、农村产权交易系统互联互通，以组织成员为分析主体，建立农村土地承包权、经营权管理台账，明晰土地承包权、经营权管理，维护村集体、组织成员和经营主体权益。

以组织成员为分析主体，与不动产登记数据对接，建立宅基地资格权管理台账和宅基地使用权管理台账。建立宅基地所有权与宅基地资格权、宅基地使用权的关联关系。各级管理部门、基层工作人员可以查看与宅基地所有权对应的宅基

地相关的宅基地资格权、宅基地使用权信息；组织成员可以查看名下的宅基地资格权或使用权信息。

1.6.2.3.“一户三权”动态校验

依托集体经济组织成员资格认定及“一户三权”台账管理，支持自动获取组织成员基本信息、家庭成员信息、产权信息，实现组织成员的股份、承包地、宅基地三类权利动态校验，对非组织成员占有权利现象预警，并将预警信息推送至村镇管理人员校验核实。

1.6.2.4.“一户三权”分析预警

1、 组织成员三权图谱：以农户为单位，关联组织成员信息、持股信息、分控信息、承包地与宅基地情况，建立组织成员图谱，构建组织成员、权利、资金关系网，直观展示成员三权信息。

2、 三权数据统计：针对集体经济组织，以农户为单位对每户持有的集体经济组织股份、承包地面积、宅基地面积总数以及人均持有数量统计分析。

3、 三权预警：针对成员信息错漏、没有股份、没有承包地、没有宅基地使用权和宅基地资格权的情况进行预警提醒。

4、 股权分红预警：结合农村产权交易数据，对有经营性资产收益没有进行股权分红情况进行预警提醒。

5、 宅基地预警：分析数据，针对一户多宅、超标占用、非集体经济组织成员占用等情况进行预警提醒。

1.6.3.电子权证服务

开发数据可查、权证可用的电子权证服务，工作人员通过后台管理端配置电子权证模板、预览电子权证、公示电子权证、修改电子权证、生成电子权证；集体经济组织成员可在农慧通小程序上查询到与自己相关联的农村土地承包经营权、宅基地资格权、集体资产收益分配权、股金分红等权证信息。通过推动个人农村土地承包经营权和闲置宅基地使用权转入集体经济组织统一发包，进一步提

升农户个人资产交易溢价率，发展壮大农村集体经济组织，保障农民股金分红的知情权。

1.6.3.1.电子权证后台管理

电子权证后台管理为基层工作人员提供电子权证信息展示、配置电子权证模板、预览电子权证、公示电子权证、修改电子权证、生成电子权证功能。

1、 通过区块链电子权证技术，对村民所在集体经济组织的股权分配情况以及村民股金分红情况做出全面展示。

- 集体经济组织总收支：展示村民所在集体经济组织的股权分配详情。
- 我家股份详情：展示农户的股本金额、总股数、集体股数、个人股数等详细数据，帮助农户及时进行股份股权的详情。
- 我家分红明细方案：展示农户每年度的股金分红具体明细方案。
- 我家分红发放情况：展示农户股金分红当前发放情况，并支持在线对资金发放进度督办。

2、 通过区块链电子权证技术，打造“我家承包地”模块，展示村民名下资产目前状态，包括基础信息，交易信息、委托信息、权属信息等。

- 我家承包地地基础信息：展示农户承包地的基础信息，如名称、四至信息等。
- 我家承包地交易信息：展示农户承包地当前交易信息以及历史交易信息。
- 我家承包地委托信息：展示农户承包地当前委托信息以及历史委托信息。
- 我家承包地权属信息：展示农户承包地权属信息。

3、 通过区块链电子权证技术，打造“我家宅基地”模块，展示农户名下宅基地权证目前状态，包括基础信息，资格权信息、使用权信息等。

- 我家宅基地基础信息：展示农户宅基地的基础信息，如名称、四至信息等。
- 我家宅基地资格权信息：享有宅基地资格权的村民，将在此模块展示村民宅基地资格权证，可申请宅基地面积等。
- 我家宅基地使用权信息：展示村民宅基地使用权证。

4、 电子权证模板配置：按国家及省市要求，统一设计电子权证样式，电子权证样式可通过系统管理进行模板配置，支持在线管理电子权证模板，包括上传、编辑、保存模板等功能。

5、 同步“一户三权”台账管理数据，系统可一键生成电子权证，支持对已生成的电子权证在线预览、修改、保存操作，支持电子权证打印。

6、 预览电子权证后，支持同步生成电子权证二维码，通过系统可一键公示电子权证，供组织成员扫码查验。

1.6.3.2.电子权证小程序服务

电子权证服务将上线在农慧通小程序上，为集体经济组织成员提供电子权证核验信息、电子权证查询查看功能。

1、 利用区块链、身份认证等多种后端能力，组织成员必须通过用户授权核身后才能访问电子权证服务；小程序根据核身结果，显示组织成员权证信息。

2、 组织成员可通过小程序查验电子权证，如发现权证信息错漏问题，可将需修改的信息反馈给村集体。

3、 股权电子权证：对村民所在集体经济组织的股权分配情况以及村民股金分红情况做出全面展示，调动村民参与村内事务积极性，可查看集体经济组织总收支分配、家庭持有股份、家庭分红等信息。

4、 承包地电子权证：展示村民名下资产目前状态，包括基础信息，交易信息、委托信息、权属信息等。

5、 宅基地电子权证：展示村民名下宅基地权证目前状态，包括基础信息，资格权信息、使用权信息等。

1.7. 同步建设安全保障措施

为落实“三同步”中“同步建设”要求，在项目建设阶段，保证以下安全技术措施的顺利准时实施，保证项目上线时，安全保护措施的验收和工程验收同步，确保只有符合安全要求的系统才能上线。

1.7.1.网络安全等保工作方案

本项目归集和存储的数据信息均涉及到相应的国家机密与个人隐私，因此方案在遵循国家电子政务总体框架和标准规范进行设计的同时，需要采取有效措施保证归集存储的信息得到有效地管理而不被泄露，防止各种恶意的入侵和破坏。

本次建设内容包括农村集体资产资源“一张图”、“一户三权”融合管理、电子权证服务，全部确定为三级安全等级。按照公安部、国家保密局、国家密码管理局、国务院信息工作办公室等四部门联合制定《信息安全等级保护管理办法》（公通字[2007]43 号文）要求，以及《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019），考虑到本项目应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

按照《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019），确定本项目建设的安全等级为三级（简称“等保三级”），应满足相应的信息安全防护要求，采用数据隔离、访问控制、加密传输、安全存储、剩余信息保护等技术手段，为用户提供端对端的信息安全与隐私保护，从而保障用户信息的可用性、保密性和完整性；并建立健全的安全防护体系，切实加强安全、保密和管理工作。

本项目按照信息系统安全三级等级标准要求进行规划建设，以确保安全。同时通过增强对系统环境的抗自然灾害的能力、加强网络设备管理维护、系统操作管理等手段来加以完善，尽可能将风险降低到能够被控制和管理的程度。

本系统实施过程中，将严格按照《中华人民共和国网络安全法》、《中华人民共和国数据安全法（征求意见稿）》以及《网络安全等级保护安全设计技术要求》等进行设计与开发。

系统完成开发并最终验收前，必须通过由第三方检测机构的系统上线测试和由相关认证单位提供的三级等保认证和上线测试报告作为系统终验的文档依据。

1.7.2.依托常州市电子政务外网安全体系

1.7.2.1.防火墙系统

在电子政务外网网络中，由于各结点在整个系统中的地位和作用各不相同，管理角色各不相同，可提供的信息资源也不相同，使用防火墙对各结点进行隔离，防范从系统外部和系统内部发起的攻击从而使系统整体的安全性大大提高。防火墙的配备对于增强外网网络与系统内网的安全会起到重要的作用。

1.7.2.2.数据捕获与入侵检测系统

入侵检测是网络安全非常重要的一个环节，入侵检测的原理主要是从计算机网络系统中的若干关键点收集信息，然后对收集到的这些信息进行分析，通过对息的分析来监控网络中是否有违反安全策略的行为或者是否存在入侵行为。入侵侦测系统是网络安全侦测的最后一道防线，它不仅能对包括内部攻击、外部攻击和误操作等进行实时监控，还能对系统进行监视、安全审计，对各种攻击进行甄别，同时提供反攻击等多项功能。因此它是网络系统安全措施的一个补充，更是网络安全防御体系的一个重要组成部分，在网络安全技术中扮演着不可替代的重要角色。

入侵检测的基础是首先对流经电子政务外网的网络数据进行数据捕获分析，并根据分析结果进行类别网络访问行为是否合法并采取下一步行为的辅助系统。在本项目的建设中建议采用诸如多个相关事件、相关协议的综合分析的方法，形成具有高级分析技术的一套完整的入侵检测系统。

当入侵检测系统检测到攻击时，系统会自动记录攻击情况，然后通知网络管理人员，同时该系统会自动和防火墙联动起来，并发出指令及时切断对的网络攻击。

1.7.2.3.脆弱性扫描系统

脆弱性扫描系统的工作原理是通过将扫描系统本身的漏洞库何网络或主机

的配置信息进行比对分析，这样来扫描出系统的脆弱性。引入脆弱性扫描设备将对增强整个系统的安全性起到重要的作用。

1.7.2.4.信息加密系统

电子政务外网网络作为涉及国家秘密的网络，需要采用国家许可的加密设备来保证系统的安全性。因此在加密设备的选购上必须严格按照国家有关规定，选用通过国家许可的加密设备。

加密系统的作用是对在广域网上传输的数据进行加密，以保证数据的机密性和完整性，防止不法分子窃取和篡改数据。加密系统可以分为二个部分，包括加密机、管理中心。

1.7.2.5.病毒防护及故障恢复系统

几乎所有的网络安全中都存在着病毒的问题，当前网络建设的发展迅速，日新月异的推广着各种网络应用，病毒的扩散出现了新的特征。因此对病毒防治的问题就成为了电子政务外网建设中需要特别关注和重点考虑的问题，所有电子政务外网的安全保障体系必须相互结合、相互协同，构建出的防护体系要求必须是立体的。对于电子政务外网，重点考虑网络防病毒系统。

当系统遭受病毒侵害不能正常工作或者其它一些原因导致系统不能正常工作时，故障恢复系统则是一个必须的选择。所以在电子政务外网安全方案中故障恢复系统也是至关重要的。

1.7.2.6.安全审计系统

安全审计系统是安全保障体系的一个重要组成部分。它对合理的搭配安全防范措施起到很好的指导作用。安全审计系统主要完成一些功能和任务：

- 支持基于 PKI 的应用审计，在有策略配置的指导下，对信息系统产生的数据进行实时或定时采集，并将采集到的相关信息进行有效的转换和整合。
- 支持基于 XML 的审计数据采集协议。
- 提供灵活的自定义审计规则。

- 提供系统审计和网络审计服务。

1.7.2.7.信息安全防御系统

信息安全防御系统是政务外网上基本安全防护系统的重要组成部分，它的一个重要的核心就是 WEB 信息防篡改系统，它的主要任务就是监控 WEB 服务器和应用服务器上的文件目录，并通过可信部署进行合法更新。

信息安全防御系统在功能上必须能够支持诸如：Windows 系列、UNIX 系列、LINUX 系列等多种操作系统，还要必须具备非常高效的信息扫描速率，同时还不能够影响到服务器的工作效率。具有集成发布与监控功能，使系统能够区分合法更新与非法篡改等等这样一些功能和作用。

1.7.3.应用服务安全防护内容

1.7.3.1.Web 安全防御

采用安全资源池提供的虚拟应用防火墙，对访问 WEB 应用的网络流量进行安全检查，一旦发现攻击行为立刻中断连接保护 WEB 服务器的安全。

1.7.3.2.Web 漏洞扫描

采用安全资源池提供的虚拟 web 漏洞扫描系统，对部署在 vpc 中的 WEB 应用系统进行漏洞检测，及时发现 web 应用系统存在的安全漏洞并提供修复建议。

1.7.3.3.网页防篡改

采用安全资源池提供的虚拟网页防篡改系统对部署在 vpc 中的 web 应用系统进行网页篡改监控，一旦发现网页被篡改，及时报警并采取恢复措施。

1.7.3.4.增强认证

应用系统用户口令基本要求由口令长度、口令字符复杂度和口令最长有效期

限组成。

- 口令最小长度：8 位；
- 口令字符组成复杂度：口令由数字、大小写字母及特殊字符组成，且至少包含其中三种字符；
- 口令最长有效期：系统口令最长有效期限为 90 天。

1.7.3.5.用户角色权限管理

本项目正式验收前，需要严格管理用户角色权限。武进区农业农村局拥有应用系统管理的最高权限，为运维单位开放应用系统最小权限，每当运维单位需使用其他权限时，必须向最高权限拥有者提出权限申请。

1.7.3.6.业务行为审计

业务行为审计系统获取、解析网络流量，提取业务操作用户、业务操作内容、业务操作行为，根据设定的安全监控策略，判断业务操作用户是否为授权用户，业务操作内容和操作行为是否在授权范围内。如果业务操作用户、业务操作内容、业务操作行为违反授权策略，则阻止业务操作用户针对业务内容的操作行为。

- 业务操作用户识别

从网络流量数据中提取 IP、主机名、账号、邮件接收地址，通过这些信息，关联到真实用户名称、部门名称。

- 业务操作内容识别

不同的业务类型，业务项可能是菜单、菜单项、表单、功能按钮、页面、输入框，从网络流量数据中提取业务操作的具体业务项。

- 业务操作行为识别

从网络流量数据中提取业务操作行为，根据操作行为时间先后，形成业务操作行为序列，还原业务操作人员的操作场景与操作过程，如：下载了某个文件、删除了某个文件、修改了耨各业务数据、提交了某个业务表单、完成了某项业务的授权等。

1.7.3.7.代码安全审计

软件开发通常会引入安全缺陷，平均的缺陷密度为 6 个缺陷/KLOC，假设 1%的安全缺陷是可被黑客恶意利用实施攻击的，则一个业务系统软件大概存在 3-6 个可被利用的安全漏洞。

采用源代码静态分析技术，自动将获取到的被测软件源代码在相应的编译环境中进行编译，再通过数据流分析技术、符号执行技术、内存精确建模技术等分析并检查源程序的语法、结构、过程、接口等来确定源代码的安全性。

1.7.3.8.网站安全监测服务

提供网站云检测服务、漏洞扫描服务、网站安全验证服务、应急响应服务、渗透测试服务、漏洞修复整改跟踪服务、网站安全预警通告服务、网站失陷检测服务、网站安全攻击事追踪溯源服务。

1.7.4.数据安全保障方案

1.7.4.1.数据隔离措施

在网络拓扑结构安全中，可采用网络监控与入侵防范解决数据传输安全问题，通过防火墙防护技术和隔离网闸进行数据的有效隔离。整个系统网络部署架构分为三层。在最外面一层是互联网层，主要提供集体经济组织成员用户访问电子权证。中间层是电子政务网 outside 区域，主要部署本次建设的应用模块。第三层是电子政务网 inside 区域，主要部署业务数据存储。

1.7.4.2.加密传输措施

政府机构要按照国家相关政策要求，在现有网络基础上构建起内部专属网络，并通过对加密技术与认证技术的运用，对数据传输安全性进行保证。同时政府机构还要做好信息传输加密处理，要通过对 IPsec 以及其他加密手段的运用，对数据传输过程形成有效保护，从而有效防止数据在传输过程中出现被篡改的情

况。

由于本项目需要与其他系统进行交互，因此需要保证各种级别的数据传输安全性，要求系统在平台及平台以上级别均需提供不同层次的数据加密,数据传输时必须进行加密处理。

1.7.4.3.数据存储安全

数据信息存储介质包括：纸质文档、语音或其录音、输出报告、硬盘、磁带、光存储介质。存储介质管理须符合以下规定：包含重要、敏感或关键数据信息的移动式存储介质须专人值守。删除可重复使用存储介质上的机密及绝密数据时，为了避免在可移动介质上遗留信息，应该对介质进行消磁或彻底的格式化，或者使用专用的工具在存储区域填入无用的信息进行覆盖。任何存储媒介入库或出库需经过授权，并保留相应记录，方便审计跟踪。

本项目涉及敏感数据存储（账户信息、组织机构信息、个人隐私信息等），需对数据库中敏感数据进行加密存储，使用数据脱敏技术对敏感信息进行模糊化处理。敏感数据在数据写入存储介质前将数据进行加密，实现数据的存储加密；在从存储介质加载数据到内存前进行数据解密，实现数据的解密使用。

1.7.4.4.数据库安全配置

本项目使用 MySQL 数据库，为保障数据库的安全运行，在数据库安装和运行过程中，必须完成以下配置工作：

1、消除授权表的通配符

MySQL 的访问控制系统是通过一系列所谓授权表进行运作的，这些授权表使我们能够在数据库、表和列水平上定义每一位用户的访问级别。而这些表也能够让管理员授予某用户普适许可(即总是允许)或授予表使用通配符的权限，这样做相当危险，因为黑客有可能会使用一个被盗帐号来获取访问系统其他部分的权限。因此，在分配用户权限时要谨慎行事，做到准确无误，并且始终确保用户获得的访问权限恰好足够他们完成任务即可。此外，还要谨防给个人用户分配 SUPER 特权，因为这个级别的权限允许用户操纵基本服务器配置并访问所有数

据库。

2、使用安全密码

只有在使用密码的情况下，用户账户才能得到安全保障。因此，当你安装MySQL时要做的第一件事就是给MySQL的根账户设置一个密码(默认情况下密码为空)。当你堵住这个大漏洞之后，下一步就是要求每一个用户账户都设置好自己的密码，并确保没有使用具有启发式信息的容易被识破的密码。

3、对客户端服务器传输进行加密

在MySQL的客户端服务器架构(对于任何此类架构也是如此)中，关于在网络中传输数据时保证数据安全的问题非常重要。如果客户端服务器事务是以明文(信息未加密)的方式进行的，那么黑客很容易就能发现这些传输中的数据包，并从中获取敏感信息。可以激活MySQL设置中的SSL，或者使用OpenSSH这类的安全外壳实用程序，以便为通过的数据创造一个安全的加密通道。通过这种方式对客户端服务器连接进行加密，未经授权的用户就很难读取这些不断在通道中往来传输的数据了。

4、禁用远程访问功能

设置服务器使用了--skip-networking选项启动，这样做能够屏蔽MySQL的TCP/IP网络连接，并确保没有用户能够远程连接到系统。

5、积极监控MySQL的访问日志

MySQL里具有很多不同的日志文件，用来记录客户端连接、查询和服务器错误。其中最重要的就是通用查询日志(general query log)，其中以时间戳记录了每一个客户端连接和断开连接，并记录了客户端执行每一次查询的情况。如果你怀疑MySQL出现了不寻常的活动，例如和网络侵入有关的活动，那么最好对这个日志进行监控，往往就可以查出此类活动的源头。

1.7.4.5.数据库审计

使用专用文件或数据库，自动将用户对数据库的所有操作记录下来，包括用户审计和系统审计。用户审计记录所有对表或视图进行访问的企图（包括成功或不成功的），以及相关的用户名、时间和操作代码等信息，将这些信息记录在日志中。系统审计由数据库管理员进行，审计内容主要为系统一级命令和数据对象

的使用情况

1.7.5.数据库备份方案

1.7.5.1.备份原则

为了保障系统的数据，不影响中心正常的业务，应当制定一个严格的工作制度，规范化数据库维护与备份的工作流程。

数据库管理员应当按照以下原则进行数据库系统的维护与备份：每日值班的数据库管理员应当随时监控主数据库服务器、备份数据库服务器的软件、硬件的正常运行，一旦出现故障，应立即向领导汇报并采取相应恢复措施；管理员应当每日察看数据库的冷备份报告，出现问题及时检查备份文件，保障每日数据库服务器的备份正常运行。

当主数据库服务器出现数据库错误时，应检查数据库的工作状态。如果工作不正常应及时将最新的备份数据覆盖当前数据库的损坏数据，并重新启动机器，检验数据库系统是否能够自行恢复运行。如果重新启动后数据库系统不能正常运行，则数据库系统文件被破坏，应重新安装数据库并启用紧急恢复方案。

当主数据库服务器出现硬件故障时，应在 1 小时内更新备份数据库为最新数据，并启动备份数据库服务器，将备份数据库服务器升级为主数据库服务器。对于损坏的主数据库服务器应重新安装数据库，并启用紧急恢复方案。

当备份数据库服务器出现数据库错误时，应检查数据库的工作状态，如果工作不正常应及时将最新的备份数据覆盖当前数据库的损坏数据，并重新启动机器，检验数据库系统是否能够自行恢复运行。如果重新启动后数据库系统不能正常运行，则数据库系统文件被破坏，应重新安装数据库并启用紧急恢复方案。

每周至少一次将备份数据转移到移动磁盘内，以防止出现自然灾害的事故而导致的备份数据丢失。

1.7.5.2.备份方式

正确的备份策略不仅能保证数据库服务器的 7×24 小时的高性能运行，还能

保证备份与恢复的快速性与可靠性。在制定备份策略时，需要考虑备份窗口、最大备份数据源、总数据量、更新的数据量、备份方式、业务特征、网络传输速度等因素。

目前，本系统需要7×24小时连续在线服务，并且经过多年的运行，具有一定的数据量。通过分析MySQL数据库存储结构、数据库的运行方式，结合MySQL几种备份方式的优缺点和，制定了如下备份策略：

1、差异备份方式

差异备份策略包括执行常规的“完全备份”加“增量备份”。具体过程为。第一次执行数据库的“全备份”完全备份数据库。然后每天或定期做一次“增量备份”。一段时间后再做一次完全备份，如此反复。策略具体如下：

（1）采用MySQL提供的Mysqldump备份工具与完全备份、增量备份、逻辑备份相结合的方式。

（2）创建主服务器到备份服务器之间的安全通道，用于备份数据的安全传输。

（3）备份触发方式：定时启动计划任务。根据业务特点，确定备份周期．执行备份方案。

2、自动备份

若采用手动备份则需要系统管理员定时地进行手工操作。这种方式无形中增加了管理员的工作量，同时也增加了备份过程中因人为错误而导致的损失。本项目将基于服务器操作系统，采用自动备份方式完成数据库备份工作。

1.7.5.3.日志、控制文件备份

由于日志和控制文件是数据库在恢复时不可缺少的组成数据，应当在做数据备份时进行同步日志和控制文件的备份。为了确保安全，建议日志和控制文件备份到与数据备份不同的物理介质上。对于备份时间和备份调度，建议一天一次，同样调度在系统闲时。由于日志和控制文件起到了增量恢复的作用，控制文件的备份点应当比数据文件的备份点多。由于控制文件小，不会占用系统资源，建议在重要的业务数据操作时间点之后紧接着进行备份。要选择比较重要的数据处理节点，进行日志和控制文件的备份。