

# 明道技术安全白皮书

2017.9



# 明道技术安全白皮书

2017年9月

信任是商业的基石，透明度是信任的来源。明道藉由五年多来的SaaS产品安全运营里程和团队的运营经验，特别撰写此简明扼要的技术白皮书，一方面为自己建立持续的自律，其次为建立用户对明道及SaaS行业的信任，再次可以为同类产品的运营提供经验参考。本白皮书略去了繁冗晦涩的技术词汇，但保留了关键细节，所以即使非技术人员也能够顺畅阅读。

有关此白皮书的疑问，可以根据文末署名联系明道团队。

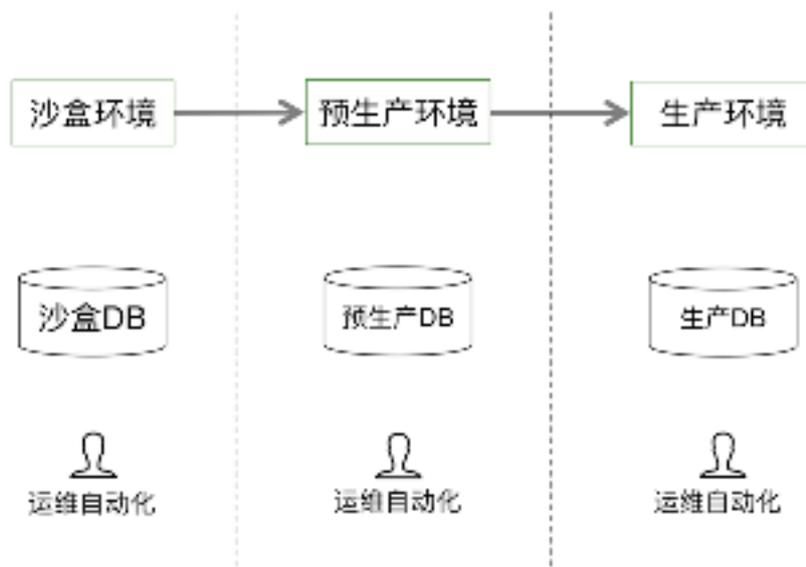
# 1. 运维流程和制度

安全运营的首要来源是人，而不是技术与设施。人之不完美是安全事故的主因，其不完美来自管控缺失下的自律丧失和非故意的疏忽差错。因此，云服务的运维流程和制度应当首先着眼于最小化来自人的风险。

## 1) 减少不必要的生产数据接触

在针对人的管理工作中，成本最低，也是价值最大的在于减少不必要的生产数据接触。明道将开发，测试使用的应用数据和提供正式服务的生产数据完全隔离，保证绝大多数的技术人员和工作无须接触真实的生产数据。在实践中，将接触生产数据的员工减少到五人以下，其中包括CEO、CTO、主管开发工程师和运维工程师。这样可以保证任何运维数据事故的责任检查范畴大大缩小。

利用开发和测试服务环境完成完美的代码发布，需要精密的协调，对发布系统的反复测试。确保沙盒类系统和生产类系统的环境一致性。明道至少维护了和生产数据环境一致的三套沙盒系统，并支持生产环境变更后的快速回滚（数分钟之内）。



## 2) 独立的密码管理和接触日志管理

- 生产数据环境下的运维工具等IT设施均需要设置强密码，专门人员管控密码表，密码按一定周期更换，数字符号多重加密并通过专门工具生成；主机和数据库的访问通过更加安全的密钥对登录方式，并配置有严格的防火墙策略。
- 指定电脑，在指定地点和IP地址，才能访问生产数据主机；
- 需要两人以上的登陆授权才能访问生产数据主机；
- 所有服务器登陆情况均有日志记录，信息安全小组成员会收到短信通知，非正常和非授权登陆支持一键踢出。

## 3) 运维人员的审查

所有从事运维工作的成员（包括非专业运维岗位）均需要通过严格的入职审查，包括历史职位的背景调查，信用报告和无犯罪记录证明。尽管因为疏忽此工作带来的事故属于低概率事件，也应该坚持执行。

## 4) 变更和发布流程规范

涉及生产数据环境的所有技术变更（包括代码、存储路径、主机环境等）均需要经过审批和记录。代码发布需要使用专门的运维工具来进行（避免工程技术人员直接操作主机），利用运维工具实现可靠的回滚，避免任何人为疏忽带来的数据损害。

正式版代码发布前应当实现在沙盒环境中进行完整的测试，特别重要的更新还应该利用灰度发布在10%以下的用户群中进行试运行。

## 5) 通过ISO27001-2013 信息安全质量认证



## 2. 系统架构

### 1) 业务数据访问平台化

为减少生产数据和主机的接触，绝大多数的数据操作均不能通过主机访问来完成。为此，公司开发了一系列平台来实现可控的数据接触和操作，包括：代码发布系统，数据备份操作，用户信息查询，账务处理等。这些平台工具限制了内部员工批量接触数据，并留下所有的操作日志，杜绝了因为人为疏忽带来的重大数据泄漏和损害。

### 2) 用户数据存储的隔离设计

为进一步防范数据泄漏和损害带来的后果，明道有意进行了数据结构设计上的加强。其原则在于尽可能分离物理数据存储，不仅通过分库分表，还根据业务需求选择使用完全不同的数据库选型，例如对于全文数据使用了没有明码表达的客户ID信息；其他数据库也根据用户ID信息和内容信息隔离存储（知道内容了也不知道是谁的）；敏感核心数据进行加密存储。在任何情况下，单库和单表的泄漏不会造成实质性的隐私侵犯。

除了ID和内容的隔离，明道企业版还贯彻了不同客户数据的物理隔离，这个措施同样大幅降低了数据整体泄漏的风险。即使在为检索服务而建立的临时索引数据中，明道还加入了扰动(scramble)数据。

读者不必因为本措施提到了数据泄漏而感受到不安，在信息安全领域，每一项安全措施都是独立的，它们叠加在一起指数级地降低系统风险。

### 3) 冗余系统

为保证产品的可用性，明道的绝大多数子系统均有冗余系统，甚至分布在不同的物理位置。Web服务的冗余系统切换几乎是无缝的，系统在数十秒内即可判断系统失败，从而转移到

正常节点。如果遇到运营商问题，明道可以在数十分钟之内在异地激活备份系统。在极端情况下需要使用冷备份系统（历史较久的文件存储），明道也能够通过逐步恢复数据的方式来尽快恢复服务。

因为受制于多家服务商和通讯网络可靠性的限制，明道单产品并不能确保100%的可用性。但实践上，在近一年的运营中，明道保持了99.95%以上的正常服务率。

#### **4) 安全传输协议**

在所有的用户访问中，均强制使用SSL安全连接（RSA-SHA256签名算法），确保数据和密码传输过程中的安全。

#### **5) 软件安全设计**

除了基础物理设施的安全考量以外，产品对于安全方面的设计也是必不可少的。在明道，用户的密码必须使用强密码规则，防止撞库被暴力破取，同时如果多次输入错误密码账号将被锁定一段时间；支持微信登录提醒，防止他人盗取账号之后的提醒，一旦发现异常提醒建议迅速修改并加强密码；敏感操作，需要再次输入登陆密码进行二次确认；不同模块的权限设计，比如管理员、审批、考勤等配置，防止越权操作；手机APP支持手势、指纹识别登录，防止手机被他人使用，存在一定的操作风险。

## 3. 云计算基础服务

### 1) 服务商的评估和选择

明道的云计算基础设施服务商选择按照同类冗余的原则进行。在云主机类服务中，目前的服务商包括阿里云和优刻得（UCloud），存储和CDN服务类选择了七牛和又拍云。同类冗余的目的是为了保证关键服务在两家服务商都出现严重故障时，依然可以通过明道的调度来恢复服务，尽管近两年来IAAS服务商的可靠性已经有了基本的保证，这一设计能够让明道的可用性保持更高的水平。

所有的云计算服务商均需要建立直接的运维沟通通道，确保在故障发生的时候能够高密度沟通。

### 2) 服务监控和告警

除了主机服务商本身提供的监控和告警服务外，明道还架设了在业界使用较多的Zabbix开源监控方案，此外还使用了监控宝作为第三方监控。监控和告警覆盖主机资源、端口、服务、性能等纬度。告警手段包括了微信、短信、Email和电话。在故障超时设置触发时，运维团队多人都能够同时收到告警。

### 3) 第三方安全服务

近年来，第三方安全服务已经日益丰富，除了IAAS公司标准的防火墙服务、防DDoS攻击以外，明道还采纳了“实时入侵检测”和“渗透测试”服务，其中渗透测试由乌云机构的专业白帽子成员组成。渗透测试一般由技术高管独立委托，在不通知运维成员的情况下进行，以准确检测当前防范措施的可靠性。

## 4. 数据备份

所有的用户数据均有独立的热备份和两套冷备份。热备份系统同时应用于业务系统，数据的同步延时在1秒以内。在遇到可用性问题时，用户数据完整性的体验接近100%。

系统同时配置了冷备份系统，并带有一定周期内的时间胶囊功能，能够按照指定时间恢复数据。两套冷备份部署在不同的物理位置（同城与异地机房），以实现灾难备份恢复。数据备份的传输也需要在安全连接下进行。

## 5. 缺陷管理

尽管缺陷管理更多是和软件质量有关，但明道将缺陷汇报中的安全类问题（比如有关数据修改和删除操作的bug，数据权限不当的bug等）升级评估，提高它们解决的优先度。

以上五个部分反映了明道SaaS软件的技术安全工作分布。尽管没有100%绝对安全的系统，但我们始终着眼于为用户提供第一流的产品安全支撑。当前明道的技术安全工作所能够提供的安全质量绝不亚于任何企业私有云系统。而且因为大量用户的分摊，每个用户并不需要为高等级的安全服务支付额外的成本。明道在运营五年多来始终保持了完美的安全记录，没有发生任何数据泄漏和明显的数据库损害事件，这得益于我们从第一天开始就坚持的安全优先原则。SaaS产品的确要比任何企业自建的信息系统要安全得多。

近年来，我们的技术安全工作和成果陆续得到了很多客户的肯定，包括来自金融，政府等领域的标杆性客户。只要能够继续增强安全性的投入，明道都会第一时间来评估。欢迎用户的持续监督和进一步的改进建议。

本白皮书撰写和联络：

明道CTO 金可伟 (jerry.jin@mingdao.com)