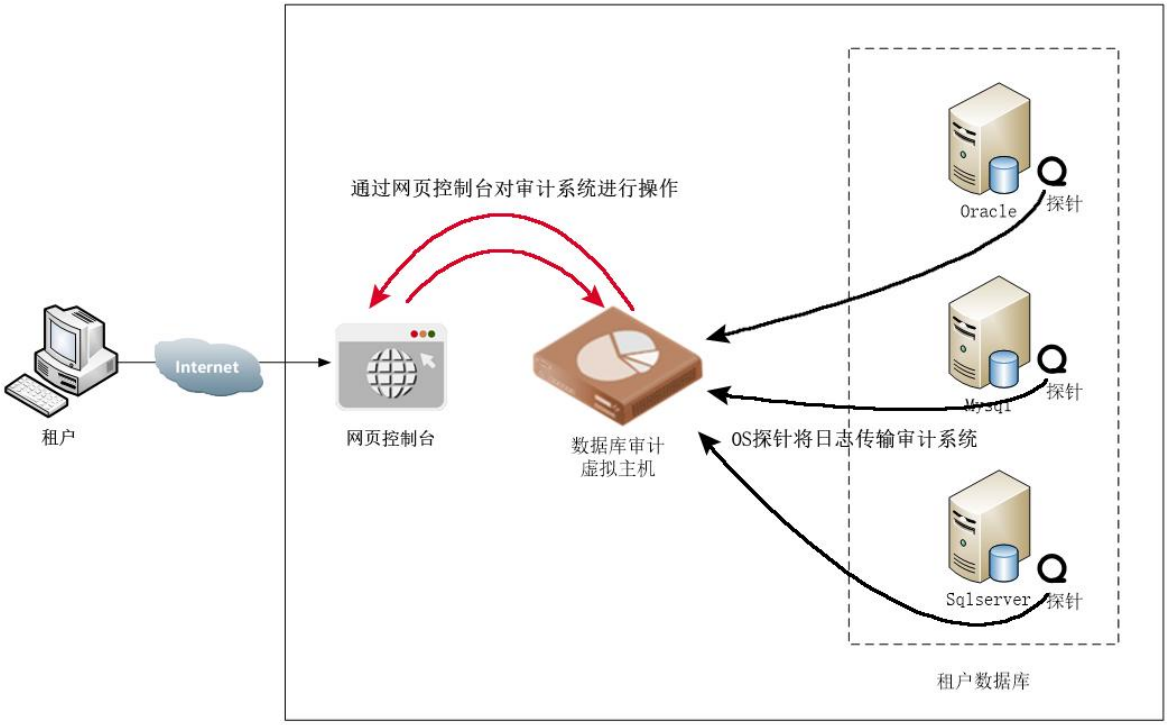
某银行私有云数据库审计项目

1、项目背景

随着全球信息化的发展，云技术得到了快速发展，某银行六年磨一剑，成功建设“新一代”核心系统，为全行未来转型发展与核心竞争力的提升打下了坚实的基础：1.建成国内金融业规模最大的私有云，率先实现数据中心云化；2.自主研发“云管理平台”，成为行业云计算应用的风向标；3.实施落地私有云战略，逐步建立行业生态系统，成就大型国有商业银行金融科技产品共享的首推之举。



建行公有云

在该私有云系统中，有大量的敏感信息，外部黑客、企业租户、数据库维护人员都有机会利用数据库存在的漏洞以及自身拥有的

高权限，直接获取敏感客户的隐私信息。数据库作为私有云的核心和基础，承载着越来越多的关键业务系统和企业的敏感数据，逐渐成为某银行私有云系统中最具有战略性的资产，数据库的安全稳定运行也直接决定着租户的系统能否正常使用。

因此，加强企业数据信息安全保护，既是某银行自身发展的客观要求，也是为了满足行业监管的需要。

2 、技术方案

数达安全提供的云数据库审计产品，可为私有云环境下租户数据库提供访问审计功能。相比银行内网私有云环境，在虚拟化环境下将必要的数据库流量进行审计，在具备高精确度的审计能力条件下，最大程度减小对租户及云环境的性能消耗。

私有云企业租户选装数据库审计模块，实现有效审计和管控企业租户自身的数据安全。采用 OS 探针部署的方式，通过在云平台中部署审计云服务器，在数据库系统部署 OS 探针，将数据库日志信息传输到企业租户云端审计系统，由租户进行管理和分析。这样可做到对企业租户数据库的访问活动进行全方位的监控与审计，对数据库所面临的风险进行多方位的评估，并提供事后追查机制。

租户选装数据库审计系统，有效监控私有云下企业租户的内部人员对数据库访问行为，租户可以实时、准确掌握自身数据库系统的安全状态，及时发现企业内外部人员和 web 系统违反数据库安

全策略的事件，实时记录，并且实现安全事件的定位分析，事后追查取证。

3 、方案价值

1）企业租户数据安全风险可视化

各租户可了解自身数据资产的分布，自动发现数据库服务器、敏感数据的分布情况，为后续安全加固明确目标；

实时掌握自身数据库系统的可用性。能对数据库运行状态进行实时监控，在状态异常时进行预警，提前防止业务瘫痪，保障业务系统的连续可用性；

实时掌握自身数据库存在的风险状况。要求能通过扫描的方式，评估企业数据库系统的风险，扫描内容包括：弱口令检测、系统漏洞、配置风险等；

进行数据活动监控，实时监控数据活动情况，记录数据访问行为，尤其是租户运维人员对敏感数据的访问行为。同时要求能实现对数据库的直接访问及通过 Web 和应用对数据库的间接访问进行全面监控。

2）数据的安全合规，帮助租户通过各种安全检查和测评。

比如等保、分保测评，以及金融行业法规标准的要求。

等保在云计算环境中有明确要求：

应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。

《中国银行业十三五信息科技发展规则监管指导意见》文件中明确提出综合运用多因素认证、访问控制、边界防护、泄密检测、密码算法和技术、数据脱敏和安全审计等手段，切实提高客户身份认证和验证强度，防范敏感数据泄露、篡改、丢失和非授权访问等风险。