基于业务视角的混合云平台可观测系统建设

莫剑锋 赵 磊 刘惠航 吴文鹏 黄信信

（南方电网数字平台科技（广东）有限公司）

摘要：随着信息技术的迅速发展，混合云也逐渐成为云计算的重要模式组成，混合云平台技术具有计算及存储能力等，其在我国多行业、领域应用广泛、灵活。但是在混合云平台高速发展的同时，信息安全也越来越引起人们的重视。因此，为了提高混合云平台的安全性，保障云平台运行中的安全，对混合云平台的监控十分重要，由此需要对云平台的可观测系统进行建设。

关键词：混合云平台；存储；信息安全；监控；可观测系统

引言

随着我国时代的不断发展，信息技术的发展更加迅猛，越来越多的用户既想将数据信息储存到私有云中，同时又想获取公有云的信息资源，因此将私有云与公有云互相结合形成混合云平台，混合云平台的建设与应用越来越普及，对云平台的安全性要求也不断增加，对混合云平台的构建与安全性进行监控，使用科学的可观测系统构建安全的混合云平台，因此，保证安全的混合云平台建设对个人或者企业都至关重要。

一、混合云平台建设现状

云平台是基于“云”服务的计算平台，是通过云计算为硬件资源与软件资源提供服务，其具备计算、网络和存储能力。云计算平台主要分为：以数据存储为主的存储型云平台，以数据处理为主的计算型云平台以及计算和数据存储处理兼顾的综合云计算平台。云平台使用虚拟软件将硬件资源虚拟化，进行管理及应用，用户可以按照自己的需要选取资源、应用和服务，其具备自动调节资源的功能，有优越的拓展性，可以灵活的控制资源的增减，降低用户在硬件维护过程中的成本，保持系统运行过程中的稳定。

混合云平台是将个人私有云与外部公有云相互融合，完善了云平台，涵盖私有云与公有云的优点，打破了私有云的硬件限制，提升了云平台的拓展性，提高云平台的运算能力，混合云平台是目前的发展的主要方向及主要的应用模式。公有的基础设施服务中，用户一般可以使用云计算访问计算、网络、存储资源。在进行混合云平台建设的过程中，工作人员需要将可利用的网络技术或者将虚拟化服务以专线的方式给用户服务。混合云平台的服务功能是混合云平台建设中的重要内容，用户可以选择合适自己的云平台建设数据库，进行云网融合，搭建完整的多业务平台。软件是云平台建设的重要载体，用户可将软件安装在自己的服务器，通过网络获取应用程序。数据是混合云平台的核心要素，通过建设独立的网络环境，使用接口及算法，以此完成数据的分析及处理。使用计算、网络、编排等与服务器进行对接，建设虚拟的环境，对云计算平台进行优化，扩大数据库等资源，由此进行平台的构建，提供混合的云服务。混合云有利于为用户及企业提供所需要的外部扩展，使用公有云的资源丰富私有云的数据资源库，混合云可对高负荷工作进行预处理，私有云可以执行公有云安排的工作任务，公有云引出了如何在公有云与私有云之间的程序的复杂性，因此要考虑数据及资源两者的联系，如果数据少，需要将数据传送到公有云进行处理。混合云包含了私有云及公有云，私有云主要是针对企业用户，公有云主要针对企业，一般来说，大部分的用户为了保护自己的隐私等，更倾向于将个人数据放在私有云，但是在工作的时候又需要获得公有云的数据资源支持，因此，混合云平台的的建设很好地将两者相结合，以获得合适的方案。混合云一般采用先进的集群、负载均衡与容错技术等，保障了云平台的安全可靠性能。使用云平台网络组成的数据计算系统，提升了云计算的可用性能，同时具备了安全性，这是不同于普通的计算机系统，且优于计算机系统。云计算可以根据用户的具体需求，从云端上获取所需要的的资源，同时，可在计算机上根据需求的不同构建不同的程序系统，并且这些程序可以支持用户的其他应用。云平台可以支持用户在任意的地方获取系统应用，资源均来自于云端，而非计算机内本来就有的软件。混合云平台具有强大的规模，可以帮助用户准确、迅速、方便的获取所需要的资源，且在应用过之后可以释放资源，减少了浪费。混合云平台的主要业务包括：数据延伸、工作转移、平滑迁移、统一管理等。混合云的实现与网络相互贯通、相互融合。当前，常见的云厂商有：阿里云、腾讯云、华为云、UCloud、京东云、百度云以及国外的 AWS、Azure、Google 云等；而一般私有云无非就是 OpenStack（开源），或者 VMWare（收费）。

二、基于业务视角的混合云平台可观测系统建设的必要性

混合云平台建设的信息安全所涉及的种类多，针对不同的种类，不同的技术有着特定性、专一性、针对性，为了使得云平台的信息安全得到保护，因此需要对云平台进行统一、整体的保护。云平台的信息安全保护包括

了信息安全保护及实时监测等多方面。云平台的信息安全保护内容主要是云平台的数据，包括了信息数据存储、应用安全等。为了预防云平台中的数据被盗取或者被攻击，因此需要定期对云平台的防盗系统进行更新、修复、优化等，同时，需要实时监测云平台，以阻止云平台运行过程中出现的漏洞、问题等，并可以及时的处理，同时，也要对用户的使用行为进行监督检测，防止网络病毒等的攻击。当前的混合云平台信息安全保护系统还不够完善，不能对出现的问题及漏洞等及时避免，因此需要采取新的技术手段对云平台的数据进行保护，确保云平台的安全性，同时，可使用数字加密对数据信息进行保护，保障用户及企业的隐私，在对混合云平台的数据保护时，可以将防火墙技术、数据加密技术、入侵检测技术技网络监控技术等进行应用，可以对云平台进行有效防护，并且通过与其他的技术之间进行合作，同时保障云平台建设的技术安全。在进行云平台管理时，应该不断的加强管理人的技术培训与工作能力，确保云平台各功能的充分利用，最后确保云平台信息安全。入侵检测是对云平台没有授权的用户进行安全检测，这样可以防止黑客、病毒等对云平台的入侵。如果黑客等通过系统中的漏洞入侵到平台，入侵检测可以对其进行检测与拦截，如果有非法的 ID 注册云平台，可以将其列入黑名单，保护其他用户的安全。入侵检测可以处理云平台中未授权但是出现数据使用，这样可以为云平台的安全性进行保障。网络检测指的是使用网络软件与硬件对云平台的网络安全进行监控，表现为监控云平台的流量及压力等。

混合云平台的不安全性主要有：数据信息的泄露、损坏或丢失，通常表现为数据未经授权被访问、下载、复制等，导致信息泄露，如果是企业机密被盗取、泄露等，给企业带来巨大的经济损失。云平台使用大数据、云计算等进行数据的分析处理，但是在数据的传输过程中也会遭受到一些非法监控等，用户及企业的私密信息被泄露。数据信息的存储是以云平台为基本依托，使用信息技术对数据进行处理，处理过程包括了用户的信息，但是处理过程中系统的整体安全保障性能较低，存在着被侵袭、攻击等的风险，致使数据信息被泄露。云计算的时候，云平台被不法分子攻击，用户信息被修改等。因此，云平台技术的发展对数据信息安全的影响相当重要，其对云平台系统的风险抵抗及防护能力有着决定性的作用。

混合云平台是以信息数据为中心，危险主要来源于信息安全，但是信息安全是不断变化、运行的，因此对云平台的信息安全保护体制不断更新、维护等，但是即使如此，也不能百分之百的保障云平台信息安全，因此，需要对混合云平台的安全性进行重视，采取有效的管理方式及手段对信息安全进行保护，使用科学的方法对信息安全进行预防，如此以来，可以保障云平台管理系统安全、稳定的运行。云平台中复杂的系统对系统的性能有着更高的要求，复杂同呈现出了更加复杂的调用关系，如图 1.1 所示。

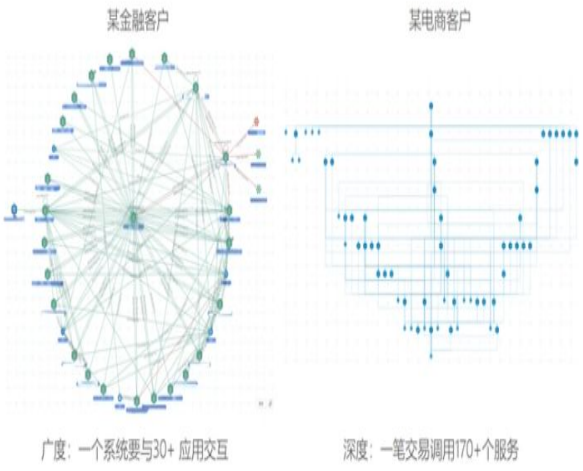

图 1.1 混合云平台系统示意图

在网络的发展过程中，衍生出了多种监控方式，传统监控只能监控一定范围内的数据信息，通过监控的数据判断出系统的运行状态，然后根据数据的聚合、异常检测等原因分析判定出问题的原因，但是由于数据割裂、监控范围等原因的限制，当出现故障的时候不能苦熬苏找出原因，因此，需要借助可观测性进行辅助监控。可观测性是一种通过检查系统中数据的输出判断系统内部状态的一种能力。监控是根据数据分析推断系统的问题所在，可观测性是探索发现系统问题的原因。监控是可观测性的一种常见手段，可观测性则是系统的关键，可以提高系统的性能。

三、基于业务视角的混合云平台可观测系统的构建

当代是微服务、云原生等技术迅速发展的时代，随着信息技术的发展与成熟，多云战略已经成为越来越多的企业的选择，用户可以在私有云或者公有云的环境中进行数据获取、互换等，但是数据的传输过程中可能会被黑客或不法分子攻击，导致个人隐私或者公司机密泄露。为保障数据信息等的安全性，因此需要对数据传输过程中进行可观测性的监控。

一般来说，实现可观测性有三大支柱：Metrics、Logging、Tracing，在三大支柱支撑下，使用不同的方法结合去保障可观测性的事项。

Metrics、Logging、Tracing 这三大支柱是独立分割的，在高负载的数据系统之下，不同的应用及服务会产生多种指标及日志，当出现故障时，分散的日志中与故障相关的数据信息，但是这个过程往往比价复杂，结果并不明显，因此，衍生出以 Tracing 为中心将数据相互连接，这样才有助于可观测性的实现，创造出更大的价值。

图 1.2 以 Tracing 为核心的可观测性示意图

Metric 提供了 Gauge、Counter、Histogram、Timer、Meter 这五种基本的度量类型，Metric 具备可累加性的特点，其具备原子性，每一个都是一个逻辑单元或者是某个时间段区域里的柱状图。比如队列的深度可以是一个用来简单累加的计数器，系统请求执行的时间的柱状图，可以在指定的时间片段之上进行更新及数据汇总。

Logging 通常描述的是一些不连续的事件，并提供系统运行的详细信息，然后进行信息记录，及时发现异常信息。比如使用一个滚动的文件输出 debug 或 erro 等数据信息，在日志系统的整理及收集下，将其保存在 Elasticsearch 中；使用 Kafka 将审批的明细数据信息保存到 BigTable 中；将具备某一特性的数据信息从服务器中分离出，然后将其发送至 NewRelic。

Tracing 通常是数据的接收到处理完的一整个生命周期跟踪途径，一般请求命令在分布式的系统中进行分析处理，在单次的请求范围里处理数据信息，所有的数据信息都被指定在某个单项任务上。比如，远程服务的某一次 RPC 执行过程；一次使用 SQL 查询语句等。

Metrics、Logging、Tracing 在可观测性的监控系统中都是不可或缺的，通常是在 Metrics 下的系统异常报警，再使用 Tracing 跟踪定位异常数据信息模块，并按照数据信息模块跟踪出系统异常的源头，最后根据反馈数据信息调整 Metrics 的预警制度，这样可以在以后发生异常情况下进行提前报警，从而提早防止数据信息处理过程中问题的出现。一般通常视同维恩图（Venn diagram）表示 Metrics、Logging、Tracing 的定义及相互关系，在某些数据运行环境之下，这三者存在着重叠的情形。

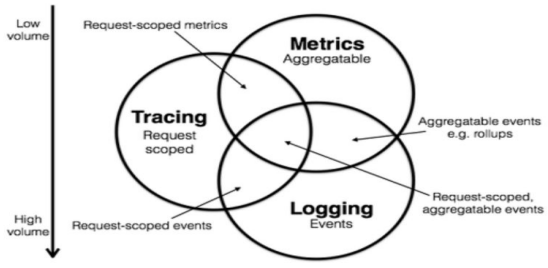

图 1.3 维恩图（Venn diagram）

根据维恩图可以发现附加的效应，Metrics 可以对数据进行压缩，可节约资源，然而日志将是不断增加的，并有可能超出预期的容量，因此，Metrics 相对高，Logging 相对低，Tracing 位于中间的位置。Metrics 指在具体的一个时间段内的一个逻辑测定、计数器或者直方图的原子。比如，服务调用的 QPS、响应时间、错误请求发生率，主要是构建集中的度量系统，主要用于数据的收集及观测等。Logging 指的是记录离散的事件，使用程序的调试、错误信息，用于构建集中的日记系统，主要是用来采取、存储及检索数据信息。Tracing 是指处理监测范围内的信息，主要是用于串联服务器之间的调用、追踪等。

目前 Metrics、Logging、Tracing 这三项功能全部应用的比较少，有的数据系统主要以 Logging 为主，有的以 Tracing 为主，大部分其他的数据信息监控系统只是监控系统的一个部分。在大部分的监控系统应用中，逻辑的处理在某一次的请求口令下完成，也并非所有的监控系统与生命周期是捆绑的，也许是逻辑组件判断及处置过程中的详尽信息，这类数据信息与离散的请求命令是正交的关系。因此，并非全部的 Metrics、Logging 可以被包括在系统跟踪的内容里面，在应用 Metrics 整理数据的过程中，对监控系统的需要特别的重要。报警是监控系统的关键，可以在第一时间内及时的发现数据异常，反映着系是否正常统的运行，是连接数据系统与用户的枢纽，也连接着整个的监控系统。数据的采集是监控的重要组成，若采集的数据异常将致使整个数据系统异常、故障等。数据存储在监控系统中也扮演着重要的角色，是记录数据的主要路径。

在混合云平台的可观测系统构建过程中，需要的是低成本的跟踪方式，需要在系统内部安装统计分析的仪表盘，而且还需要研究探索适用于复杂系统的代码等开发，解决数据集中存储的需求，从而可以满足数据的增长需要及企业用户的大量访问。

总结：综上所述，如果将混合云平台系统比作是一座冰山，通常监控所能看到的范围仅仅是冰山的山顶或者局部，但是可观测性系便可以呈现出冰山的全部，随着服务网络、微服务等技术的发展，系统信息安全的重要性越来越大，因此需要监控的各项数据信息也随之增加，所以可观测性将成为时代发展的一项趋势。

参考文献：

[1]基于数据价值视角的大数据监管系统建设的思考[J].张莹.科学与技术.2022（05）;

[2]基于云平台安全管理系统的研究[J]. 张子霄,胡蕤,张远.工程管理前沿.2022（07）;

[3]企业混合云业务组网技术与与应用[J].田江林.科学与技术.2021（25）;

[4]基于混合云的运维云服务平台的构建问题思考[J].康恺.未来科学家.2021（36）;

[5]浅析基于云平台的分布式数据采集系统[J].和乾.中国教工.2021（01）.