ICS 35.100.05, 35.240.40
L 79, A 11

IAC

中 国 保 险 行 业 协 会 标 准

T/IAC 42-2022

保险行业基于容器的云计算平台架构

Architecture of cloud computing platform based on container for insurance industry

2022-01-13 发布　　2022-04-13 实施

中 国 保 险 行 业 协 会　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国保险行业协会提出并归口。

本文件起草单位：中国信息通信研究院、中国太平洋保险（集团）股份有限公司、中国人民财产保险股份有限公司、中国人寿保险股份有限公司、安心财产保险有限责任公司、中国再保险（集团）股份有限公司、阳光保险集团股份有限公司、泰康保险集团股份有限公司、 华为技术有限公司、深圳市腾讯计算机系统有限公司、北京青云科技股份有限公司、云栈科技（北京）有限公司、杭州数梦工场科技有限公司、新华三技术有限公司。

本文件起草人：栗蔚、郭雪、卫斌、孔松、胡罡、沈大斌、张宁军、姜鑫韡、王龙涛、李玉山、袁红、冯键、成宇、尹琛、黄建坤、白阳、赵华、蒋增增、武献雨、傅帅、张春源、杜建伟、万晓兰。

引　言

保险行业在信息系统日常运营和新系统建设运营的过程中，需构建和部署开发、测试、生产等多套环境、实现应用敏捷开发、持续集成、持续交付研发运营一体化的管理，更好地支撑微服务化应用和自动化运维、微服务技术等需求。使用容器技术，能够低成本、高效率地满足上述需求。

为了保证云计算服务商或保险行业云服务科技公司在面向保险行业提供基于容器的云计算平台时，能够根据保险业实际IT系统建设和运营情况，构建满足多套环境快速部署、支撑系统应用研发运营一体化等需求的架构，本文件对保险行业基于容器的云计算平台从总体架构、平台功能要求等方面做出具体指引，确保保险行业基于容器的云计算平台满足高效可靠、安全可控等特性，推进保险行业自身科技控制及创新、服务等方面的能力。

保险行业基于容器的云计算平台架构

1 范围

本文件规定了保险行业基于容器技术的云计算平台架构，主要包括：基于容器的云计算平台应用场景、基于容器的云计算平台架构、管理平台层功能要求、安全性要求、高可用架构和基础设施层功能要求。本文件中各项指标为保险行业基于容器技术建设云计算平台基本能力要求。

本文件适用于云计算服务商和保险行业云服务科技公司正在或可能为保险行业设计、建设和应用基于容器的云计算平台架构时提供规范。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32400-2015 信息技术 云计算 概览与词汇

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源：GB/T 32400-2015，3.2.5]

3.2

容器技术 container

寄宿于操作系统的一组进程，为应用提供相互隔离的运行环境。容器具有轻量、隔离性、弹性扩容等优点，广泛应用于开发测试，运维等场景中。

4 基于容器的云计算平台应用场景

容器具有可移植性高、能够快速部署、轻量、资源利用率高等优势，基于上述优势，结合保险行业IT特性和要求，容器主要有开发测试环境、持续集成持续交付、微服务等应用场景。

4.1 总则

保险业务具有业务链路长，系统关联关系复杂、业务种类多、应用形态多等特性。

4.1.1 业务链路长、系统关联关系复杂

保险业务交易可能涉及多个业务系统合作完成，相关的业务链路长，业务系统关联关系复杂，因此需充分考虑各应用系统之间的服务发现、关联配置效率、服务健康度、服务性能、服务接口规范和安全等问题。

4.1.2 业务种类多

保险业务需求多、上线时间紧，新版本应能够快速迭代上线。

4.1.3 应用形态多

保险行业支持多种应用形态，包括各类传统架构应用和微服务架构应用，并且涉及到多种PaaS中间件和运行环境，所以需要在容器管理过程中充分考虑各种情况下的应用容器化落地。

4.2 开发测试环境

开发测试环境的有效管理有助于软件生产的正确、高效，具有一次配置多次复用、方便升级和更新、简化交付环节、减少 Mock/Stub 代码、隔离开发环境等作用。

4.3 持续集成（CI），持续交付/持续部署（CD）

保险行业业务种类及需求较多、上线时间紧，要求新版本应能够快速迭代上线，CI/CD机制能够有效满足相关要求。

4.3.1 持续集成

持续集成可以解决软件开发过程中一个项目内多个开发者代码合并问题，要求每一个开发者尽早把代码合并到团队共享的代码仓库主线中。开发者应用容器技术交付的是应用模板和镜像，镜像技术更可靠的完成了软件包和软件运行环境的交付。代码仓库中可自动触发构建镜像，并直接测试；

4.3.2 持续交付

持续交付在持续集成的基础上，通过更加全面的测试、自动化的重复部署验证等手段来保证主线代码随时处于可交付状态，以缩短软件发布周期，降低交付风险。容器利用镜像将软件的运行环境以及软件代码打包，多个镜像组合形成应用模板。将应用部署到不同的环境中，实现持续交付；

4.3.3 持续部署

持续部署指实时把合并进主线的代码发布到生产环境，是持续交付的更高阶阶段。与持续交付的区别在于，持续交付只保证代码随时处于可交付状态，管理员决定发布到生产环境时间，而持续部署侧重于实时的把通过测试的代码发布到生产环境中。

4.4 微服务应用

微服务采用一组服务的方式来构建应用，各服务独立部署在不同容器进程中，不同服务通过轻量级交互机制通信，服务可独立性扩展伸缩，定义了明确的边界。

5 基于容器的云计算平台架构

基于容器的云计算平台架构图如图 1 所示，具体包括：

a) 基础设施层：负责平台网络、存储等基础资源的管理；
b) 管理平台层：实现容器的发现、管理、调度等基本功能；
c) 高可用：实现高可用部署；
d) 监控：应具备平台监控能力，平台以及运行在平台上的应用系统应满足各公司数据中心监控规范，容器相关配置信息应在配置管理系统中进行登记；
e) 安全：平台底层主机接入安全、端口安全、API 调用安全、操作安全、数据安全和多用户安全。

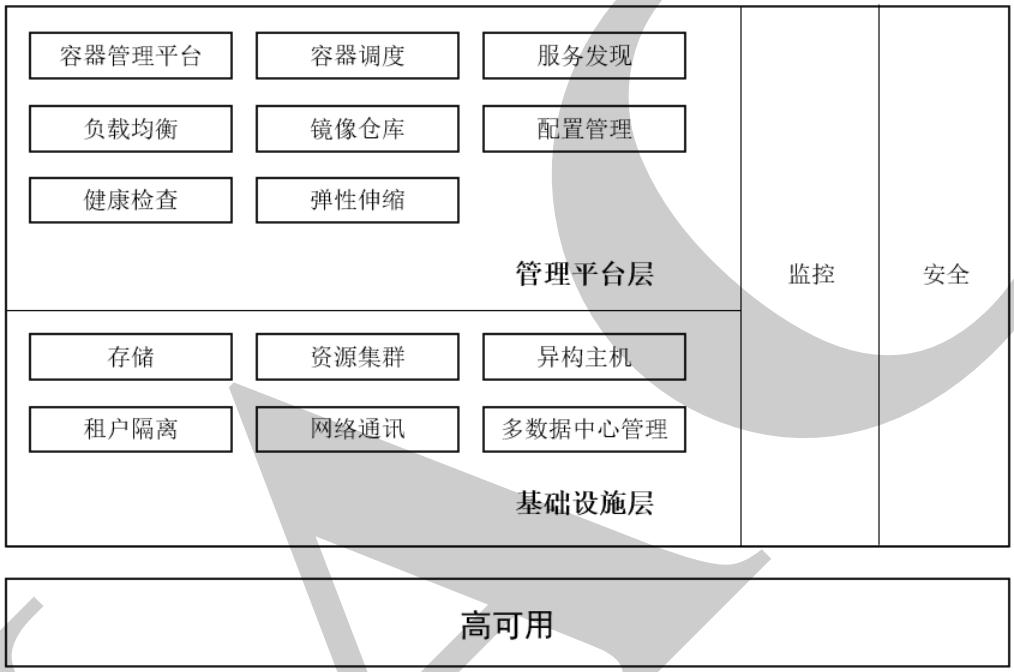

图 1 基于容器的云计算平台架构图

6 管理平台层功能要求

6.1 基本能力要求

6.1.1 管理平台

应具备管理来自所有业务区域计算资源管理、服务调度的能力，并提供统一门户。管理平台应具备资源管理能力、多集群管理能力、多租户管理能力、用户管理系统、运维系统、监控系统、服务编排系统、服务目录、日志系统等基本功能。

6.1.2 容器调度

应具备在资源集群（资源池）上进行容器调度的能力，至少包括常驻容器服务调度框架。

6.1.3 服务发现

应具备获取运行的容器信息和容器服务发现能力。容器服务能够提供相应地址和端口，供外界访问内部服务。

6.1.4 负载均衡

保险行业业务链路较长，业务系统关联关系复杂，系统间调用频繁，需有效管理系统间的服务调用。应用系统一般是通过负载均衡虚拟 IP 或域名对外暴露服务，因此基于容器的云计算平台架构应具备容器应用实例的软负载的负载均衡能力。

6.1.5 镜像仓库

保险行业支持多种应用形态，涉及到多种PaaS中间件和运行环境，常见中间件包括tomcat、weblogic、nginx、apache、redis、zookeeper等，基于每一类中间件及其特定版本应提供相应的公共镜像存储在基础镜像仓库，且需要基于特定运行环境进行镜像定制的需求，因此需要提供相应的私有镜像仓库。

故企业镜像仓库的空间可分为：基础镜像仓库、基础镜像仓库备库、项目镜像仓库、项目镜像仓库备库。基础镜像仓库存储基础的公共镜像，供所有项目共享；项目镜像仓库存储项目用户打造的私有镜像。

6.1.6 配置管理

保险行业业务系统关联关系较为复杂，需要提供便捷和模板化的配置能力，以便在开发、测试、生产等各类环境中能快速实现应用配置和关联系统配置，本项要求包括：

a) 应支持集中管理容器应用的配置属性能力，主要包括环境变量配置、日志配置、应用配置和数据库配置功能；
b) 应具备配置文件统一管理能力，容器实例启动时通过配置中心自动生成并加载配置文件；
c) 应支持配置模板化，通过模板对各具体配置项进行配置并生成配置文件实例。

6.1.7 健康检查

保险行业业务链路较长，一旦链路中某一个环节出现故障就会造成整个交易过程发生阻断。因此要求对于链路的每一个环节都要进行健康度把关，本项要求包括：

a) 应具备进程级的健康检查，即检验进程是否存活，健康启动、运行；
b) 应支持应用级的健康检查，根据服务提供的健康检查接口，监控应用的启动与运行健康状况。

6.1.8 弹性伸缩

保险行业整个业务链路中，某个环节的性能和资源不匹配会影响到整个交易流程，因此应具备根据监控的容器资源使用进行弹性伸缩的能力，以应对服务资源的动态调配，合理适配业务各环节实际资源需求。

6.2 应用场景专项要求

6.2.1 开发、测试、生产协同

保险行业业务种类及需求较多、开发测试生产流转效率较高，本项要求包括：

a) 应支持通用的协议发布代码应用，不同的人拥有不同项目的代码发布权限，并支持关键信息的审计；

b） 应支持基于特定代码或脚本等版本快速部署应用系统；
c） 应支持环境销毁能力，针对无状态应用，能够彻底删除；
d） 应支持开发负责人将环境分享给测试者，测试通过的版本可快速在生产上部署。

6.2.2 持续集成（CI）持续交付（CD）

保险行业业务种类及需求较多、新业务需要快速迭代上线，本项要求包括：
a） 应能够对接企业现有的代码版本管理系统；
b） 应具备开放的 API，能够将应用测试的服务一次性部署完成；
c） 应支持多分支多版本部署，并行测试，不发生冲突。

6.2.3 运维自动化

保险行业业务种类及需求较多、业务变更和运维动作频率较高，需要通过基于容器的云计算平台架构来促进运维自动化，本项要求包括：
a） 操作界面和数据应具备可视化功能；
b） 应支持一键部署；
c） 应支持滚动式、灰度等多种升级方式；
d） 应能够安全回退到之前的版本和配置；
e） 应支持扩容和缩容；
f） 应支持多种健康检查方式，支持服务自愈；
g） 应能够自定义报警策略，支持多种报警接收方式，具有统一的监控数据输出接口；
f） 应支持日志的采集、展现、聚合以及审计。日志分为环境日志（包括容器运行日志、宿主机容器引擎日志）、平台日志（指平台的操作日志）、应用日志（指运行在容器中的业务应用在进行业务处理中，对处理过程中的关键结果、状态所进行的记录）、安全日志（指平台用户信息变更、防火墙策略变更记录）。

6.2.4 微服务

保险行业广泛引入微服务架构应用，需要通过基于容器的云计算平台架构来有效支持微服务架构应用的落地，提高应用系统运维效率，本项要求包括：
a） 应支持分布式运行，支持每个服务运行到独立容器中；
b） 应支持基础设施自动化，支持自动集成测试，自动部署上线和服务监控恢复。

7 基础设施层能力要求

保险行业业务系统种类多，应用架构复杂。对于基础设施层设备的多样性、权限、通讯和多数据中心等有特定要求，本项要求包括：

7.1 存储

本项要求包括：
a） 应支持备份能力；
b） 应支持不同存储介质的适配能力，支持分布式存储、物理存储等多种存储介质。

7.2 资源集群

即资源池，应具备提供跨物理节点的计算资源和存储资源的能力。

7.3 异构主机

应具备基础设施适配能力，包括但不限于物理机、虚拟机、公有云、多云数据中心等支持能力。

7.4 租户隔离

应具备提供租户隔离的能力。

7.5 网络通讯

应具备跨主机通讯能力，支持容器网络管理。

7.6 多数据中心管理

应至少保证同城双中心，可自主选择建设异地数据级灾备中心，可根据自身业务需求评估是否建设双活数据中心。基于容器的云计算平台以及运行在平台上的应用系统（按系统级别）灾难恢复能力应满足《保险业信息系统灾难恢复管理指引》相关要求。

8 安全性要求

本项要求包括：

a) 应支持镜像仓库的安全扫描能力；
b) 多云、多环境主机接入时，应支持用户名和密码、令牌、证书和密钥等认证机制；
c) 对重要的数据应具有备份恢复机制，重要数据包括但不限于应用配置、程序和存储卷；
d) 应支持关键操作的审批和管理，关键操作包括但不限于应用发布、应用停止等；
e) 不同用户应具备不同的应用管理权限，应支持为每个应用系统分别开设只读账户、编辑账户和管理账户。管理账户可以在权限范围内的宿主机上运行和管理容器应用，进行镜像打包发布、配置管理、程序发布等工作，编辑账户可以对现有资源进行编辑，无法新建资源和应用，只读账户只能查看相关信息；
f) 应具备安全认证（令牌），对于容器自动扩缩容在传统数据中心要求开通多端口策略的问题，具体策略需向银保监会报备；
g) 基于容器构建的服务对外应提供多种安全性接口；
a) 应用系统网络架构分为内网应用架构、外网应用架构、内外网混合架构：
    1) 内网应用架构：应支持应用系统只接受内网用户访问，所有容器实例均运行在内网区域；
    2) 外网应用架构：应支持应用系统只接受外网用户访问，具有访问控制规则，能够监测到外网用户的网络攻击行为，能够记录攻击类型、攻击时间、攻击流量等；
    3) 内外网混合架构：应支持内网容器服务可提供外网用户访问，或者对外网其他服务提供接口访问时，应单独在外网部署软负载、服务网关与服务发现组件，并设置严格的白名单和访问策略并且加强流量监测与审计。

9 高可用架构

基于容器的云计算平台应具备高可用架构，本项要求包括：

a) 应满足高可用部署规范，各功能模块，如调度模块、镜像模块、监控模块、配置管理模块等，

不允许存在单点故障技术风险；

b) 应支持二级域的划分，基于容器的云计算平台架构应能支持在平台统一管理的情况下，对于容器资源区域进一步做二级域划分，每个二级域配备独立的容器管理调度集群，且不同的二级域所管理的资源彼此隔离，某个二级域的故障不会对另一个二级域造成影响，以此限制故障波及范围，增加平台整体可用性。本指标考察容器管理层面的二级域划分能力，对具体划分策略不做要求，可以但不限于基于业务属性、网络区域等方面进行划分。在基于业务属性划分情况下，可以结合保险业务，例如为寿险公司和财险公司分别划分业务区域，寿险公司的服务部署在寿险公司业务区域，财险公司的服务部署在财险公司业务区域；

c) 应支持控制平面节点和计算节点的分离。

参 考 文 献

[1] GB/T 31167-2014 信息安全技术 云计算服务安全指南
[2] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
[3] GA/T 1390.2-2017信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求
[4] GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求
[5] ISO/IEC TR 27015:2012 信息技术 安全技术 金融服务信息安全管理指南
[6] JR/T 0071-2020 金融行业网络安全等级保护实施指引
[7] JR/T 0072-2020 金融行业网络安全等级保护测评指南
[8] 2012-2513T-YD 可信云开源容器类解决方案认证评估方法