ICS 35.100.05, 35.240.40
L 79, A 11

IAC

中 国 保 险 行 业 协 会 标 准

T/IAC 44-2022

保险行业基于容器的云计算平台成熟度模型

Maturity model for cloud computing platform based on container in 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。

本文件主要起草人：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

为建立保险企业基于容器的云计算平台评价体系，衡量保险企业容器技术发展水平，推动容器技术快速部署、轻量灵活等特性在保险行业的深入应用，本文件对保险行业基于容器的云计算平台成熟度模型进行定义，主要包括落实程度、应用成效、平台技术能力和安全保障四个方面。

保险行业基于容器的云计算平台成熟度模型

1 范围

本文件规定了保险行业基于容器的云计算平台成熟度模型，具体包括四方面：落实程度、应用成效、平台技术能力和安全保障。

本文件适用于保险行业云服务科技公司或保险业科技部门部署、实施和监测基于容器的云计算平台相关场景。

注：本文件以容器平台为考察单位，若保险企业具备多个容器平台，应单独考察每个平台的成熟度等级。

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。

3.3

容器平台 container platform

以容器或容器组为最小调度单元，通过容器编排技术处理实现任务间的关联关系（调用、访问、代理等），用于构建、发布和运行分布式应用的云平台。容器平台为开发者提供了管理和部署容器化应用程序和集群的能力。

4 成熟度模型概述

保险行业基于容器的云计算平台成熟度模型从四个维度进行衡量：

a） 落实程度：保险企业内容器平台在部门、信息系统等方面的覆盖情况；

b） 应用成效：容器平台在提高效率、节约建设成本等方面的应用成效；

c） 平台技术能力：容器平台的技术能力水平；

d） 安全保障：容器平台安全保障制度的完备性和能力水平。

各项指标从弱到强的要求分为基础级、增强级和先进级，落实程度、应用成效、平台技术能力和安全保障四个方面的各项指标为某一级，则评定基于容器的云计算平台为相应级别，成熟度等级划分见表1。

表 1 容器平台成熟度等级划分

容器平台成熟度等级划分	
基础级	在企业内构建基于容器的云计算平台，一定范围推行并获得初步成效。
增强级	在企业内构建基于容器的云计算平台，大范围推行并获得较高效率提升。
先进级	在企业内构建基于容器的云计算平台，全面落地并达到整体效率得到较大优化

5 落实程度要求

5.1 业务系统使用率

本指标考察保险企业内基于容器平台的业务系统数量。

容器平台业务系统使用率的计算公式，见式（1）。

$$P1 = (A \div B) \times 100\% \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots（1）$$

式中：

P1 -- 容器平台业务系统使用率；

A -- 实际使用容器平台的业务系统数量；

B -- 业务系统总数。

注：若保险企业具备多个容器平台，本指标只区分使用容器平台的业务系统和未使用容器平台的业务系统，不对业务系统使用的容器平台作区分。

a） 业务系统总数大于 30 的保险企业的容器平台业务系统使用率参考标准见表 2。

表 2 容器平台业务系统使用率参考标准

容器平台业务系统使用率参考标准		
基础级	增强级	先进级
不低于 15%	不低于 30%	不低于 50%

b） 业务系统总数小于等于 30 的保险企业的容器平台业务系统使用率参考标准见表 3。

表 3 容器平台业务系统使用率参考标准

容器平台业务系统使用率参考标准		
基础级	增强级	先进级
实际使用容器平台的业务系统数量不低于 5 个	实际使用容器平台的业务系统数量不低于 10 个	实际使用容器平台的业务系统数量不低于 15 个

6 应用成效要求

6.1 效率提升成效

本指标考察保险企业基于容器的云计算平台对应用扩缩容部署时间的效率提升，参考标准见表4。效率提升比的计算方法，见式（2）。

$$P2 = [(C - D) \div D] \times 100\% \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots（2）$$

式中：

P2 -- 效率提升比；

C -- 传统模式效率：抽样一定体量的应用，传统模式下扩缩容一定体量应用，部署所耗工作量（人*天）；

注：本文件中传统模式针对的是传统的服务器脚本部署或者手动部署方式。

D -- 基于容器的云计算平台效率：抽样同等体量的应用，基于容器的模式下扩缩容同等体量应用，部署所耗工作量（人*天）。

注：本指标仅考察该容器平台上所有业务系统迁移到容器平台前后工作量的对比。

表 4 容器平台效率提升成效参考标准

容器平台效率提升成效参考标准		
基础级	增强级	先进级
不低于 100%	不低于 200%	不低于 300%

7 平台技术能力要求

7.1 容器管理平台层能力要求

对容器管理平台层的能力要求见表5。

表 5 容器管理平台层能力要求参考标准

容器管理平台层能力要求参考标准			
要求项	基础级	增强级	先进级
容器管理平台	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。容器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。	同上一级	同上一级
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。	同上一级	应具备资源集群（资源池）服务调度能力，包括：常驻服务调度框架，**批处理调度框架**等。**批处理调度框架能够定时执行和结束某些任务。**
负载均衡	应具备容器应用实例的软负载均衡能力。	同上一级	同上一级

表 5 容器管理平台层能力要求参考标准（续）

容器管理平台层能力要求参考标准			
要求项	基础级	增强级	先进级
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。	同上一级	同上一级
镜像仓库	应具备企业私有镜像仓库。	应具备企业私有镜像仓库。**镜像仓库的空间分为：基础镜像仓库、项目镜像仓库。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。**	同上一级
配置管理	应具备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。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。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。	同上一级	同上一级
批处理应用		**应支持批处理任务。批处理任务运行在指定的资源组中，可以与同一应用系统下的其他资源组共用，但不同应用系统之间的批处理任务资源隔离。**	同上一级
健康检查	应具备容器异常时预警能力。	应具备容器异常时服务自愈能力。	应具备容器异常智能分析及自愈策略优化及自愈能力。
弹性伸缩	应具备根据业务活动需要伸缩容器资源的能力。	应具备根据服务资源压力自动伸缩容器资源的能力。	应具备应用运行智能识别、优化容器资源自动伸缩支持应用自动扩容的能力。

7.2 容器基础设施层能力要求

对容器基础设施层的能力要求见表6。

表6 容器基础设施层能力要求参考标准

容器基础设施层能力要求参考标准			
要求项	基础级	增强级	先进级
存储	应具备备份能力。	应具备备份能力。**应具备不同存储介质适配能力，支持分布式存储、物理存储等多种存储介质 。**	同上一级
资源集群	应具备提供跨物理节点的计算资源和存储资源的能力。	同上一级	同上一级
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。**	同上一级	同上一级
租户隔离	应具备提供租户隔离的基本能力。	同上一级	同上一级
网络通讯	应具备跨主机通讯能力，支持容器网络管理。	同上一级	同上一级
多数据中心管理	应具备“同城双中心的容灾能力。 容器平台以及运行在容器平台上的应用系统（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。	**应具备异地灾备的容灾能力。可根据自身业务需求评估是否建设双活中心。** 容器平台以及运行在容器平台上的应用系统（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。	

7.3 容器平台高可用架构

对容器平台高可用架构的能力要求见表7。

表7 容器平台高可用架构能力要求参考标准

容器平台高可用架构能力要求参考标准			
要求项	基础级	增强级	先进级
高可用架构	——应满足高可用部署规范，容器平台各功能模块，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。 ——二级域划分：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。 ——控制平面节点和计算节点分离。	在上一级的基础上仍需满足： **——三级域划分：每个业务区域划分若干个子域。例如，为寿险公司业务区域划分移动 APP 子域和小程序子域。本指标考察容器平台管理层面的三级域划分能力，具体划分策略不做要求。** **——通过增加子域来实现业务区域计算资源扩容。** **——资源集群中可为每个应用系统划分资源组，不同资源组下的宿主机相互隔离。每个应用系统不同服务间若需要资源隔离，也可以创建多个资源组，宿主机可以是虚拟机或者物理服务器。** **——能够基于应用服务进行负载均衡实例配置，可以自动注册和发现应用服务，并且可以根据应用服务的实际性能需求为其分配相应处理能力的负载均衡实例。**	在上一级的基础上仍需满足： **——每个业务区域划分若干个子域，每个子域部署两个不同的资源集群来实现双活与高可用架构。应用系统可选择高可用部署，高可用架构下应用系统的同一功能集群的容器分别部署在两个不同的资源集群上，当某一资源集群发生故障，由另一个资源集群上的容器持续提供服务，反之亦然。**

8 安全保障要求

对容器台的安全保障能力要求见表8。

表8 容器平台安全保障能力要求参考标准

容器平台安全保障能力要求参考标准			
要求项	基础级	增强级	先进级
镜像仓库安全性	应支持镜像仓库的安全扫描能力。	同上一级	同上一级
管理平台安全性	各主机接入到管理平台应需要支持用户名和密码、令牌、证书和密钥等认证机制。	同上一级	同上一级
数据安全性	对重要的数据、配置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。	同上一级	同上一级
操作安全性	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。	同上一级	同上一级
多用户角色管理	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。	同上一级	同上一级
端口安全性	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。	同上一级	同上一级
接口安全性	基于容器构建的服务对外应提供多种安全性接口。	同上一级	同上一级
应用接口网络架构安全性	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。		

表8 容器平台安全保障能力要求参考标准（续）

容器平台安全保障能力要求参考标准			
要求项	基础级	增强级	先进级
镜像安全性	应提供镜像完整性校验功能，防止容器镜像被恶意篡改。	**应支持镜像升级，防止镜像内服务存在漏洞导致部署风险** **应针对重要业务系统提供加固的镜像。**	**应支持对容器镜像进行安全扫描。**

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 0071-2012 金融行业信息系统信息安全等级保护实施指引
[7] JR/T 0072-2012 金融行业信息系统信息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