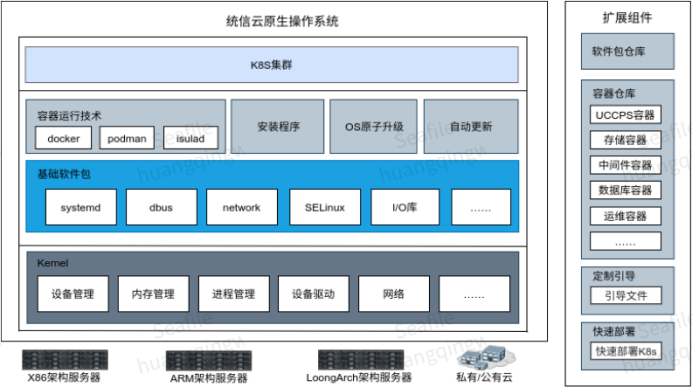
功能概述

统信云原生操作系统是由统信自主研发的一款轻量化操作系统，它是在统信服务器操作系统V20上经过二次精简和定制衍生出来的，结合了Kubernetes和容器技术，提供了轻量、快速、安全、便捷的服务，用于云计算/云原生场景，被广泛视为可支撑应用平台的云底座。统信云原生操作系统可用于金融、军工、公安、教育行业，以及政府部门和大中小企业。对于拥有多个中小型部门或远程地点的大型机构数据中心，统信云原生操作系统可满足它们应用业务的上云需求。



图一：统信云原生操作系统架构图

统信云原生操作系统可助力用户轻松搭建PAAS和SAAS平台，并提供云计算/云原生场景的解决方案产品。

统信云原生操作系统包含四个模块和一个扩展组件。

容器层：当多个容器同时运行时，通过使用原子更新保护机制，可以使集群内的所有云原生操作系统的软件包内核版本是一致且固化的；通过自动更新模块，可以使集群内的所有云原生操作统一升级到新版本。例如，只需要一次简单的统一升级即可以快速修复一次CVE漏洞。

基础软件和内核层：基于统信服务器操作系统V20的产品软件包和内核软件包，裁剪掉与系统运行无关的软件包如python，gcc等。

扩展组件：主要是辅助用户快速搭建和更好的使用统信云原生操作系统。

功能介绍

1. 容器云的现状与需求分析

1.1. 现状分析

近年来我国经济发展迅速，数字化产业不断创新，数字中国已成功举办了五次峰会，国内的IT技术成为经济发展注入新的活力。随着云计算技术的发展，虚拟化这一词不断的被人们广泛了解。目前云计算功能是把资源虚拟化为“云”后存储起来，为用户提供服务。随着虚拟化技术发展，传统虚拟化技术有，比如VMWare、KVM、Xen等，目标是创建完整的虚拟机调度使用。随着一朵朵私有云产品建立，如何实现更为高效、敏捷应用及开发，满足更为多样化企业上云要求和多样化复杂性IT架构需求。单一云已不能满足当前IT信息技术发展需求，企业不得不进行云数量增加，以满足不同异构场景需求。

针对上云采用虚拟化技术存在主要问题如下：

* 为了运行应用，除了部署应用本身及其依赖(通常几十MB)，还得安装整个操作系统(几十GB)，空间资源占用大。
* 虚拟机技术中服务器与应用的映射关系从一对一变为了一对多，这样会使得使得不同的虚拟机间会竞争带宽、宿主机端口资源等。在负载较高的情况下，虚拟机的性能则会变得很差，资源利用率大大下降，导致调度分发也缓慢。
* 虚拟机平台有数量限制，传统云平台一般数量只有几十个。
* 云平台虚拟机提供的产品较为单一，每次需要针对镜像进行手动定制服务，准备时间长周期久，迭代更新缓慢。

1.2. 需求分析

根据中国信通院的数据记载，2020 年全球云计算市场规模为 2083 亿美元，到 2025年将超过 6000 亿美元。而且，中国信通院在《数字政府云原生基础设施白皮书》中表示：当前，国内需要一款成熟、可靠的面向云计算/云原生的轻量化操作系统，用于实现政府、金融、中小型企业等行业的云建设、运维、运营模式的新一轮升级，进而加速数字政府建设的全面升级。

在国际市场中，用于云计算/云原生场景的专业操作系统目前主要有 Red Hat 发布的 RHCOS 和 SUSE 发布的 Micro。它们占据了国际云计算/云原生等边缘计算场景 60%的市场。然而，国内传统操作系统难以完全满足快速启动、系统轻量化、集群化、应用与系统架构分离化、系统固化等需求。因此，在云计算/云原生场景下场景下，基于传统操作系统进行定制裁剪的国内轻量化操作系统应运而生。

新的需求如下：

* 以应用为中心，提供配置、存储、镜像仓库等完整的、容器引擎模块，支持应用的弹性伸缩、高可用、负载、均衡等特性
* 通过可视化的流水线设计任务，对构建、测试、部署等各类任务做流程化设计，一键完成持续/交付工作
* 可视化的编辑界面，以编辑YAML文件的方式设计复、杂的应用模板，简化应用部署难度并提升灵活性
* 实现了完整的微服务治理体系，支持服务发现、熔断、负载均衡、配置及调度分析
* 应用层面实现负载均衡、弹性扩容、故障自动恢复等功能，并配备监控告警、健康检查和自动化作业平台、等智能化运维工具

2.  细分场景

针对不同的应用场景，统信云原生操作系统支持如下三个版本：

(1) 精简化云原生的操作系统版本，该版本是一个最轻量化的云原生操作系统，

只有 300MB 左右。可以根据用户需求定制针对不同业务的云原生操作系统，

例如可以为分布式存储、分布式数据库和私有云计算 IAAS 平台等业务定制专

门针对存储、数据库和云计算 IAAS 平台的专用云原生操作系统。

(2) 在精简化云原生的操作系统版本，针对云原生 Kubernetes 的操作系统版本，该版本集成了 Kubernetes 相关组件，同时提供了 Kubernetes 的快速集群部署方案，用户只需要进行一些 IP 网络的基础配置就可以得到一个 Kubernetes集群。

(3)  在精简化云原生的操作系统版本，针对 IAAS/PAAS 平台的操作系统版本，该版本集成了统信容器云管理平台，用户可以得到一个 PAAS 容器云。

3. 方案特点

3.1.  轻量化

统信云原生操作系统基于统信服务器操作系统 V20 剔除了非核心的软件，例如GUI、包管理器、开发语言等，使得系统与应用高度分离，更极大的提升了启动速度。根据实测数据显示，统信云原生操作系统运行时内存使用量小于 100M，资源占用率比常见的服务器操作系统小 50%。模部署容器时，与使用其他操作系统相比，统信云原生操作系统凭借 Docker 的快速启动能力，在性能和启动速度上有更加明显的优势。同时，统信云原生操作系统支持在裸金属中直接部署容器运行环境，无虚拟化开销，支持存储协同调度，释放硬件最大效能。

3.2.  高可靠性

在大规模全 CPU 架构的整机上，统信云原生操作系统采用 LTP 工具进行测试，测试结果如下：在 LTP Stress 7×24 小时高负荷条件下，无宕机；测试用例通过率超过 97%；卸荷后，在不超过 60 秒内，系统和各应用可以流畅运行。

统信云原生操作系统通过使用 rpm-ostree 机制，可以保证每次进行系统更新或补丁升级时，应用程序的运行不会被打断。另外，如果系统更新或补丁升级失败，系统可以快速回退到上一版本。

3.3.  高安全性

统信云原生操作系统通过使用 rpm-ostree 的只读文件系统机制，既降低了系统被病毒感染的风险，又保证了升级、回滚时系统的完整性。统信云原生操作系统默认关闭了 sshd 服务，裁剪了 samba 和 python 等软件包，只保留了系统运行必要的软件包和容器运行时依赖包，降低了漏洞产生等风险。

3.4.  易维护性

统信云原生操作系统通过提供系统监控 web 界面，方便查看系统的状态和运行负载情况。它自带云原生容器化平台和标准化的应用开发能力，可实现整个应用集群的自动化运维。

4. 具体功能介绍

4.1. 安装程序

统信云原生操作系统内置了一个安装程序，通过使用定制引导模块提供的引导文件，可以自定义或使用默认方式配置系统中的 Roota 和 Rootb 等磁盘的分区大小、选择安装的软件包、导入配置文件等。

4.2. 安装程序

统信云原生操作系统采用双系统分区 (dual root partition) 设计。即两个系统分区，分别为主动分区和被动分区并在系统运行期间各司其职。主动分区负责系统运行，被动分区负责系统升级。系统通过集成 rpm-ostree 技术进行系统更新升级，一旦这个新版本的操作系统将被使用，现在使用的系统文件将被下线至被动分区，并在系统重启时从新版本分区启动，原来的被动分区将切换为主动分区，而之前的主动分区则被切换为被动分区，两个分区扮演的角色将相互对调。同时在系统运行期间系统分区被设置成只读状态。如果当系统更新出现故障或问题时也可以使用 rpm-ostree回退到上一个系统状态。rpm-ostree 是 ostree 和 rpm 的结合，一方面提供基于 rpm 的软件包安装，一方面提供基于 ostree 的操作系统更新。rpm-ostree 将这两种操作都视为对操作系统的更新，从而确保更新全部成功或全部失败，并允许在更新系统后回滚到更新前的状态。这种特性视为原子升级/回滚。

4.3. 自动更新

统信云原生操作系统内置一个自动更新模块，会实时检查软件仓库中是否有最新的软件包。当统信云原生操作系统开启自动更新功能后，一旦发现有最新软件包，系统会调用 rpm-ostree 进程对集群系统进行统一更新。

4.4. 容器化应用部署

统信云原生操作系统的总体设计主要面向集群化与容器化场景不在提供何软件包管理器，将所有其它应用都将作为 Docker 容器运行，从而保证各服务实现隔离、可移植以及外部管理能力。实时上，开发者将应用部署到云基础架构上时变得日益流行。通过容器化 (containerized) 的运算环境向应用程序提供运算资源，应用程序之间共享系统内核和资源，却互不干涉运行。单个容器的故障能够快速的重启修复，并且容器内的应用故障不会引起整个系统的崩溃。统信云原生操作系统不但提供了各种容器运行时如欧拉社区 isulad，还提集成了 Kubernetes，同时也提供了如中间件，数据库等容器镜像，节省了用户部署配置时间。这种方式，保障了整个集群内 Host 节点操作系统内核和系统软件包版本的一致性，简化了由于版本问题带来的操作复杂性，使得操作系统自身的维护更加容易。

5.  方案优势

5.1. 快速部署，开箱即用

统信云原生操作系统基于统信服务器操作系统 V20，进行二次开发，可快速部署容器中的集群环境。例如，统信云原生操作系统可按照用户需求在一分钟内快速拉取一个 K8S 应用集群，无需单独配置应用、中间件、数据库等信息。统信云原生操作系统还提供自动构建镜像能力，内置灰度发布，流量控制，环境隔离，应用监控诊断，零基础、开箱即用。

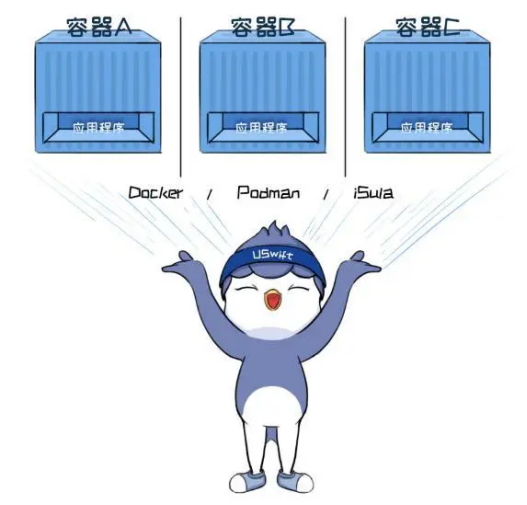


5.2. 多架构支持，广泛兼容

统信云原生操作系统兼容主流服务器设备，适配主流中间件和数据库，并兼容适配了 30000 余国内外主流软件包，为用户构建软硬件系统架构提供了更多的组合选择。在硬件兼容方面，统信云原生操作系统实现了对全系列国产处理器架构（AMD64、ARM64、LoongArch 等）、主流服务器硬件的良好适配。同时，针对其它配件，统信服务器操作系统 V20 完成了大量的兼容性适配和测试工作，包括 HBA 卡、万兆网卡、AI加速卡等。

5.3. 容器管理

所有应用以容器化方式运行，保证各服务应用独立运行，无依赖冲突等问题。提供Docker、Podman和iSula等运行时，用于创建、删除、修改、运行容器镜像。



5.4. 安全管理

基于统信自身的经验和成果，积极汲取上游社区的优势并适配Kata Containers容器安全隔离技术，让容器能运行在安全且隔离的环境中。

固化文件系统,提供操作系统固化能力,通过使用Rpm-ostree的只读文件系统机制,既降低了系统被病毒感染的风险,又保证了升级、回滚时系统的完整性.

默认文件系统权限见下图

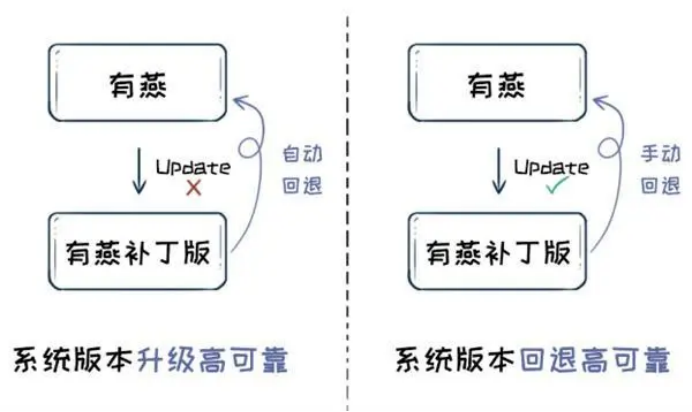


5.5. 轻量化管理

通过剔除GUI等非核心组件,使镜像大小仅为500MB,不仅减少了系统受攻击面,提升了系统安全性,也加快了启动速度,并方便了统一运维.

5.6. 高可靠

通过使用Rpm-ostree机制,即结合dnf与OSTree技术,在不可变基础设施的基础上,使某些不易容器化的组件（例如驱动）,能以包的形式扩展操作系统的能力,有效确保系统在更新前或者更新后都可以使用.



5.7. 高稳定

在LTP Stress 7 x 24小时高负荷条件下，压力测试无宕机，测试用例通过率平均超过98%。

5.8. 可定制

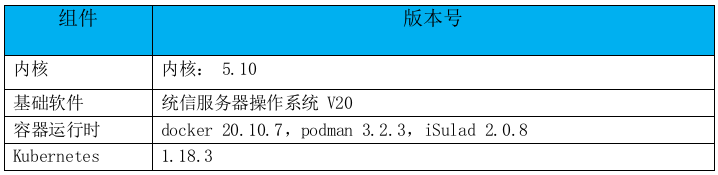
基于不同的系统组件或容器镜像，可进行有针对性的定制，保障兼容性及原有业务的稳定性，同时提供集成了统信容器云管理平台的镜像，可使开发人员能够创建、测试和运行应用程序，并且将它们快速部署到集群中。



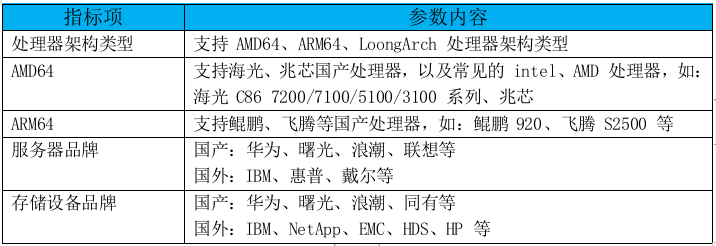
准备环境



部署环境要求



软件环境



硬件支持

安装步骤

见安装手册