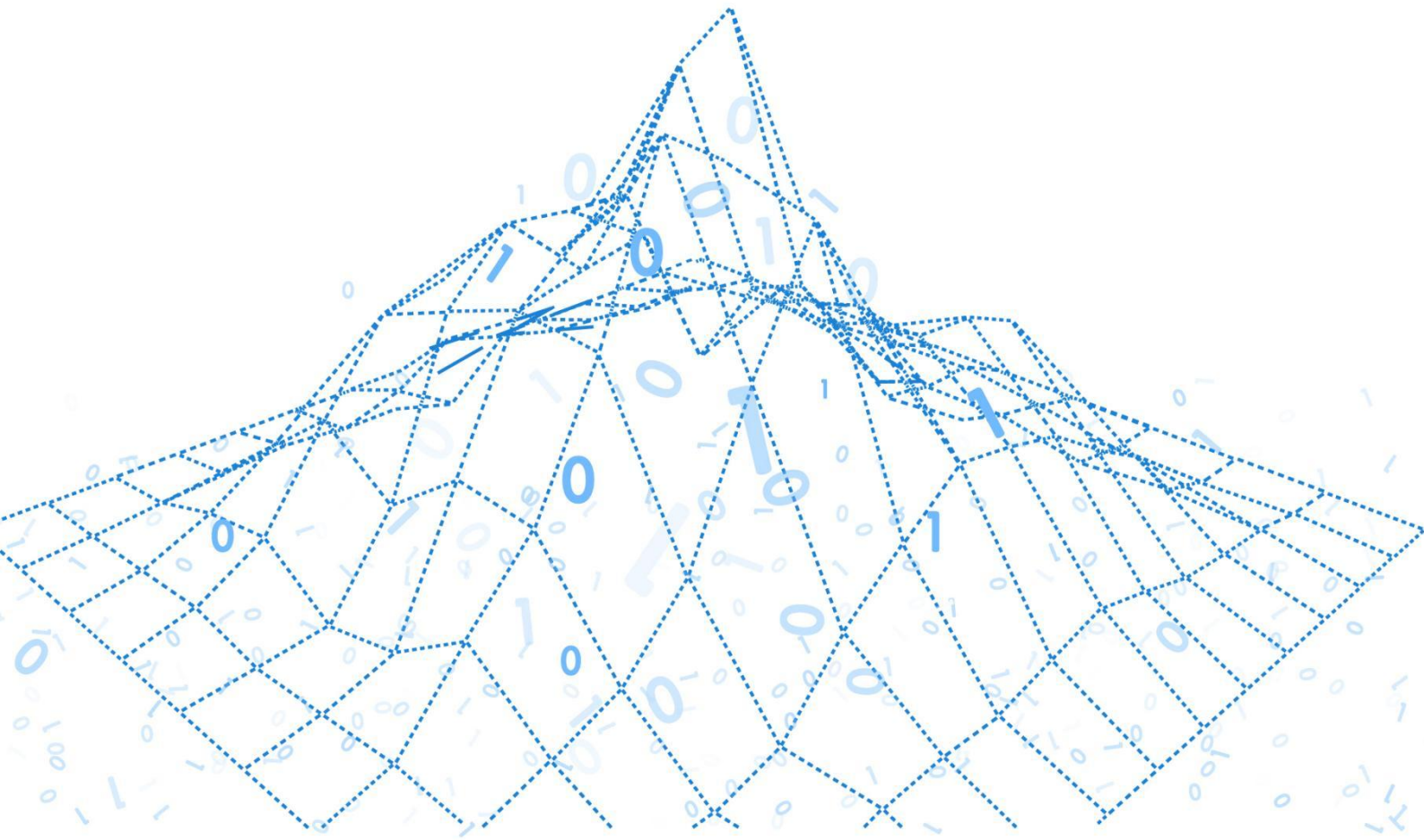
2023年第二期 | 总第四期

全球开源发展态势洞察



开放原子开源基金会出品
2023年2月7日

目录

国际开源基金会

Apache Linkis 正式毕业成为 Apache 软件基金会顶级项目

据 Apache 软件基金会官方消息，Apache 软件基金会（ASF）于 2022 年 12 月 03 日，通过了 Apache Linkis 计算中间件项目的孵化毕业投票。于 2023 年 01 月 18 日，Apache 软件基金会官方宣布 Apache Linkis 正式毕业，成为 Apache 顶级项目（TLP）。

Apache Linkis 计算中间件项目，是由微众银行大数据平台团队于 2019 年 7 月进行开源，并于 2021 年 8 月正式捐献给 Apache 软件基金会（ASF），由 Apache 软件基金会（ASF）进行孵化，并在 2022 年 12 月 03 日通过孵化毕业投票。

Apache Linkis 在上层应用程序和底层引擎之间构建了一层计算中间件。通过使用 Linkis 提供的 REST/JDBC/Shell 等标准接口，上层应用可以方便地连接访问 MySQL/Spark/Hive/Trino/Flink 等底层引擎，同时实现变量、脚本、函数和资源文件等用户资源的跨上层应用互通，以及通过 REST 标准接口提供了数据源管理和数据源对应的元数据查询服务。

自开源以来，开源社区群用户总数超 7600 人，沙箱累计试用公司超 2600 家，收到超过 110 家企业已投入生产的反馈，生产环境支撑的数据量超 400PB，生产服务的用户超 5000 人，涉及金融、电信、制造、互联网等多个行业。许多公司已经用 Linkis 来解决大数据平台连通、扩展、管控、编排等计算治理问题。在一年多的孵化期间，Apache Linkis 由社区开发者主导发布了 7 个 Apache 版本，平均约两个月就会发布一个版本。新加入了 4 个 PPMC 成员（项目管理委员会）和 13 个 Committers，来自不同的公司和团队，贡献人数达到 127 人。

Apache bRPC 正式毕业成为 Apache 软件基金会顶级项目

据 Apache 软件基金会官方消息，Apache 软件基金会（ASF）于 2023 年 1 月 26 日，官方宣布 Apache bRPC 正式毕业，成为 Apache 顶级项目（TLP）。

Apache bRPC 是由百度初始创立并持续贡献的工业级别 RPC 开源项目，在 2018 年正式贡献给 Apache 软件基金会进

行项目孵化，在 2022 年 12 月 24 日，Apache bRPC 项目顺利毕业，成为 Apache 软件基金会顶级项目（TLP）。

bRPC 于 2014 年诞生于百度基础架构部，用 C++编写的工业级 RPC 框架，常用于搜索、存储、机器学习、广告、推荐等高性能系统。2017 年正式在 GitHub 进行开源，并于 2018 年 11 月正式捐献给 Apache 软件基金会（ASF），对外开源版本的名称为 Apache bRPC。

经过四年多的孵化，bRPC 开发者数量增长数倍、在 GitHub 上的 Star 数也超过 14.4K，目前已覆盖了互联网、人工智能、搜索、推荐、电商和教育等多个行业和领域，被百度、爱奇艺、作业帮、字节跳动、京东、拼多多、滴滴、B 站、vivo、小红书、第四范式、欢聚时代、shopee 等公司广泛使用并对该项目进行持续贡献，线上服务实例数已超过 600W，现已成为业界广受欢迎的开源 RPC 框架之一。

Jina AI 正式将 DocArray 捐赠给 Linux 基金会

Jina AI 是一家商业化开源软件公司，专注于打造针对多模态应用的 MLOps 开发运维工具。DocArray 是一个用于处理、传输和存储多模态数据的 Python 工具包。DocArray 提供便捷的多模态数据处理功能，具备基于 Protobuf 提供高性能的网络传输性能，同时也为多种向量存储方案提供统一的 API 接口。

日前，Jina AI 正式将 DocArray（github.com/docarray）项目捐赠给 Linux 基金会，致力于打造一个中立、包容和通用的标准多模态数据模型。

近日，DocArray v0.21.0 发布，更新内容：

- 新增 OpenSearch 后端存储，增加向量存储新选项；
- 新增带颜色的 Point Cloud 数据，以便更好地展示和分析点云数据；
- 支持 Redis 的多语言文本搜索，只需要在配置中修改 language 参数。

Paralus 正式成为云原生计算基金会沙箱项目

日前，Paralus 已经作为沙箱项目正式加入云原生计算基金会（CNCF）。加入云原生计算基金会，为 Paralus 增加了更多的可信度，并希望帮助更多的人采用和贡献 Paralus。

Paralus 可以帮助每个人大规模管理对多个集群的访问。凭借其即时服务帐户创建和细粒度用户凭证管理，Paralus 提供了一个适应性强的系统，可确保在必要时安全访问资源。除此之外，Paralus 还内置了零信任原则，支持多个身份提供者、自定义角色等。

行业发展

英特尔暂停 RISC-V 计划和网络交换机业务

英特尔 2022 年第四季度亏损 6.61 亿美元，利润率跌至几十年来的最低点。近日，该公司宣布新的成本削减措施，这包括它将不再为其网络交换机业务投资新产品，类似于它最近决定结束其 Optane 内存业务一样，使该部门停产。令人质疑的是，英特尔在还没有正式宣布的情况下，已经退出其备受推崇的 RISC-V 探路者计划。

openKylin 0.9.5 发布：首次支持 Arm、RISC-V

近日，中国桌面操作系统根社区 openKylin（开放麒麟）正式发布了 0.9.5 版本。基于 Linux 5.15 内核构建，面向 5G 时代打通平板、PC 等设备，有效弥补国产 OS 的短板。除了 x86 架构，新版本全新解锁 ARM 架构，官方适配 Raspberry Pi、Cool Pi 开发板，支持树莓派软硬一体的开发模式。同时，完成 RISC-V 开发板适配，满足用户多元场景需求。

华为云发布冷启动加速解决方案：助力 Serverless 计算速度提升 90%+

冷启动（Cold Start）一直是 Serverless 领域面临的优化难题之一，华为云创新提出了基于进程级快照的冷启动加速解决方案，致力于在用户几乎无感知的前提下，有效提升应用的冷启动性能。

CNCF 基金会将在第三季度推出 Kubernetes 和云安全（KCSA）认证

KCSA 认证考试旨在为希望从事云原生安全的个人提供一个切入点。考试考查应试者制定安全策略和程序、识别评估并减少安全风险和漏洞、协助事件响应和取证调查、测试和监控安全系统等云原生安全能力。考试系统目前处于开发阶段，预计将在 11 月北美 KubeCon 召开前推出。

cdCon + GitOpsCon 2023 议题征集中（截止到 2.10）

cdCon + GitOpsCon 2023 由 CD 基金会和 CNCF 基金会主办，将于 5.8-5.9 在温哥华举行。议题内容可包括：GitOps

入门、扩展和管理 GitOps、从生产部署中吸取的教训、先进的交付技术、云原生环境中的开源 GitOps 和 CD 技术实践、供应链安全等。

Istio 发布 2022 年安全审计结果

Istio 用于在其 Kubernetes 生产环境中实施安全策略。在代码安全日益重要的情况下，Istio 致力于维护一个健壮的漏洞管理程序。为了验证工作，Istio 定期邀请项目的外部审查，这是第二次安全评估。审计员的评估是，“Istio 是一个维护良好的项目，有一个强有力和可永续的安全方法”，没有发现关键问题。该报告的亮点，是发现了 Go 编程语言中的 1 个漏洞。

Venafi 推出云原生机器身份管理服务 TLS Protect for Kubernetes

TLS Protect for Kubernetes 是 Venafi 机器身份管理平台 Control Plane for Machine Identities 的一部分，帮助安全和平台团队在多云和多集群 Kubernetes 环境中管理云原生机器身份，如 TLS、mTLS 和 SPIFFE，增强机器身份管理的可观测性、控制和自动化。

K8s DevOps 平台 Tanzu Application Platform v1.4 发布

近日，K8s DevOps 平台 Tanzu Application Platform v1.4 发布，更新内容：

- 支持 shared ingress issuer；
- 新增命名空间配置器实现安全自动化的命名空间配置；
- 新增 TAP 遥测报告以供查看 TAP 的使用情况；
- 新增 Visual Studio 的 IDE 扩展 —— Tanzu Developer Tools for Visual Studio、支持 External Secrets Operator。

应用连接平台 Tetrate Service Bridge v1.6.0 发布

近日，应用连接平台 Tetrate Service Bridge v1.6.0 发布，更新内容：

- 增加安全域、服务安全设置等安全规则；
- 增加东西向网关改善集群间的服务故障转移；
- 用户界面优化，支持可视化和监控平台和服务活动；

• 新增排障工具，无需集群的访问特权即可排障；
• 支持集群内的多 Istio 环境；
• 支持跨网关和服务代理的 WASM 扩展；
•Skywalking 的后端服务 OAP 代替 Zipkin，用于收集和和查询 trace。

容器安全工具 Qualys Container Security v1.21 发布

近日，容器安全工具 Qualys Container Security v1.21 发布，更新内容：
• 支持为普通和 CI/CD 传感器提供传感器配置文件；
• 支持在传感器配置文件中定义传感器配置；
• 在自动注册表扫描时允许扫描所有镜像。

多云多集群 Kubernetes 管理方案 Tanzu Mission Control 更新

近日，多云多集群 Kubernetes 管理方案 Tanzu Mission Control 更新，更新内容：
• 支持 Pod 安全策略；
• 支持 Tanzu Kubernetes Grid 2.1（包括 ClusterClass）；
• 支持集群组的持续交付；
• 支持从 Git 仓库中安装 Helm chart 到集群中。

OpenShift Container Platform 4.12 发布

近日，OpenShift Container Platform 4.12 发布，更新内容：
• 使用 OVN-Kubernetes 网络插件作为默认网络插件；
• 新增拓扑感知的生命周期管理器用于管理多个单节点 OpenShift 集群的部署和升级；
• 支持通过 cgroup v2 优化资源分配管理；
• 支持快速、低内存占用的 crun 容器运行时；
• 针对断网环境优化基于代理的安装器；
• 支持管理节点层面的防火墙配置；
•支持根据集群中的指标动态扩展默认的 Ingress 控制器；
• 支持为 SR-IOV 设备配置多网络策略；
• 支持 Serverless function 功能；
• 新增 OpenShift Network Observability Operator 进行网络排障；
• 新增 Security Profiles Operator 改善安全态势；

• 支持将生产级 Kubernetes 部署到边缘设备上。

Spot by NetApp 推出 Kubernetes 应用持续交付产品 Ocean CD

Ocean CD 是一个支持多集群的 SaaS 方案，以 Argo rollouts 为引擎，并在上面叠加许多管理功能。

• Ocean CD 允许快速启用智能部署，如金丝雀、蓝绿部署或使用验证和失败策略的简单滚动更新；

• 支持持续验证，根据金丝雀策略定义正确执行回滚和自动行动；

• 提供一个开发者友好型的 UI 界面。

服务网格产品 Kong Mesh v2.1 发布

近日，服务网格产品 Kong Mesh v2.1 发布，更新内容：

• 完成所有下一代策略的实现，包括增加 MeshHTTPRoute、MeshCircuitBreaker、MeshFaultInjection、MeshOPA 等策略；

• 在用户界面中增加了网关视图；

• 支持在 eBPF 模式下配置端口。

Docker BuildKit 0.11 添加供应链安全功能

Docker 已将供应链安全功能添加到 BuildKit（Docker 引擎的构建组件）中，包括出处证明和生成 SBOM（软件物料清单）的能力。

Docker Engine 有多个组件，其中之一是 Moby BuildKit。与原始 Docker 构建相比，它具有许多附加功能。访问这些功能通常是通过一个名为 docker-buildx 的插件，它向 Docker CLI（命令行界面）添加了一个 buildx 命令，Docker Desktop 会自动安装它。

OpenTelemetry PHP 发布测试版

日前，OpenTelemetry PHP SIG 宣布发布 OpenTelemetry PHP v1.0.0beta1。这是 OpenTelemetry PHP 团队 3 年多工作的结晶。

目前，他们正在积极征求开发社区对该库的反馈。试用 Beta 版，用它测试 PHP 应用程序。

Kubefirst 平台改善本地体验和密码管理

近日，开源基础设施应用平台 Kubefirst 发布 1.11 版本。此版本增加了对其本地安装的改进支持，包括新的本地 DNS 实现，为本地安装启用 Traefik 入口控制器，并添加了受信任的本地 TLS 证书。

Kubefirst 是一个自动化平台，旨在提供、配置和连接云应用程序中常用的许多开源服务。它可以部署在本地或 AWS 中。当 kubefirst cluster create 针对一个空的 AWS 账户运行时，许多服务被部署到 Amazon Elastic Kubernetes Service (EKS) 中，包括 Kubernetes、HashiCorp Vault、NGINX 和 Argo CD。这些服务使用 Terraform 部署并与 Atlantis 集成，以进一步自动化基础设施即代码工作流。

Kubernetes Java Client 17.0 提供对 Kubernetes 1.25 的支持

Kubernetes Java Client 17.0 的发布提供了对 Kubernetes 1.25 的支持，提供了动态检索信息的能力。例如，用于监控目的，并允许更改和删除 Kubernetes 集群中的项目。Kubernetes 客户端可以作为命令行 Kubernetes 工具的替代。

Kubernetes 报告表明配置不当的工作负载有所增加

Kubernetes 软件提供商 Fairwinds 发布了他们的 2023 年 Kubernetes 基准报告。该报告表明受调查组织中配置问题恶化的总体趋势，这包括越来越多的组织运行允许 root 访问的工作负载、未设置内存限制的工作负载以及受图像漏洞影响的工作负载。

Kubernetes 2022 年报告表明，在一般情况下，只有不到 10%的工作负载受到不良或不当配置的影响。今年，他们发现在可靠性、安全性和成本治理领域的分布更加多样化。该报告提供了一些假设，说明为什么整体趋势逐年趋向于配置更差的工作负载。

开源安全

Apache Superset 存在 SQL 注入漏洞

Apache Superset 是一款现代化的开源大数据工具，也是企业级商业智能 Web 应用，用于数据探索分析和数据可视化。

在受影响版本 Apache Superset 中，即使用户默认已禁用功能标识 ALLOW _ ADHOC _ SUBQUERY，SQL Alchemy 仍会允许具有数据库读访问权限的用户在 WHERE 和 HAVING 子查询中添加同一数据库下没有访问权限的数据表。

Apache HTTP Server mod_proxy_ajp 模块存在 HTTP 请求走私漏洞

Apache HTTP Server 是一个开源的 HTTP 服务器，mod_proxy_ajp 模块是为 Apache JServ Protocol 版本 1.3（简称 AJP13）提供支持的一个模块。

Apache HTTP Server mod_proxy_ajp 模块处理请求出错时未断开与后端服务的连接，可能将请求直接转发到后端处理转发请求的 AJP 服务器上。

GitLab CE/EE 存在授权绕过漏洞

GitLab 是一款基于 Git 的集成软件开发平台。

GitLab CE/EE 受影响版本在项目成员使用特制链接访问代码仓库时，未授权用户可能会绕过授权读取代码仓库的内容。

Argo CD < 2.5.8 OIDC 存在签名验证绕过漏洞

Argo CD 是一款开源且主要针对 Kubernetes 来做 GitOps 的持续交付工具。

Argo CD 受影响版本在验证令牌是否由其配置的 OIDC 提供商签名时，只基于 groups 授权而不验证 audience 声明（OIDC 提供商在已签名的令牌中包含 aud 声明，指定令牌的预期 audience，即接受令牌的服务），导致 Argo CD 可以接受不合法的令牌。攻击者可以利用颁发给其他 audience 的合法令牌直接访问 Argo CD。

Apache Airflow MySQL Provider 存在任意文件读取漏洞

Apache Airflow 是一个创作、调度和监控工作流的可编程开源平台。

Apache Airflow MySQL Provider 在 4.0.0 以前的版本中当连接 MySQL 时 local_infile 设置为 true（默认未开启），其作用于整个连接，攻击者可能利用客户端信任的 MySQL hook 中的 LOAD DATA LOCAL INFILE 功能读取客户端主机中的文件。

Apache Linkis < 1.3.1 存在任意客户端文件读取漏洞

Apache Linkis 是一个用于将上层应用与底层数据引擎解耦，提供标准化接口的中间件。

受影响版本的 Apache Linkis 在与 MySQL Connector/J 一起使用时，恶意用户在控制连接的 MySQL 服务并设置 jdbc url 中的 allowLoadLocalInfile 参数为 true（默认 false）后能够读取客户端有权限访问的任意本地文件。

攻击者控制 jdbc url 将 allowLoadLocalInfile 参数设置为 true，再通过控制 MySQL 服务读取客户端有权访问的本地文件。

Apache Linkis < 1.3.1 存在反序列化漏洞

Apache Linkis 是一个用于将上层应用与底层数据引擎解耦，提供标准化接口的中间件。

受影响版本 Apache Linkis 在与 MySQL Connector/J 一起使用时，当恶意用户完全控制应用程序连接的 MySQL 服务并设置 jdbc url 中的 autoDeserialize 参数为 true（默认 false）时，可能通过反序列化在客户端执行远程代码。

攻击者控制 jdbc url 将 autoDeserialize 参数设置为 true，再通过控制 MySQL 服务在客户端执行任意远程代码。

Apache InLong 存在任意文件读取漏洞

Apache InLong 是可用于构建基于流式的数据分析、建模等一站式的海量数据集成框架。

在 Apache InLong 受影响版本中，由于 MySQLSinkDTO

.java 中的 filterSensitive 方法未对 allowLoadLocalInfile，allowUrlInLocalInfile，allowLoadLocalInfileInPath 参数进行校验，当恶意用户完全控制应用程序连接的 MySQL 服务并设置 jdbc url 中的 allowLoadLocalInfile，allowUrlInLocalInfile，allowLoadLocalInfileInPath 参数为 true（默认 false）时，可能通过控制 MySQL 服务读取客户端有权访问的本地文件。

hutool 存在反序列化漏洞

hutool 是一款采用 java 开发的工具类库。

该项目受影响版本存在反序列化漏洞，由于 XmlUtil.readObjectFromXml 方法调用 XMLDecoder.readObject 解析 xml 数据，未对输入的 XML 字符串进行安全检查，导致远程攻击者可以通过控制 XML 字符串进而执行任意代码。

Docker 存在容器文件权限校验不严漏洞

Docker 是一个开源的应用容器引擎。

在 Docker 受影响版本中，由于权限认证不当，当 Docker 容器中某个文件 UID/GID 与宿主机用户相同时，在文件被容器内的进程打开时，宿主机相同 UID/GID 的（低权限）用户也具备该文件权限。

当攻击者具有宿主机中与容器内目标文件所属 UID/GID 相同的用户权限时，可以通过遍历/proc 目录获得容器内打开的文件描述符，通过文件描述符，对文件进行读取、写入操作。

Jira Service Management 存在身份验证不当漏洞

Jira Service Management 是 Atlassian 公司开发的帮助台软件。

在受影响版本中存在身份验证不当漏洞，可能导致攻击者冒用其他用户的身份。由于 Jira Service Management 开启用户目录和邮件外发的写入权限时，如果攻击者被包含在用户的 issues、requests 中，或攻击者获取了特定用户 View Request 邮件（如邮件转发），攻击者可以获得这些未登录用户的注册 token，从而冒用其账号。

在开启单点登录的情况下，由于任何人都可以创建账号，项目中的外部客户账号将会受到影响。

Apache AGE <= 1.1.0 SQL 存在注入漏洞

Apache AGE 是用于图形数据库功能的 PostgreSQL 扩展。

Golang 和 Python 的 AGE 驱动程序存在缺陷，当使用 cypher 方法时，在 1.1.0 版本及之前的 PostgreSQL 11 的 AGE 和 PostgreSQL 12 中存在 SQL 注入风险。

由于 cypher()在 Apache AGE 中作为占位符，并未实际运行，导致对于接收的值不能直接进行参数化处理，攻击者可能利用此缺陷，构造恶意 graphName 参数，造成 SQL 注入漏洞，获取数据库敏感信息。

Apache IoTDB-Workbench < 0.13.3 存在身份验证绕过漏洞

Apache IoTDB-Workbench 是 IoTDB （一款针对时序数据的数据管理系统）的可视化管理工具。

受影响版本的 Apache IoTDB-Workbench 能根据默认的 root 用户名构造 JWTToken，导致攻击者能绕过登录限制直接访问工作台。

前沿技术

OpenShift Container Platform 4.12 发布

OpenShift 是红帽的云开发平台即服务（PaaS）。自由和开放源码的云计算平台使开发人员能够创建、测试和运行他们的应用程序，并且可以把它们部署到云中。Openshift 广泛支持多种编程语言和框架，如 Java，Ruby 和 PHP 等。另外，它还提供多种集成开发工具如 Eclipse integration、JBoss Developer Studio、Jenkins 等。OpenShift 基于一个开源生态系统为移动应用、数据库服务等，提供支持。

近日，OpenShift Container Platform 4.12 发布，更新内容：

- 使用 OVN-Kubernetes 网络插件作为默认网络插件；
- 新增拓扑感知的生命周期管理器用于管理多个单节点 OpenShift 集群的部署和升级；
- 支持通过 cgroup v2 优化资源分配管理；
- 支持快速、低内存占用的 crun 容器运行时；
- 针对断网环境优化基于代理的安装器；
- 支持管理节点层面的防火墙配置；
- 支持根据集群中的指标动态扩展默认的 Ingress 控制器；
- 支持为 SR-IOV 设备配置多网络策略；
- 支持 Serverless function 功能；
- 新增 OpenShift Network Observability Operator 进行网络排障；
- 新增 Security Profiles Operator 改善安全态势；
- 支持将生产级 Kubernetes 部署到边缘设备上。

服务网格产品 Kong Mesh v2.1 发布

近日，服务网格产品 Kong Mesh v2.1 发布，更新内容：

- 完成下一代所构想策略的实现，包括增加 MeshHTTPRoute、MeshCircuitBreaker、MeshFaultInjection、MeshOPA 等策略；
- 在用户界面中增加了网关视图；
- 支持在 eBPF 模式下配置端口。

云原生批量计算项目 Volcano v1.7.0 发布

Volcano 是一个基于 Kubernetes 的云原生批量计算平台，也是 CNCF 的首个容器批量计算项目，主要用于 AI、大数据、基因、渲染等诸多高性能计算场景，对主流通用计算框架均有很好的支持。它提供面向高性能负载的调度策略、完善的作业生命周期管理、异构硬件管理、面向高性能负载的性能优化等能力，目前在很多领域都已落地应用。

近日，Volcano v1.7.0 发布，更新内容：

- 增加 Pytorch job 插件；
- 支持为分布式高性能 AI 计算框架 Ray 提供批量调度；
- 丰富调度策略以支持更多长期运行服务的应用场景；
- 支持 Kubernetes v1.25；
- 支持多架构镜像；
- 支持实时查看队列的资源分配信息。

CNI 插件 Kube-OVN v1.11.0 发布

近日，CNI 插件 Kube-OVN v1.11.0 发布，更新内容：

- Underlay 和 Overlay 子网互通；
- 新增 SR-IOV Network Operator 进行自动化网卡配置；
- 支持自定义 VPC 内部负载均衡；
- 新增 vpc-dns CRD；
- 支持默认 VPC 下的 Load Balancer 类型 Service。

云原生证书管理项目 Cert-manager v1.11.0 发布

近日，云原生证书管理项目 Cert-manager v1.11.0 发布，更新内容：

- 支持使用 Azure Workload Identity Federation 进行认证；
- 支持指定 cert-manager 在与 ACME 服务器通信时使用的信任存储；
- 支持 gateway API v1beta1；
- 启用针对 Kubernetes 1.26 的测试。

CNI 插件 Calico v3.25.0 发布

近日，CNI 插件 Calico v3.25.0 发布，更新内容：

• 优化 eBPF 数据平面，确保连接时间负载均衡（Connect Time Load Balancing）在规模更大的、快速变化的环境中工作；

• Felix 组件支持重写内部 readiness/liveness watchdog 的超时；

• Typha 组件支持关闭。

K8s 本地开发工具 Telepresence v2.10.0 发布

近日，K8s 本地开发工具 Telepresence v2.10.0 发布，更新内容：

• 流量管理器支持被团队模式和单用户模式；

• 在 Helm Chart 中添加拉取镜像的 secret；

• OSS Helm chart 将被推送到 telepresence 专有仓库（原先为 datawire Helm 仓库）。

云原生网关 APISIX v3.1.0 发布

近日，云原生网关 APISIX v3.1.0 发布，更新内容：

• 支持将插件的特定字段加密保存到 etcd 中；

• 允许将敏感信息存储在外部安全服务中；

• 实验性地支持基于 gRPC 的 etcd 配置同步；

• 新增基于 Consul 的服务发现功能；

• 增加了一个内置的调试器插件。

云原生分布式块存储 Longhorn v1.4.0 发布

近日，云原生分布式块存储 Longhorn v1.4.0 发布，更新内容：

• 支持 Kubernetes 1.25；

• ARM64 的支持升级为 GA；

• 网络文件系统 NFS 的支持升级为 GA；

• 支持卷快照校验；

• 支持卷 Bit-rot 保护；

• 提高卷复制的重建速度；

• 支持通过删除旧快照来回收空间；

• 支持在线卷扩展；

• 允许用户创建一个停留在一致位置的副本卷；

• 增加卷的 I/O 指标；

• 支持备份和恢复 Longhorn 系统。

分布式应用交付工具 Sealer v0.9.0 发布

近日，分布式应用交付工具 Sealer v0.9.0 发布，更新内容：

• 支持通过 Clusterfile 配置标签、权限、角色、注册表、集群主机别名；

• 支持 ipv4/ipv6 双栈；

• 支持本地注册表的高可用模式；

• 支持基于 buildah 的 OCI 标准；

• Kubefile 支持 Helm 包、k8s yaml 文件、shell 脚本等应用类型。

CNI 插件 Antrea v1.10.0 发布

近日，CNI 插件 Antrea v1.10.0 发布，更新内容：

• 增加 L7 网络策略功能；

• Antrea 的 CRD API 能够在任何 K8s 节点或 External Node 上收集 support bundle 文件；

• 增加对跨集群流量的网络策略的支持；

• 在 Windows 上使用 containerd 作为运行时，antrea-agent 可作为 DaemonSet 运行。

Go1.20 版本发布

2023 年 2 月 2 日，Go1.20 版本正式发布。在距离 Go 1.19 发布六个月后，新版本在性能和构建速度上带来新的提升。本次新版本的更改大都体现于工具链、运行时和库的实现方式中。

该版本主要更新内容：

•Go 1.7 增加了从 slice（切片）到数组指针转换的功能，Go 1.20 对该功能进行了扩展——可直接从 slice 转换成数组。

•标准库 unsafe 包定义了 3 个新函数：SliceData、String 和 StringData。与 Go 1.17 的 Slice 一起，这些函数现在提供了构建和解构 slice 和字符串值的完整功能，而不依赖于它们的精确表示。

• Go 语言规范进行了更新，定义结构体变量的值每次只比较一个字段，字段比较的顺序和字段在结构体里定义的

顺序保持一致。一旦某个字段的值比较出现不一致，就会马上停止比较。

• Comparable 类型（例如普通接口 ordinary interfaces）现在可以满足 comparable 约束，即便类型实参（type argument）不是严格可比较类型。

该版本还包括一些其他更新内容。

开源政策

德国多特蒙德加大开源产业发展力度

德国多特蒙德开源产业兴起已有数年，2016 年多特蒙德公开表示接受开放文档格式（ODF）标准的电子文档，标志着其数字基础设施建设工作正式起步。2018 年，该市制定了全面的开放标准规范体系，并详细说明该市加快数字化发展计划。

2022 年，多特蒙德通过成立自由软件工作组，于 10 月提出建立开放源码协调机构的初步建议，这一建议建立在德国内政部关于加强数字主权的声明之上。12 月 15 日，市议会批准成立新的数字主权和开源协调部门，并发布招聘通知。长期目标是通过即将到来的“开源三巨头”项目与其他德国城市达成合作，为开源治理制定共同政策。目前，多特蒙德市正积极推进其中短期开源产业发展目标，即到 2025 年促使开源的使用和开发成为其公共管理的规范。其协调小组首先就如何在城市管理中更好地实施开源解决方案进行一些研究工作。

一是携手 KGSt 开发开源治理模型。KGSt 是一家私营公司，为德国、奥地利和瑞士的城市提供实际操作的标准化公共服务。携手 KGSt，多特蒙德市有可能开发一个可复制的开源治理模型，可以被 KGSt 的成员重用。该开源治理模型将合作开发，多特蒙德市已经在即将到来的“开源三巨头项目”下与慕尼黑和柏林市启动了一个开源项目。Do-FOSS 倡议的常务董事 Christian Nähle 在参加该市围绕数字化的论坛后，指出有关数字化战略演变的决策过程的重要作用，通过与 KGSt 建立稳定的合作伙伴关系，有助于加强该市的开放管理计划。

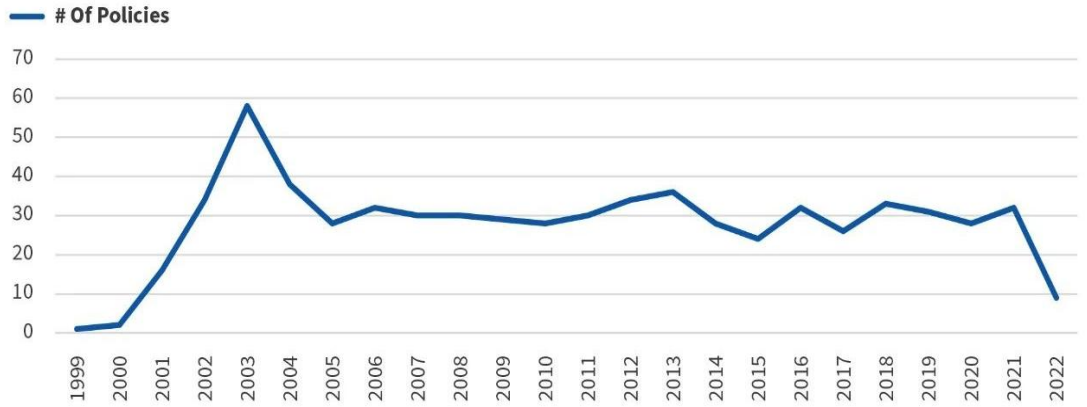
二是与其他城市展开合作。与其他城市的合作也是该项目及实现未来目标的重要组成部分，因为它还为开源治理的发展设定了协作方面。Christian Nähle 认为开放的 CoDE 平台对这次合作至关重要，通过这个针对公共管理部门的存储库，“开源三巨头”将实现工作共享，并可能与项目的未来成员分享。

开源报告

CSIS 发布《政府在助推开源发展方面的作用》

CSIS 政府发布《政府在助推开源发展方面的作用》，汇集研究世界各国政府参与助推 OSS 的方式。研究时间为 2022 年 1 月至 8 月，研究资料主要基于公开发布的信息。

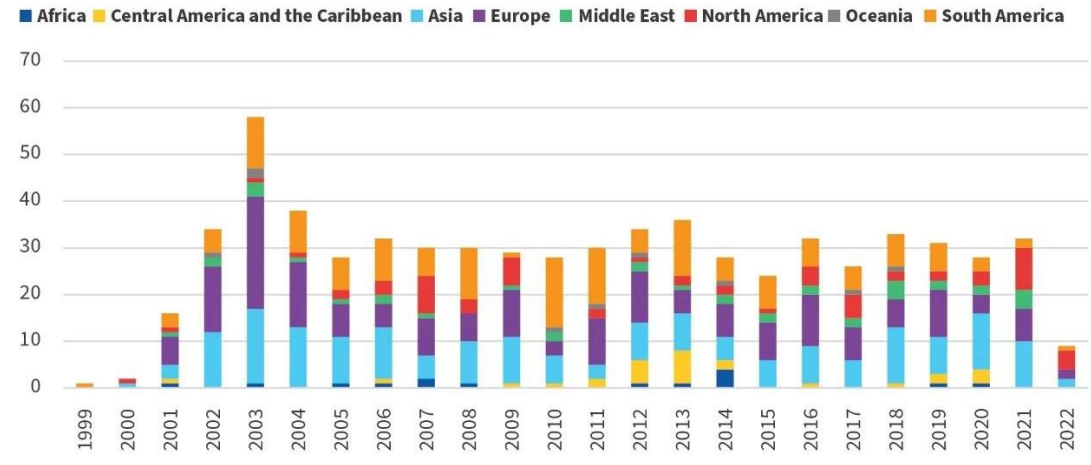
报告显示，1999 年至 2022 年间，各国共出台 669 项开源政策倡议。自 2003 年起，OSS 政策大幅增加（2003 年出台 58 项倡议，是迄今为止最为活跃的一年），增加的政策主要是针对开源安全方面，如图 1。



数据来源:CSIS

图 1 1999 年-2022 年世界各国 OSS 政策倡议

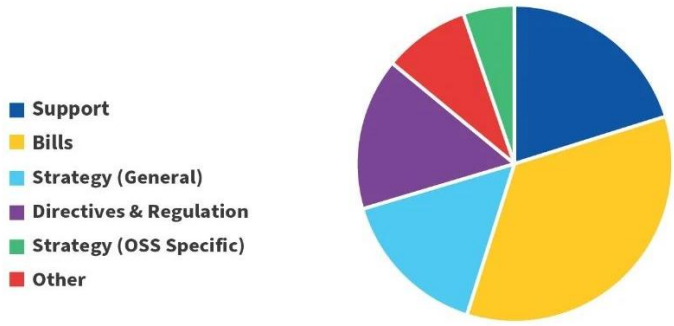
总体来看，政府对促进开源发展的趋势基本稳定，平均每年有 28 项开源政策举措出台，如图 2。



数据来源:CSIS

图 2 1999 年-2022 年世界各国开源政策举措出台情况

政府在助推开源产业发展所出台的政策形式多样。这种支持可以是采取利益声明的形式、政府资助的计划及会议等，如图 3。

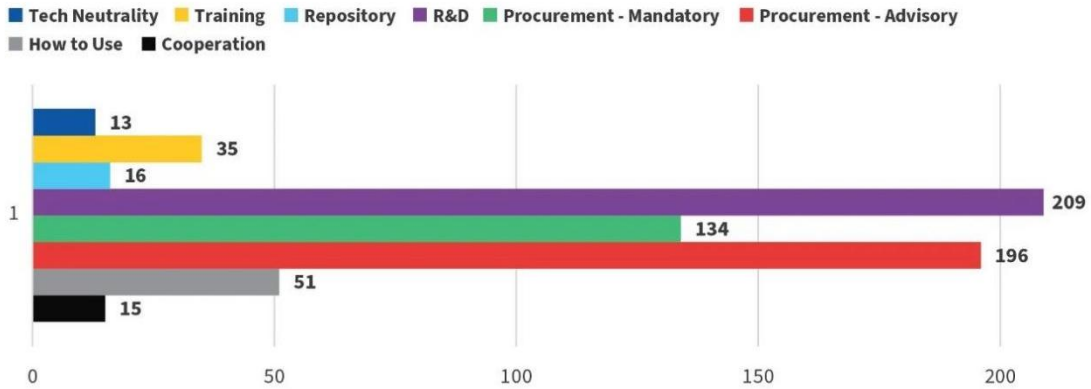


数据来源:CSIS

图 3 政府助推开源产业发展政策形式

在研究中，将已出台政策分为八类，如图 4：

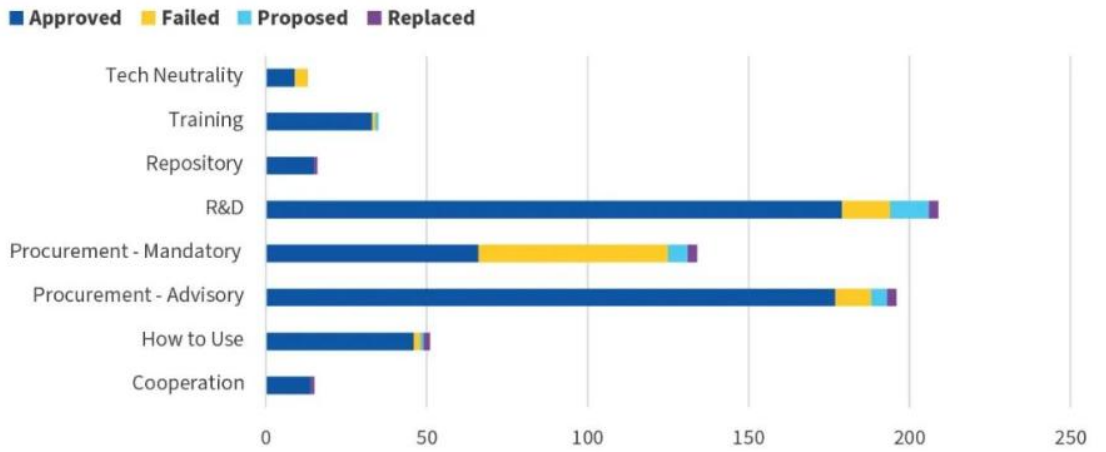
1. 强制性采购决策；
2. 咨询性采购决策；
3. 研发计划（R&D）；
4. 存储库；
5. 政府官员及公民培训；
6. 与私营部门的合作关系；
7. 开发或过渡到 OSS 解决方案的指南；
8. 软件采购的技术中立。



数据来源:CSIC

图 4 已出台政策分类及占比

总体来看，已出台的政策中，采购政策（不区分强制性和咨询性）最为常见，政府出台的研发计划（R&D）也具有普遍性。反映政府通过出台相关政策积极支持开源软件的研发和产业化的意图明显，如图 5。



数据来源:CSIC

图 5 各国政府已出台政策类型

通过对 669 项出台政策的统计分析发现，OSS 是使用最广泛的术语，占总体出台政策的 65%；FLOSS/FOSS 次之，占总体出台政策的 31%，如图 6。

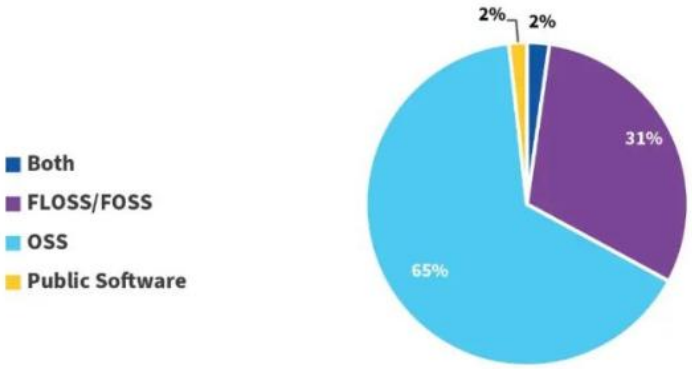


图 6 政策术语分析

进一步分析发现，各国政府在出台助推开源产业发展政策时初衷不同，669 项出台政策涵盖了预算、主权、支持民族工业、现代化、透明度、安全等六大目标，如图 7。

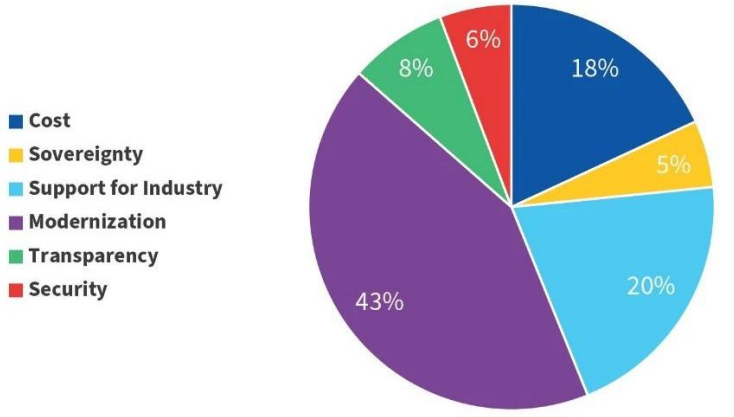


图 7 政府出台助推开源发展的目标分类

政府在助推开源发展的主要原因是为了现代化，43%的政策属于这一类。现代化类别包括数字化、电子政务、互操作性及培训等方面。支持民族工业排在第二位，20%的政策属于这一类。研究 OSS 的预算影响排在第三位，18%的政策属于这一类。8%的政策明确指出政府使用 OSS 有助于提高政府资金使用方式和采购保障方式的透明度。特别是在南美洲，OSS 与主权之间的联系非常紧密，政府将 OSS 视为实现技术主权和自主的一种方式。近年来，对 OSS 解决方案的安全方面的关注越来越多，凸显了安全性越来越受到政策制定者关注，如图 8。

Table 1: Regional Breakdown of Stated Objective* (overlap)

	Cost	Sovereignty	Support for Industry	Modernization	Transparency	Security
Africa	4	1	5	14	1	0
Asia	58	10	82	107	5	14
Central America and the Caribbean	4	4	5	13	1	4
Europe	32	8	35	168	20	3
Middle East	12	3	25	31	3	7
North America	12	2	5	25	13	17
Oceania	3	0	2	9	1	0
South America	58	26	48	64	35	13

*Aggregate polices do not equal 669 as policies were often categorized with more than one objective

CSIS | STRATEGIC TECHNOLOGIES PROGRAM

图 8 各地区政府开源政策目标分类

2022 年 CNCF 基金会和 Linux 基金会开源项目排名

根据本次 CNCF 和 Linux 基金会开源项目的排名情况，可以获取以下信息：

1．在 CNCF 开源项目中，Kubernetes 拥有最多的贡献者；

2．OpenTelemetry 贡献者群体持续扩大。目前，已成长为 CNCF 生态系统中排名第二的项目；

3．Backstage 贡献群体继续增长。由于 Backstage 解决了云原生开发者体验中的一个重要痛点，Backstage 在 2022 年升级到孵化阶段，将继续培育开发者门户生态。

4．GitOps 项目 Argo、服务网格技术 Envoy、Cilium 和 Istio 等排名也位居前列。

2022 年 CNCF 项目排名如下图（气泡面积与项目的数量成正比，y 轴为 pr 和 issue 的数量、x 轴是 commit 的数量）。

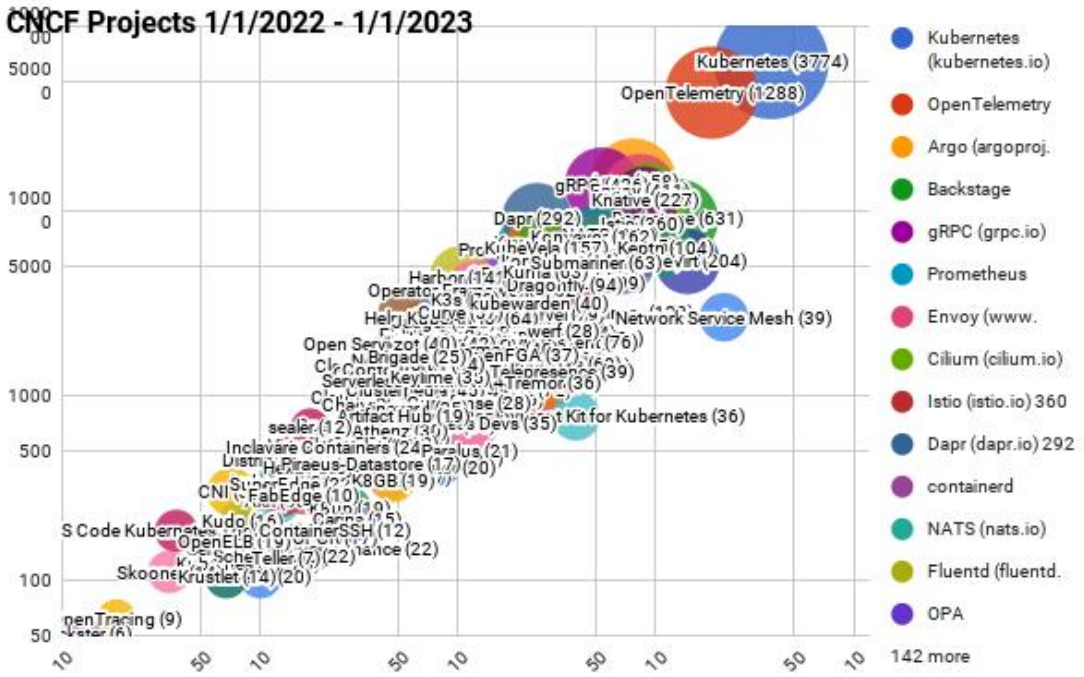


图 1 CNCF 项目－过去 12 个月

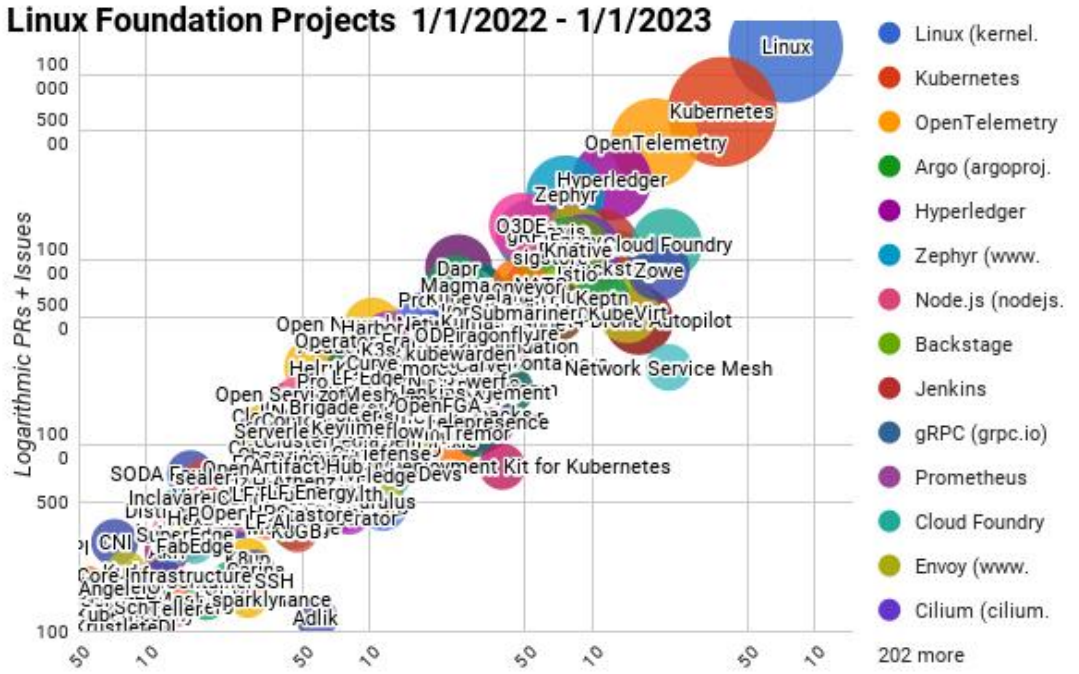


图 2 Linux 基金会项目－过去 12 个月

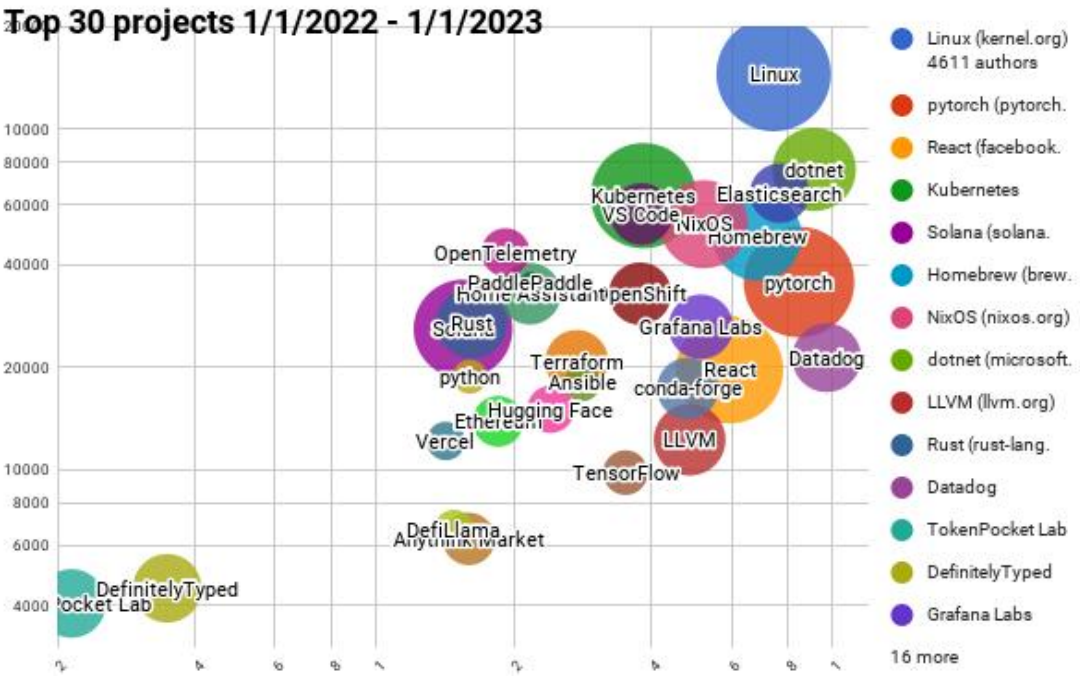


图 3 Top30 开源项目－过去 12 个月

Cilium 发布 2022 年度报告

Cilium 发布 2022 年度报告，该报告旨在汇报一些 Cilium 项目的贡献者和最终用户社区的增长和活动情况。报告记录了 2022 年 Cilium 项目的贡献者增长、版本亮点、用户调查结果、生产落地情况、社区活动，以及 2023 年的发展方向。

该报告的亮点，是如何展示了金融、零售、软件和电信等不同行业的最终用户都意识到了 Cilium 和 eBPF 的优势，并表明它可以在生产环境大规模使用。报告显示，2022 年，Cilium 的贡献和采用均实现大幅增长，Cilium 已成为标准的 CNI，并开启了围绕 Cilium 的项目和集成的生态系统。

此外，报告对 Cilium 2023 年发展方向做出如下总结：

1. 在 2023 年，Cilium service mesh 将发展成熟；
2. 通过 eBPF 捕获的内核数据将帮助周边生态为终端用户建立更好的平台；
3. 供应链安全功能将得到加强。

繁荣开源事业　共享开源价值

地址：北京市北京经济技术开发区科谷一街8号院8号楼22层2201
网址：https://www.openatom.org/home
资金捐赠：sponsorship@openatom.org　项目捐赠：sponsorship@openatom.org