

d.run 平台安全白皮书

d.run 平台是基于 Kubernetes (K8s) 容器化平台构建的算力调度、AI 开放生态平台。为了确保平台的安全性，d.run 平台采用了严格的安全措施。本白皮书旨在向您介绍平台具体安全架构以及措施。

一、平台安全架构

d.run 平台采用容器化微服务架构，基于 Kubernetes 进行应用编排和管理。平台安全架构主要包含以下部分：

1. **身份认证与访问控制：**使用 OAuth2.0 和基于角色的访问控制（RBAC）进行权限管理，确保只有授权用户可以访问特定资源。
2. **数据加密：**所有存储数据和传输数据均使用 AES-256 和 TLS1.3 进行加密，以防止数据泄露和篡改。
3. **日志与监控：**集成 OpenTelemetry 进行全方位日志记录，并使用 Prometheus 和 Grafana 进行实时监控，确保安全事件的可追溯性。
4. **容器安全：**采用 Pod Security Policies 限制容器的权限，使用镜像签名确保镜像来源可信，并通过容器运行时安全策略防止恶意代码运行。
5. **网络安全：**基于 Istio 实现零信任网络，确保微服务之间的安全通信，并使用 CNI 插件强化容器网络隔离。
6. **模型安全：**针对大模型应用的安全需求，d.run 平台采用一系列措施保障模型的完整性和可信性。

二、身份与访问控制

d.run 平台采用多层次身份认证机制，确保用户身份的安全性：

1. **OAuth2.0+OIDC 进行单点登录（SSO）认证，**使用户可以安全访问多个服务，无需重复输入凭据。
2. **基于角色的访问控制（RBAC），**允许管理员定义不同角色的权限，确保用户只能访问与其职责相关的资源。
3. **多因素认证（MFA），**要求用户在登录时提供额外的身份验证信息（如短信验证码或硬件令牌），以增强账户安全性。
4. **API 访问密钥管理，**提供短周期 Token 和细粒度权限控制，确保 API 访问受到严格限制，防止未授权调用。

三、数据加密

1. **传输加密：**所有 API 通信均通过 TLS1.3 加密，确保数据在传输过程中不会被拦截或篡改。

2. **存储加密：**所有存储的数据均使用 AES-256 进行加密，保证数据的机密性，即使磁盘被盗或丢失，数据仍然无法被访问。
3. **密钥管理：**使用 Kubernetes Secrets 和 HashiCorp Vault 进行密钥管理，定期轮换密钥，并限制密钥访问权限。

四、数据备份与恢复

1. **定期数据快照：**每天进行增量备份，每周进行完整备份，并存储于多个地理区域，以防止数据丢失。
2. **灾难恢复（DR）方案：**采用异地备份和故障自动转移策略，确保服务在遭遇灾难时可以迅速恢复。
3. **数据完整性校验：**使用哈希算法定期校验数据完整性，防止数据篡改或损坏。

五、网络安全

d.run 平台采用零信任安全架构，确保平台网络安全：

1. **东西向流量安全：**Istio Service Mesh 通过 mTLS（双向 TLS）加密微服务之间的通信，并提供流量控制、认证和授权。
2. **南北向流量安全：**WAF（Web 应用防火墙）过滤恶意流量，防止 SQL 注入、XSS 等常见攻击。
3. **DDoS 防护：**通过 Kubernetes Ingress 和 CDN 进行流量清洗，自动检测和缓解分布式拒绝服务攻击。
4. **防火墙策略：**使用 Kubernetes Network Policy 规则限制 Pod 之间的访问，确保最小权限原则。

六、容器与计算安全

d.run 平台在容器层面采用多种安全策略，以保障计算安全：

1. **镜像安全：**所有容器镜像在部署前都需经过 Trivy 扫描，检测已知漏洞，并进行修复。
2. **Pod 安全策略：**限制特权容器，避免使用 root 权限运行服务，以减少被攻击的可能性。
3. **沙箱运行时：**支持 gVisor 和 Kata Containers，在容器与主机之间增加额外的安全隔离层。
4. **实时威胁检测：**使用 Falco 监控容器运行时行为，检测异常访问、恶意进程和可疑网络流量。

七、大模型安全

d.run 平台针对 AI 大模型的安全性采取了以下措施：

1. **模型完整性保护：**通过模型签名和哈希校验，确保模型文件未被篡改。

2. **模型访问控制：**采用 RBAC 和 API 访问令牌限制对模型的调用，防止未经授权的访问。
3. **推理安全：**使用沙箱环境执行 AI 推理任务，防止恶意代码在推理过程中执行。
4. **数据隐私保护：**采用同态加密和差分隐私技术，防止 AI 训练数据泄露。
5. **对抗攻击防护：**检测和缓解对抗样本攻击，防止恶意输入导致模型错误推理。

八、监控与审计

1. **日志采集：**集成 OpenTelemetry，对所有 API 调用、用户操作和系统事件进行日志记录，确保可追溯性。
2. **安全事件监控：**使用 SIEM（安全信息和事件管理）工具分析日志，检测潜在的安全威胁，并生成自动警报。
3. **异常检测：**利用 AI 识别异常行为，例如异常登录、权限提升或恶意代码执行，并自动采取响应措施。
4. **操作审计：**记录所有用户操作，满足合规要求，提供可验证的审计日志。

九、安全认证

d.run 平台遵循国际与行业安全标准，目前已取得 **ISO/IEC27001:2022** 认证。

d.run 平台采用适当的符合业界标准的安全防护措施，确保平台在算力租赁、大模型服务和 AI 应用管理等场景下的安全性和稳定性。未来，我们将持续优化安全机制，以应对不断变化的安全威胁，并保障用户的数据和计算安全。

版本日期：2025 年 5 月