智享 | 知识分享行动

Docker 最佳实践 [201708v2]

镜像

- **减少层次数量** — 合并成单行命令
- **单层最小化** — 命令结束执行清理
- **使用构建变量** — 相对微小变化，如：版本号
- **使用临时变量**
  - 构建过程中使用 export
  - 减少不必要使用 ENV
- **标签命名清晰** — 容易找到 build-id 或代码 commit-id

容器

- **轻量 / 一次性 / 用完即可丢弃**
  - 易于扩容缩容
  - 易于替换更新
- **可收容僵尸进程的 PID1** — 参数 run --init
- **用数据卷存储共享数据**
- **单容器单功能单进程**
- **日志轮转** — 使用 –-log-opt 配置

安全

- **限制外来网络访问** — 参数 run --network=isolated
- **默认不信任外来镜像**
  - 只是用官方镜像
  - 只是用自编译程序
- **限制文件系统访问**
  - 参数 run --read-only
  - 参数 -v x:y:ro
- **限制内存使用量** — 参数 run -m ... --memory-swap ...
- **进行安全扫描**
- **最小权限原则** — 不使用 root — 使用 USER ...
- **放弃未使用功能权限** — 参数 run --cap-drop=all --cap-add=...
- **管理凭据和密码** — 工具：vault

镜像仓库

- **选择存储后端**
  - 对象存储提供更好的可用性和操作便捷性
  - 不要使用 NFS
- **执行垃圾整理** — bin/registry garbage-collect

应用

- **日志默认写标准输出**