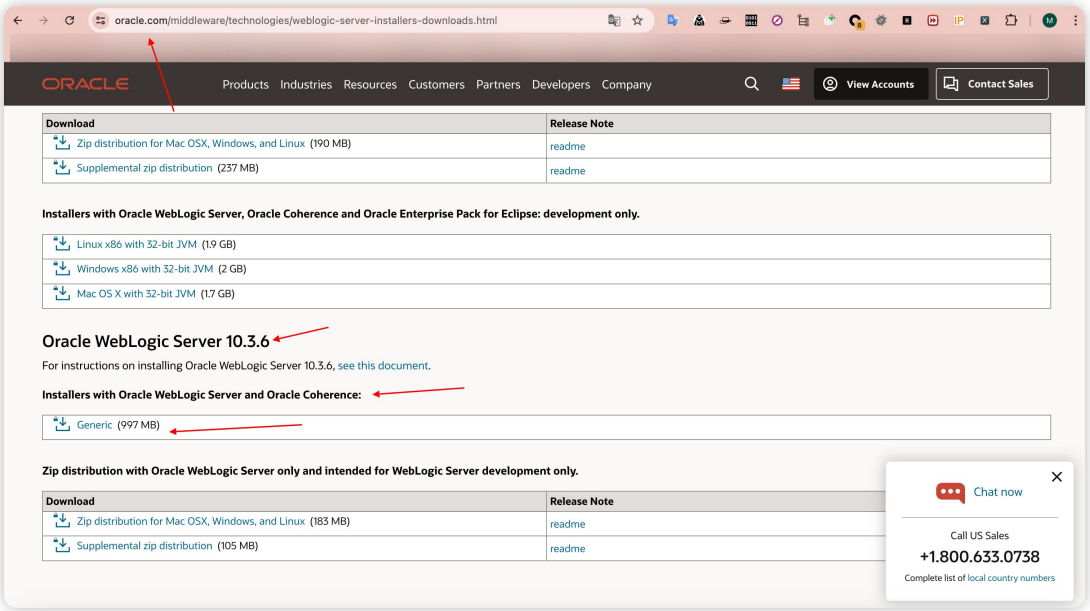
利用 QAX-Ateam 的 WeblogicEnvironment 搭建 Weblogic 漏洞复现环境踩到的坑（M1 Mac 系统）

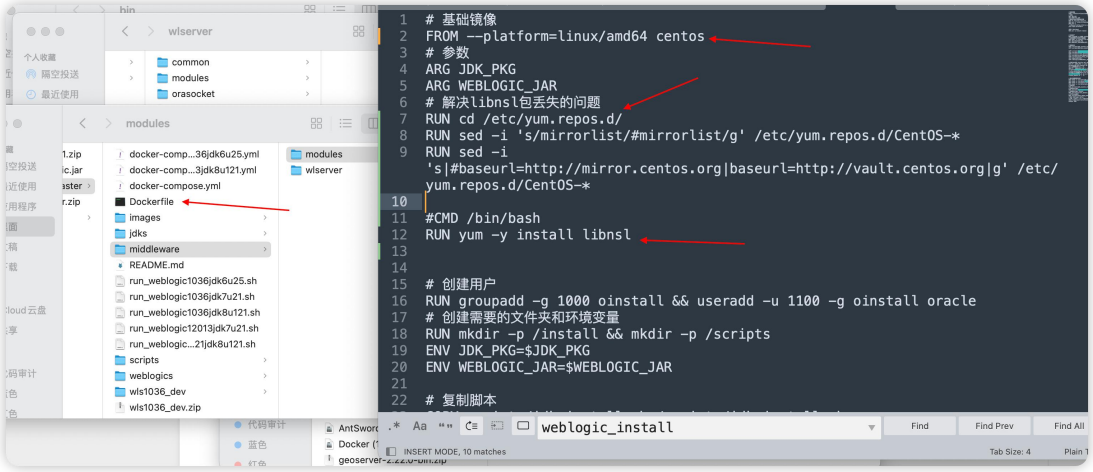
github 项目链接：https://github.com/QAX-A-Team/WeblogicEnvironment

前面基本跟项目描述一致。
创建一个 jdks，weblogics 文件夹，把对应的 jdk 和 weblogic 安装包下载好。

第一个：安装包要一致
因为我当时是在 M1 Mac 上的实验，下了 10.3.6 Weblogic 版本的 m1 安装包，但是下来的是 zip，而且跟项目描述的也不一致，这里我们要下完整的 generic 安装 jar 包。



第二个：docker build 环境要指定平台+部分变动
因为 M1 特殊情况吧，在 docker 跑 centos 安装 libnsl 的时候会出现报错中断的问题，要改一下配置文件。
M1 搭建项目过程中的 dockerFile 变动如下



基础镜像 指定平台架构

FROM --platform=linux/amd64 centos

参数

ARG JDK_PKG

ARG WEBLOGIC_JAR

解决 libnsl 包丢失的问题 通过设置 sed 等就可以正常跑 libnsl 安装了

RUN cd /etc/yum.repos.d/

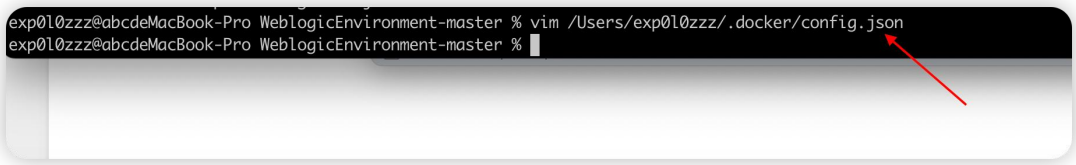
RUN sed -i 's/mirrorlist/#mirrorlist/g' /etc/yum.repos.d/CentOS-*

RUN sed -i 's|#baseurl=http://mirror.centos.org|baseurl=http://vault.centos.org|g' /etc/yum.repos.d/CentOS-*

#CMD /bin/bash 这个是网上顺便粘贴在一起的，目前来看不影响编译

RUN yum -y install libnsl

然后 M1 docker 跑的时候还会爆一个问题就是



/Users/名字/.docker/config.json 路径会爆错终止

原文件内容：

```
{
	"auths": {
		"https://index.docker.io/v1/": {}
	},
	#"credsStore": "desktop",
	"currentContext": "desktop-linux",
	"plugins": {
		"debug": {
			"hooks": "exec"
		},
		"scout": {
```

```
                "hooks": "pull,buildx build"
            }
        },
        "features": {
            "hooks": "true"
        }
}
```

变动内容： 把 credsStore 字段删除，跟我上面一样加个#井号注释掉也不影响编译，只是命令敲下去会报个井号异常错误。

```
{
        "auths": {
            "https://index.docker.io/v1/": {}
        },
        "currentContext": "desktop-linux",
        "plugins": {
            "debug": {
                "hooks": "exec"
            },
            "scout": {
                "hooks": "pull,buildx build"
            }
        },
        "features": {
            "hooks": "true"
        }
}
```

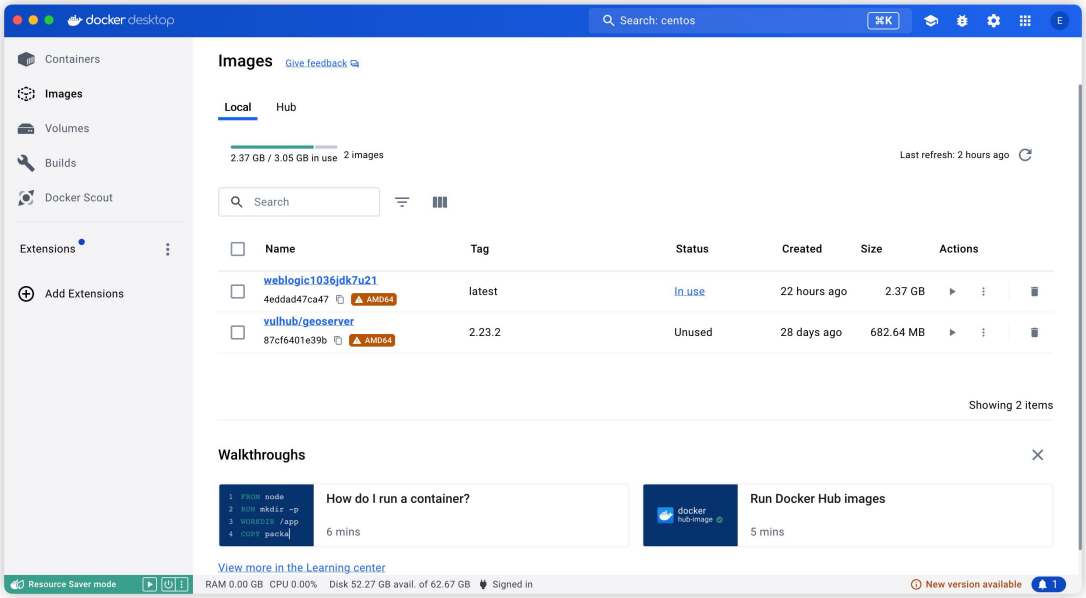
最后一步：正常使用 docker build 编译镜像即可

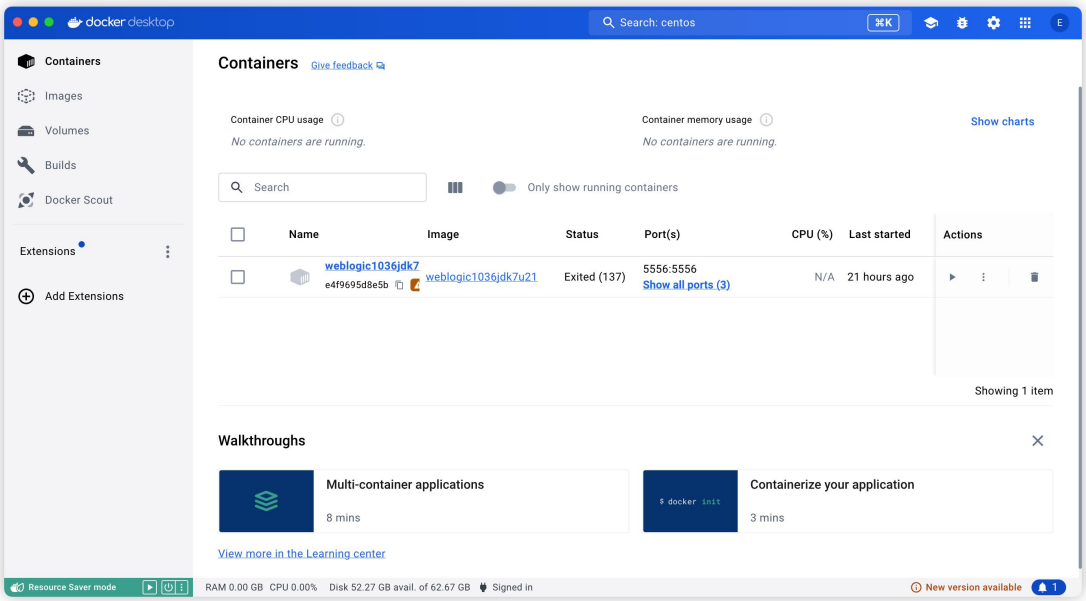
sudo docker build --build-arg JDK_PKG=jdk-7u21-linux-x64.tar.gz --build-arg WEBLOGIC_JAR=wls1036_generic.jar -t weblogic1036jdk7u21 .

docker 启动镜像

sudo docker run -d -p 7001:7001 -p 8453:8453 -p 5556:5556 --name weblogic1036jdk7u21 weblogic1036jdk7u21

因为是 Mac 环境，Mac 下还有个 Docker Destop，在上面 GUI 直接启动也可以





疑难杂症：
如果在你启动这个 webloigc 镜像过程中，你突然发现你之前就已经启动过一个 weblogic 还没关闭的话。假设是打开是 14 版本的 weblogic，在命令终止关闭以后。
再次访问相同路径，自然就会进入到 docker 环境的 1036 版本的 weblogic，但是你可能会出现输入正确账号密码以后，只是刷新了页面，并没有成功登陆。

解决办法是：清除 cookie 缓存

出现的原因：猜测是不同版本 weblogic 加密密码或者 cookie 等等不相同，导致出现这种冲突。

如何发现的：刚好我就是在编译过程中就有这么一个情况，在更换浏览器打开界面输入账号密码以后，又成功登陆了，所以猜测就是缓存 cookie 这些有冲突。