

参数介绍：

- 1. docker run：Docker 的命令，用于从指定的镜像启动一个容器。
- 2. -d：表示在“分离模式”（detached mode）下运行容器，即容器在后台运行，并返回容器的 ID。
- 3. --name my_web：给这个容器指定一个名字，叫做 my_web。这样，之后你可以通过这个名字来管理这个容器。
- 4. --restart always：这个参数设置了容器的重启策略。always 表示无论容器退出的状态码是什么，Docker 都会尝试重新启动这个容器。
- 5. -p 7090:8080：端口映射。这表示将宿主机的 7090 端口映射到容器的 8080 端口。这样，当你访问宿主机的 7090 端口时，实际上会访问到容器内的 8080 端口。
- 6. -v /data/tomcat/data:/usr/local/tomcat/webapps/ROOT/：卷挂载。这表示将宿主机的 /data/tomcat/data 目录挂载到容器的 /usr/local/tomcat/webapps/ROOT/ 目录。这样，容器对这个目录的读写操作实际上是在操作宿主机的对应目录。

查找镜像：

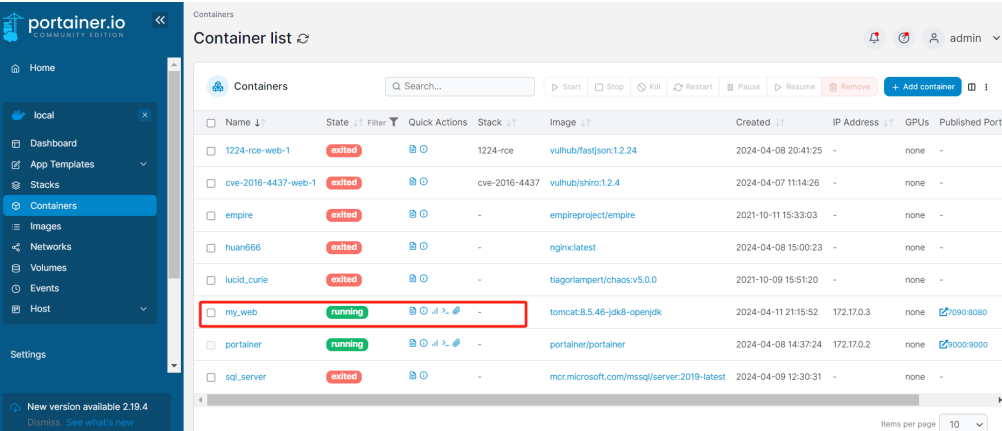
docker search tomcat

docker pull tomcat:8.5.46-jdk8-openjdk

物理机创建挂载目录：mkdir -p /data/tomcat/data，目录赋予可读写执行权限

docker run -d --name my_web --restart always -p 7090:8080 -v

/data/tomcat/data:/usr/local/tomcat/webapps/ROOT/ tomcat:8.5.46-jdk8-openjdk




经过访问，tomcat服务部署成功



冰蝎特征分析

版本：2.0

特征：accept 里面有个 q=.2



2.0.pcapng

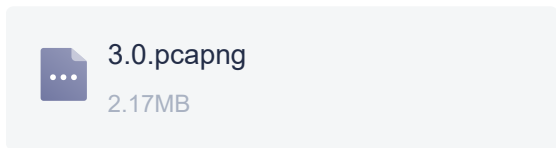
830.49KB

No.	Time	Source	Destination	
1485	9.311193	192.168.192.178	192.168.192.132	GET /shell.jsp?pass=720 HTTP/1.1
1488	9.311574	192.168.192.132	192.168.192.178	User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0
1489	9.311678	192.168.192.178	192.168.192.132	Safari/535.1 QQBrowser/6.9.11079.201
1491	9.312471	192.168.192.178	192.168.192.132	Host: 192.168.192.132:7090
1492	9.312772	192.168.192.132	192.168.192.178	Accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
1499	9.316407	192.168.192.132	192.168.192.178	Connection: keep-alive
1500	9.318386	192.168.192.178	192.168.192.132	HTTP/1.1 200
1503	9.318881	192.168.192.132	192.168.192.178	Set-Cookie: JSESSIONID=439F68E232E9C0B06113109A65664E44; Path=/; HttpOnly
1505	9.323206	192.168.192.132	192.168.192.178	Content-Type: text/html; charset=ISO-8859-1
1506	9.324698	192.168.192.178	192.168.192.132	Content-Length: 16
1507	9.325085	192.168.192.132	192.168.192.178	Date: Thu, 11 Apr 2024 13:35:30 GMT
1508	9.327061	192.168.192.132	192.168.192.178	94388645faac3a24
1517	9.335209	192.168.192.178	192.168.192.132	ET /shell.jsp?pass=460 HTTP/1.1
1519	9.335374	192.168.192.178	192.168.192.132	User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/13.0
1520	9.335374	192.168.192.178	192.168.192.132	Safari/535.1 QQBrowser/6.9.11079.201
1521	9.335374	192.168.192.178	192.168.192.132	Host: 192.168.192.132:7090
				Accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
				Connection: keep-alive

> Frame 1	0000	00 0c 29 f0 ab 7f 00 0c	29 3b 79 f4 08 00 45	HTTP/1.1 200
> Ethernet	0010	01 46 de 5d 40 00 80 06	00 00 c0 a8 c0 b2 c0	Set-Cookie: JSESSIONID=4BE3FF3BFEB18A90290E4D30A46338B42; Path=/; HttpOnly
> Internet	0020	c0 b4 d6 45 1b b2 c9 d4	16 25 e9 74 7c f2 50	Content-Type: text/html; charset=ISO-8859-1
> Transport	0030	20 14 03 c1 00 00 47 45	54 20 2f 73 68 65 6c	Content-Length: 16
> Hypertext	0040	2e 6a 73 70 3f 70 61 73	73 3d 3f 32 30 20 48	Date: Thu, 11 Apr 2024 13:35:30 GMT
	0050	54 50 2f 31 2e 31 0d 0a	55 73 65 72 2d 41 67	
	0060	6e 74 3a 20 4d 6f 7a 69	6c 6c 61 2f 35 2e 30	
	0070	28 57 69 6e 64 6f 77 73	20 4e 54 20 36 2e 31	

版本3.0:

特征: Content-Type: application/octet-stream、UA头比较老: Trident

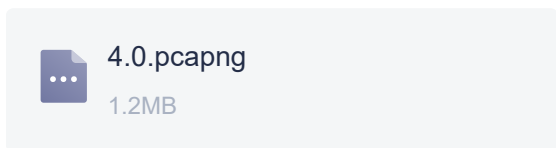


No.	Time	Source	Destination	
1302	7.242187	192.168.192.132	192.168.192.178	POST /shell3.0.jsp HTTP/1.1
1303	7.242276	192.168.192.178	192.168.192.132	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
1304	7.243004	192.168.192.178	192.168.192.132	Accept-Encoding: gzip, deflate, br
1305	7.243142	192.168.192.178	192.168.192.132	Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
1306	7.243142	192.168.192.178	192.168.192.132	Content-Type: application/octet-stream
1307	7.243142	192.168.192.178	192.168.192.132	Referer: http://192.168.192.132:7090/LGS.jsp
1308	7.243142	192.168.192.178	192.168.192.132	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:79.0) Gecko/20100101 Firefox/79.0
1309	7.243142	192.168.192.178	192.168.192.132	Cache-Control: no-cache
1310	7.243142	192.168.192.178	192.168.192.132	Pragma: no-cache
1311	7.243784	192.168.192.132	192.168.192.178	Host: 192.168.192.132:7090
1312	7.243849	192.168.192.132	192.168.192.178	Connection: keep-alive
1313	7.247295	192.168.192.132	192.168.192.178	Content-Length: 8128
1314	7.247414	192.168.192.132	192.168.192.178	Cookie: JSESSIONID=619F4D0B0444B3FC9F4D5698100F4EF7
1315	7.247448	192.168.192.178	192.168.192.132	
1386	7.316075	192.168.192.178	192.168.192.132	
1387	7.316385	192.168.192.178	192.168.192.132	

> Frame 1	0000	00 0c 29 f0 ab 7f 00 0c	29 3b 79 f4 08 00 45	eFmJvQ1Au4I5SDQf5CnRqfL0iV7LxXUI6DPEF2fQ100R9Gh3wDxA9o9z/Aytfc+HdCUX9NH0k0aAM6MK+XkXQ1Q
> Ethernet	0010	03 64 de a9 04 1b b2 00 18	00 00 c0 a8 c0 b2 c0	y1860dbxfY0Q41C10/aGe1V6djp3TRima4k1TznbgAOwguPcmPn1ahaRCISwB3H2gnCFqq8pady+U19dSV/+OKC0f
> Internet	0020	c0 b4 d6 45 1b b2 00 18	16 25 e9 74 7c f2 50	TrSPde0Adz9Uoh/MJ3ffHayNbnprRd9U882nZd242z0VK/U+UL89f1PnLqMK6G3n1jvN5rDYvuuUjkrWSp+1Gicu
> Transport	0030	20 14 05 df 00 00 38 54	46 71 56 34 45 57 51	bpQPfP/OC3ETX8zmQmg3d+Fw1Xds9Hr471tzeT7Z1K2I291rWle+rm3Kjvkt0t9Kw8NVXUq1Wjt9655o1Xn1lmsC
> [7 Reas	0040	46 5a 51 64 49 32 5a 32	62 42 4d 5a 31 30 74	NT18K0SADAg8tZd6pAcA29LcxuYm6tYKGI0ppgeZefh9p4dE0myvs1kc+Y8PudqTIdog1nmbhclXqpH9Y4KwG
> Hypertex	0050	58 4f 2f 71 5a 31 45 37	54 30 50 52 73 5a 43	CaHfPpFTMR0jpyk7421asQUtmkspc050ymM1G1wR80R6nw1BoV12Xpxp/1UR8nFhlpV871KLywAwEAp74PCr+
> Data (8	0060	41 57 62 4a 33 69 64 37	78 7a 54 4b 67 4e 67	4B2SVdG6C9nwa410x5CgHNaWQ15swGK82jVVDYIM5tR5xL03E3zdvHRXTMGRT4CNMLkP2CG2/kDlgeb0FLYOUFgib1

版本4.0

特征: 10个内置UA头、Accept: application/json, text/javascript, */*; q=0.01



POST /shell4.0.jsp HTTP/1.1	
Accept: application/json, text/javascript, */*; q=0.01	
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7	
Referer: http://192.168.192.132:7090/XK1YI.jsp	
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36	
Content-Length: 6132	
Host: 192.168.192.132:7090	
Connection: Keep-Alive	
Accept-Encoding: gzip	
....29ftc.e9'v	
..0.@...V.M.L1..Qb338fu.T.X.Y..S.*QX...e5g82<'..ZKYS0.db2.V\A..@4e!~S....X\RM6@G.]U.geiE.@^Z..v.Z.J39a7.D.	
\AAce&y.RDXI .[.].W..WA^2214..E.WAPce3f.@AP .c5b.[[. .	
4e0..0db519=9bc421309wdb".XDTM U[. .aM...R&L[Y..F2e >9ke1?d-2 ce2T.CWW.db.LuXT...Y.]U.5.. \	
.. ..UC..^X..Mf.K[[.'A\ WWK]ib'd185ve-4d..o'V.F5Sy...e^6.v^1.).P[w]2.ACVI.N...V0.v.)0um.	
SR. .	
.a] FB6..w?VQC..5.1J\S.'SE&[G]VSV<[v0..*sT.kx.0' C'.T...zZ!g_s. 0b.hYmR.B@0.ec.V.]SW.Q..n~	
{et..QC.[.2laewpe'#.,w.OQV..	
a6{Q.S3.*wcs;.C@...V!+Zy.uFS/)p...~h.	