Ad04

(HCL Connections) Admin Toolbox

Christoph Stoettner

@stoeps

Bruges, 24.05.2022

Christoph Stoettner

☎ +49 173 8588719

stoeps@vegardit.com

linkedin.com/in/christophstoettner

stoeps.de

christophstoettner

@stoeps

HCL Ambassador

- Senior Consultant at Vegard IT
  - Linux (Slackware) since 1995
  - IBM Domino since 1999
  - IBM Connections since 2009
- Experience in
  - Migrations, Deployments
  - Performance Analysis, Infrastructure
- Focusing in
  - Monitoring, Security
- More and more
  - DevOps stuff

Open Source Software - Give Something Back

- Support Open Source developers!
    - Tons of options, contribute, test, document, or recommend tools

> *If we want to see a lively open source scene, we need to keep actively using open source software, and not be afraid of trying out new ones. If we find something good, we shouldn’t hesitate to recommend it to others, so they can also benefit from it.*

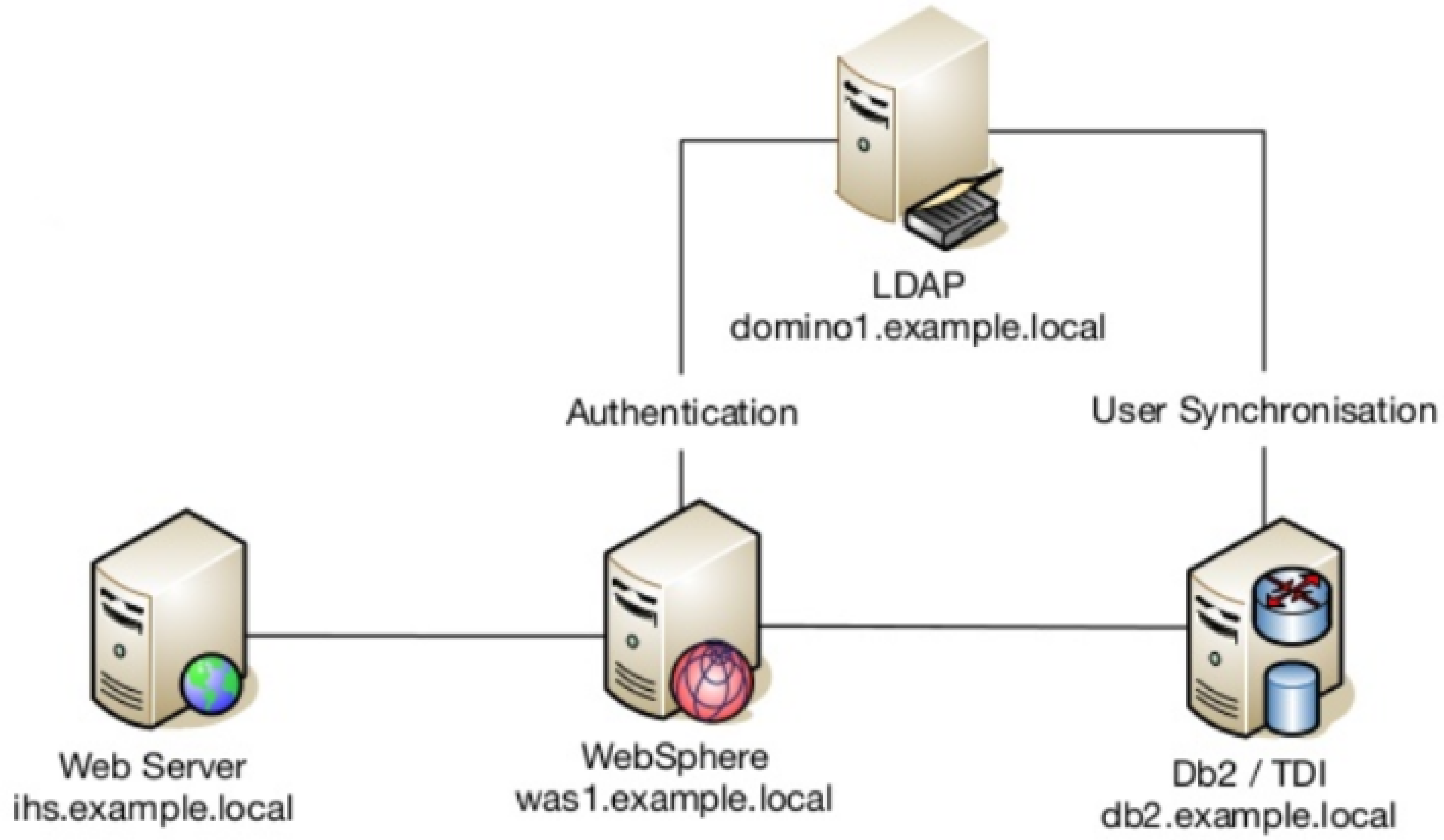
https://www.hongkiat.com/blog/open-source-community-give-back/

HCL Connections Admin Challenges

- Huge backend options
  - Database (DB2, Oracle MS SQL)
  - Java backend (WebSphere Application Server)
  - Container (Component Pack, PFKAP — Product Formerly Known as Pink)
    - Dependencies not documented
    - multiple places to search for log files
- Multiple options to access Connections
  - Browser, Plugins, Mobile App
- Security
  - Single Sign On
    - SPNEGO / Kerberos, SAML, LtpaToken
  - SSL / TLS

The Old IBM View

- Often got this deployment plans in the first years
- Lotus Wiki (official documentation)



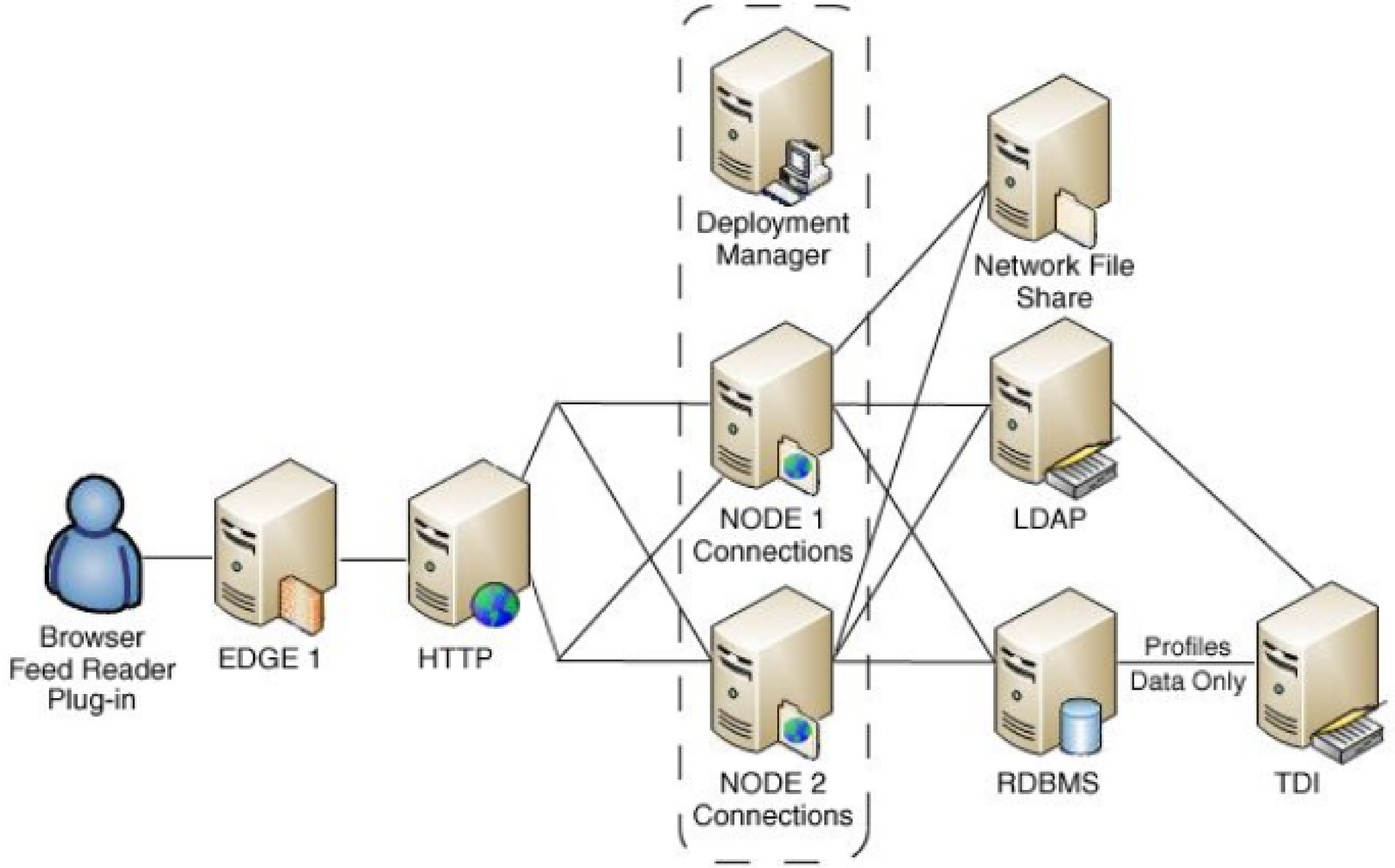
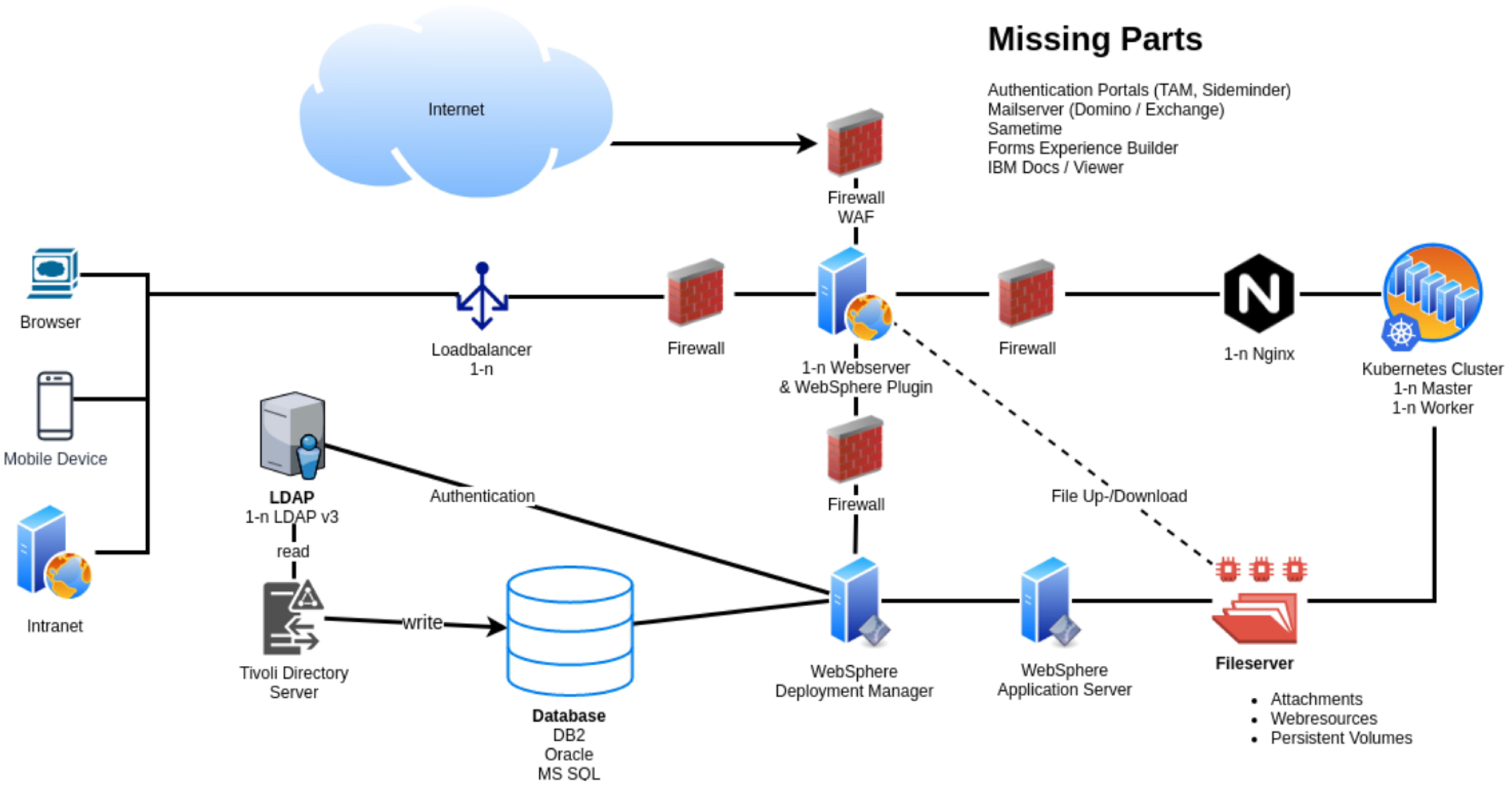


Figure 1. Image IBM

More Realistic

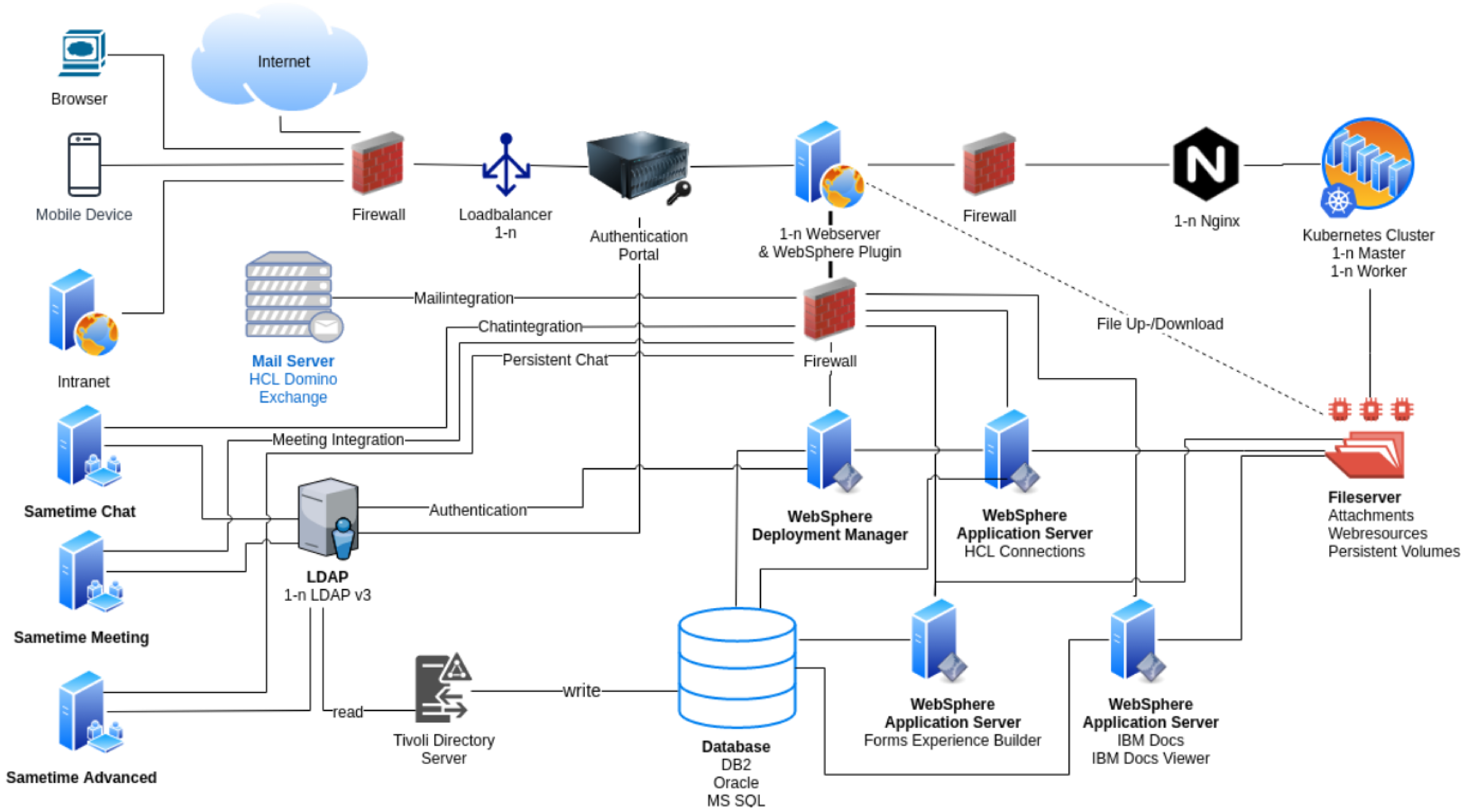


- Attachments
- Webresources
- Persistent Volumes

Missing Parts

Authentication Portals (TAM, Sideminder)
Mailserver (Domino / Exchange)
Sametime
Forms Experience Builder
IBM Docs / Viewer

And Now Mostly Meeting Reality



Check After Installation And Updates

- Is the environment working as expected
    - Smoke testing
- Does it scale for your planned user count
    - Load testing

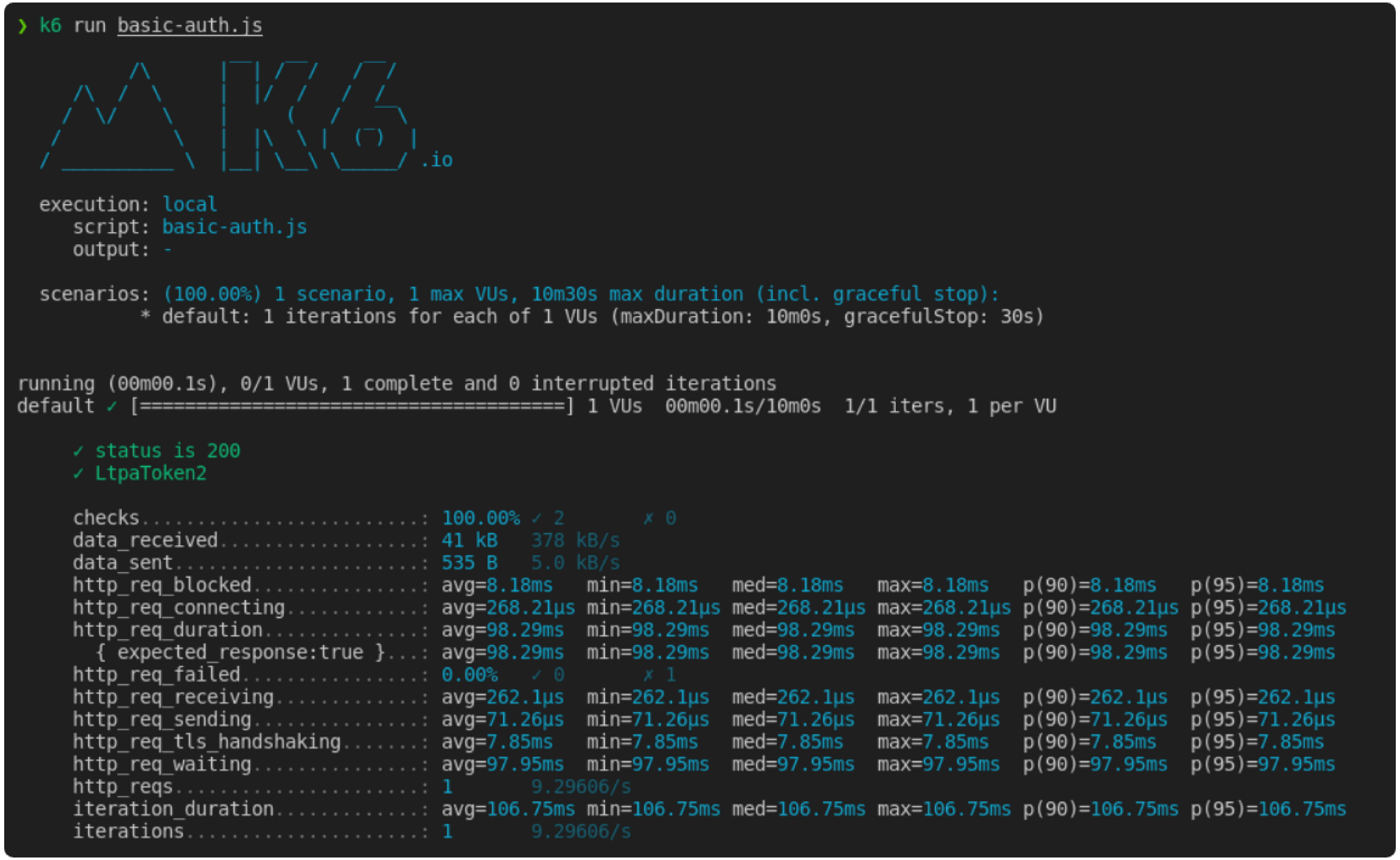
Tools For Testing

- K6
  - https://k6.io
  - Windows, Linux, macOS, Docker
  - JavaScript
  - Load testing, chaos and reliability testing, performance testing
- Selenium
  - Automates browsers (needs Chrome webdriver, Firefox webdriver)
  - Cross browser & smoke testing
  - https://www.selenium.dev
- Apache JMeter
  - https://jmeter.apache.org

K6 Example

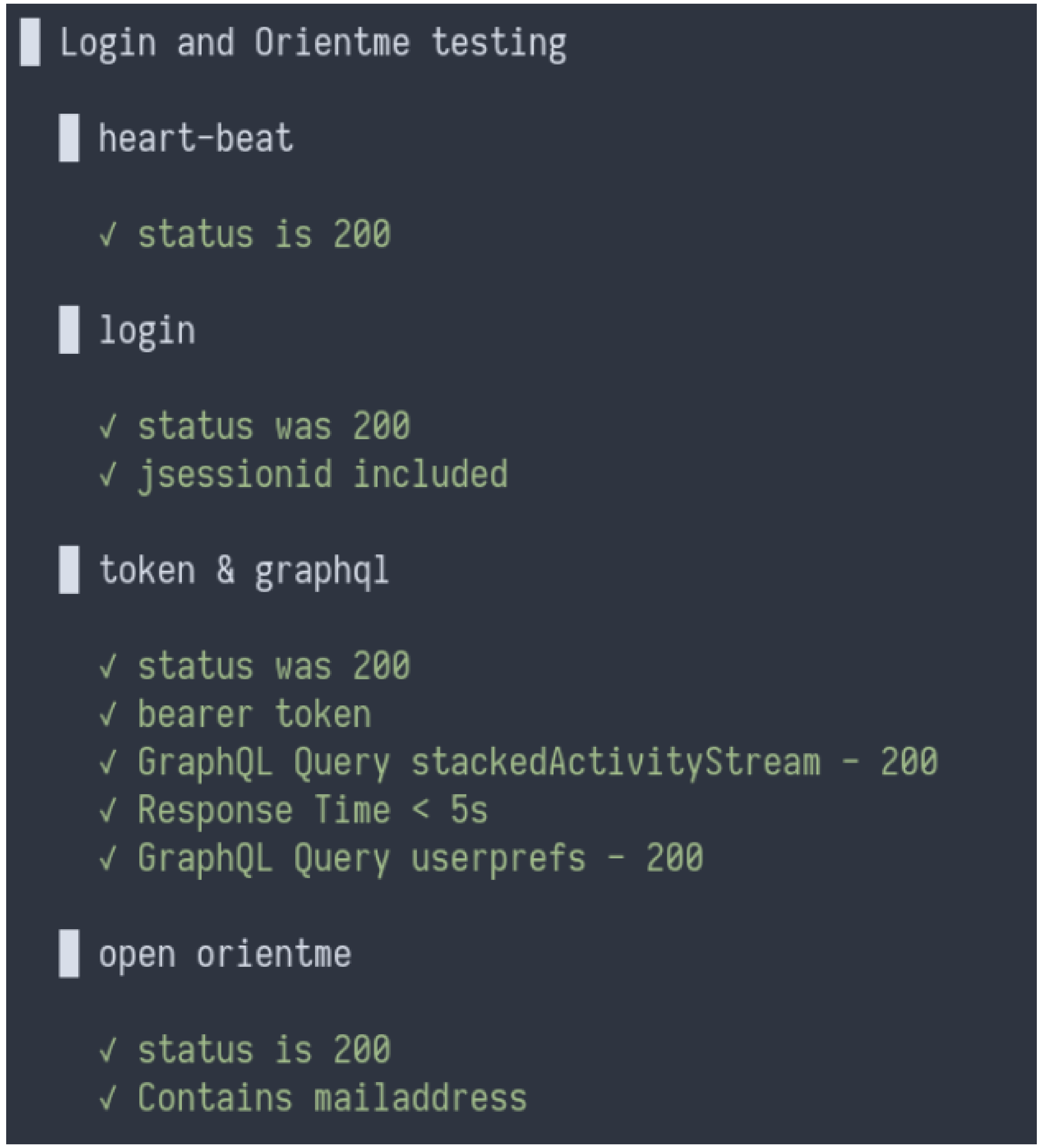
```
import encoding from 'k6/encoding';
import http from 'k6/http';
import { check } from 'k6';
const username = 'jjones3';
const password = 'password';

export const options = {
    insecureSkipTLSVerify: true
};
export default function () {
  const credentials = `${username}:${password}`;
  const url = `https://${credentials}@cnx7-rh8.stoeps.home/wikis/home`;
  let res = http.get(url);
  check(res, {
    'status is 200': (r) => r.status === 200,
    'LtpaToken2': (r) => r.headers.LtpaToken2 !== 0,
  });
}
```

K6 Result - Single User Connect

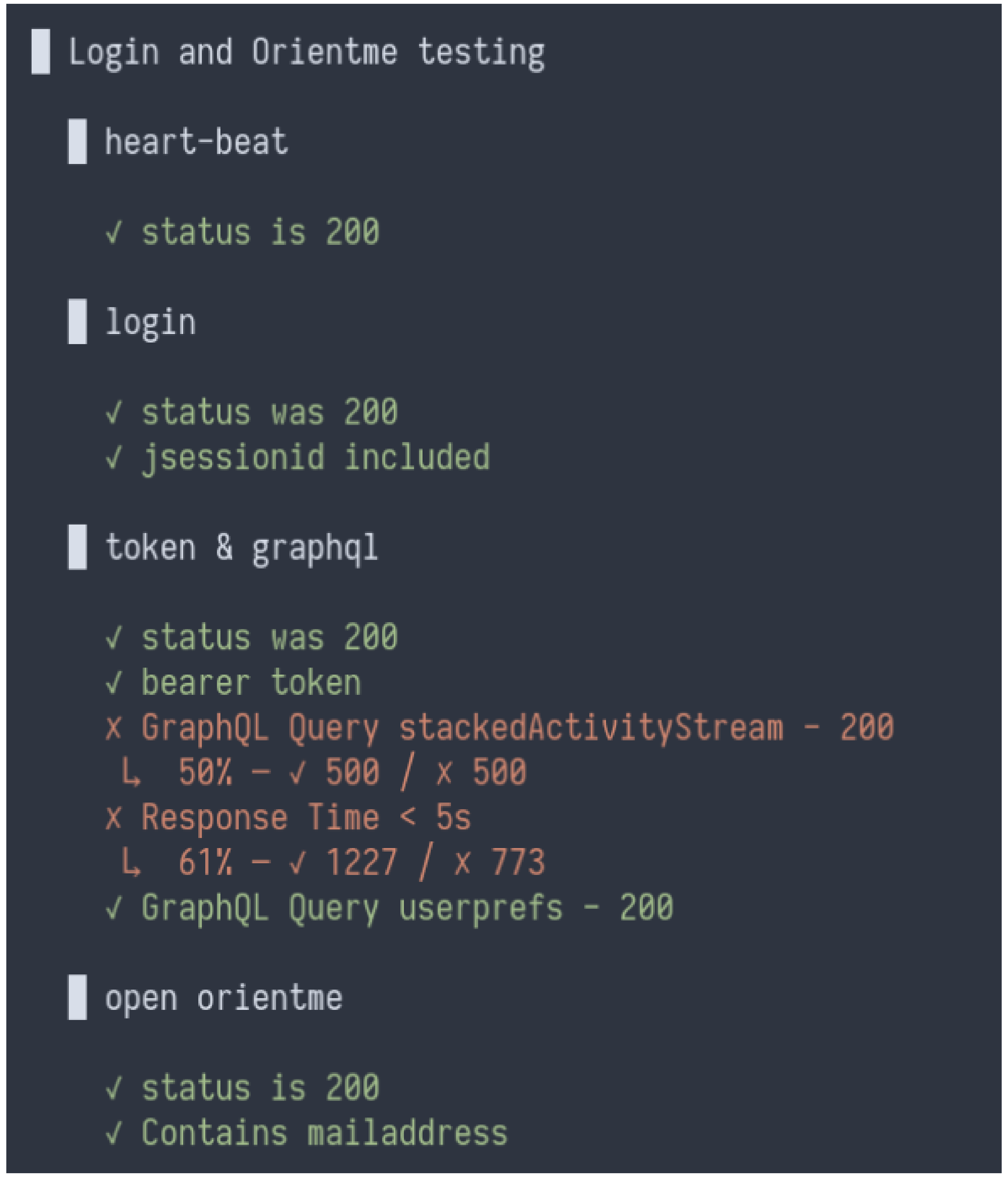


```
❯ k6 run basic-auth.js

          /\      |‾‾| /‾‾/   /‾‾/
     /\  /  \     |  |/  /   /  /
    /  \/    \    |     (   /   ‾‾\
   /          \   |  |\  \ |  (‾)  |
  / __________ \  |__| \__\ \_____/ .io

  execution: local
     script: basic-auth.js
     output: -

  scenarios: (100.00%) 1 scenario, 1 max VUs, 10m30s max duration (incl. graceful stop):
           * default: 1 iterations for each of 1 VUs (maxDuration: 10m0s, gracefulStop: 30s)


running (00m00.1s), 0/1 VUs, 1 complete and 0 interrupted iterations
default ✓ [======================================] 1 VUs  00m00.1s/10m0s  1/1 iters, 1 per VU

     ✓ status is 200
     ✓ LtpaToken2

     checks.........................: 100.00% ✓ 2        ✗ 0
     data_received..................: 41 kB   378 kB/s
     data_sent......................: 535 B   5.0 kB/s
     http_req_blocked...............: avg=8.18ms   min=8.18ms   med=8.18ms   max=8.18ms   p(90)=8.18ms   p(95)=8.18ms
     http_req_connecting............: avg=268.21µs min=268.21µs med=268.21µs max=268.21µs p(90)=268.21µs p(95)=268.21µs
     http_req_duration..............: avg=98.29ms  min=98.29ms  med=98.29ms  max=98.29ms  p(90)=98.29ms  p(95)=98.29ms
       { expected_response:true }...: avg=98.29ms  min=98.29ms  med=98.29ms  max=98.29ms  p(90)=98.29ms  p(95)=98.29ms
     http_req_failed................: 0.00%   ✓ 0        ✗ 1
     http_req_receiving.............: avg=262.1µs  min=262.1µs  med=262.1µs  max=262.1µs  p(90)=262.1µs  p(95)=262.1µs
     http_req_sending...............: avg=71.26µs  min=71.26µs  med=71.26µs  max=71.26µs  p(90)=71.26µs  p(95)=71.26µs
     http_req_tls_handshaking.......: avg=7.85ms   min=7.85ms   med=7.85ms   max=7.85ms   p(90)=7.85ms   p(95)=7.85ms
     http_req_waiting...............: avg=97.95ms  min=97.95ms  med=97.95ms  max=97.95ms  p(90)=97.95ms  p(95)=97.95ms
     http_reqs......................: 1       9.29606/s
     iteration_duration.............: avg=106.75ms min=106.75ms med=106.75ms max=106.75ms p(90)=106.75ms p(95)=106.75ms
     iterations.....................: 1       9.29606/s
```

K6 - GraphQL Load Testing



```
█ Login and Orientme testing

  █ heart-beat

    ✓ status is 200

  █ login

    ✓ status was 200
    ✓ jsessionid included

  █ token & graphql

    ✓ status was 200
    ✓ bearer token
    ✓ GraphQL Query stackedActivityStream - 200
    ✓ Response Time < 5s
    ✓ GraphQL Query userprefs - 200

  █ open orientme

    ✓ status is 200
    ✓ Contains mailaddress
```



```
█ Login and Orientme testing

  █ heart-beat

    ✓ status is 200

  █ login

    ✓ status was 200
    ✓ jsessionid included

  █ token & graphql

    ✓ status was 200
    ✓ bearer token
    ✗ GraphQL Query stackedActivityStream - 200
     ↳  50% — ✓ 500 / ✗ 500
    ✗ Response Time < 5s
     ↳  61% — ✓ 1227 / ✗ 773
    ✓ GraphQL Query userprefs - 200

  █ open orientme

    ✓ status is 200
    ✓ Contains mailaddress
```

Selenium Example - Python

```python
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.chrome.service import Service as ChromeService

options = webdriver.ChromeOptions()
options.set_capability('acceptSslCerts', True)
service = ChromeService(executable_path='/snap/chromium/1985/usr/lib/chromium-browser/chromedri
driver = webdriver.Chrome(service=service, options=options)

driver.maximize_window()
driver.get("https://cnx7-rh8.stoeps.home/wikis/login")
driver.find_element(by=By.ID, value="username").send_keys('jjones3')
driver.find_element(by=By.ID, value="password").send_keys("password")
driver.find_element(by=By.CLASS_NAME, value="lotusBtnSpecial").click()
```

Logs

- Log file analytics, traces
  - Find the right trace strings
- IBM Thread and Monitor Dump Analyzer for Java (TMDA)
- ELK (Elasticsearch, Logstash, Kibana)
  - Using Docker and ELK to Analyze WebSphere Application Server SystemOut.log
  - Better logstash filter to analyze SystemOut.log and some more
- GoAccess
  - Open source real-time web log analyzer
  - Interactive viewer that runs in a terminal

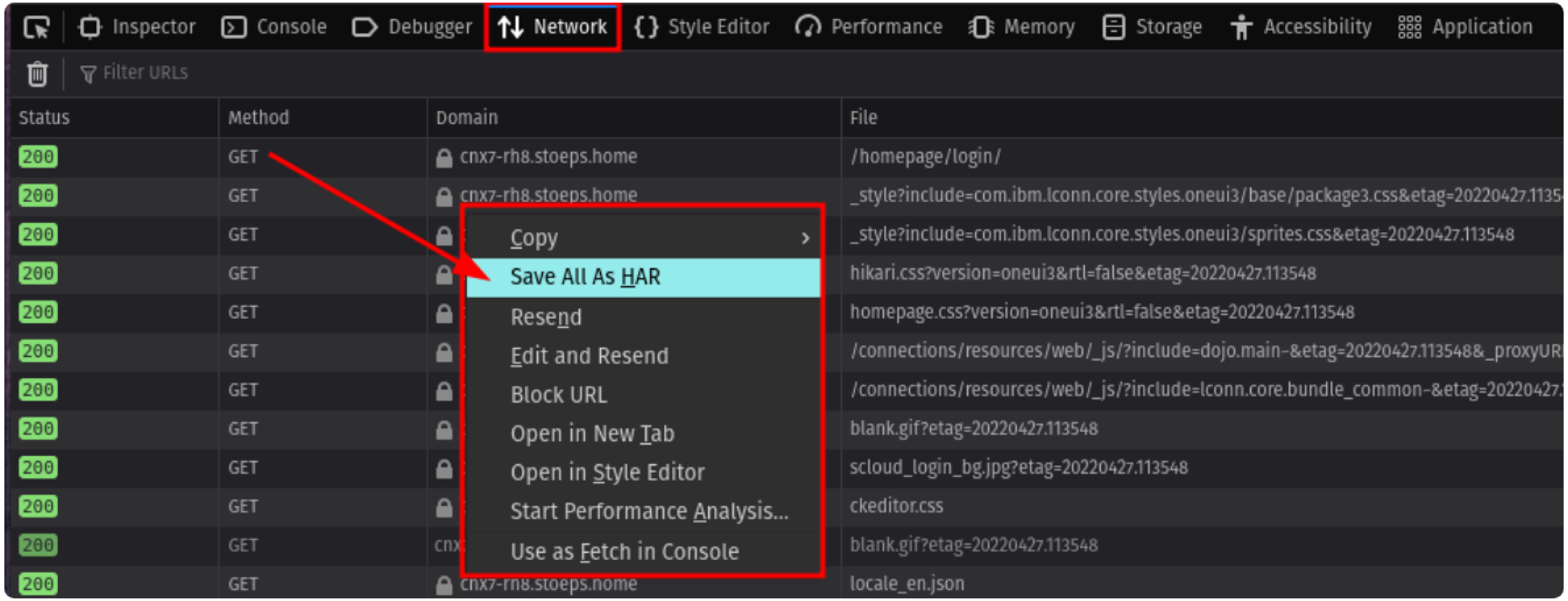
Browser

- DevTools (Firebug, Chrome Web Developer)
  - HAR Analytics (HTTP Archive)
  - Copy as `curl`
- Addons
  - SAML-tracer
  - Multi-Account Container & Container Proxy
- Intercept Proxy
  - OWASP Zed Attack Proxy (ZAP), Burp Suite
  - mitmproxy, Charles

💡 Disable uBlock origin for Connections

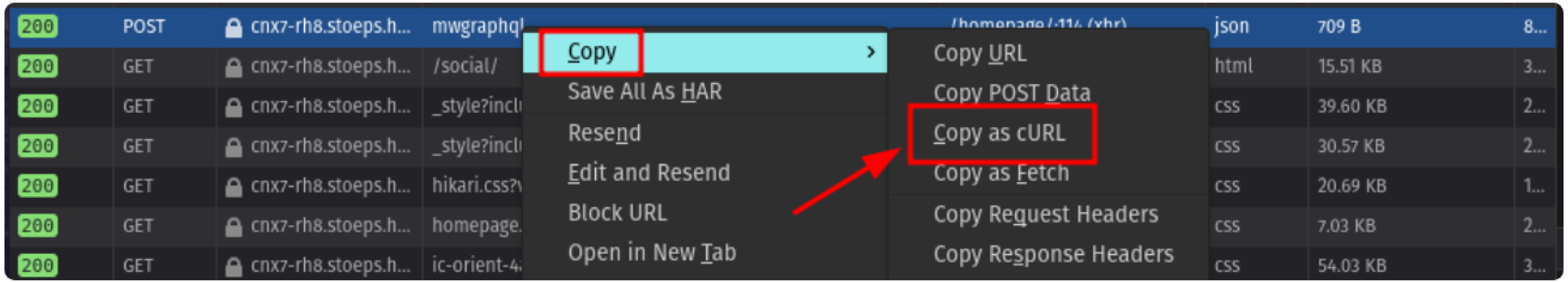
Replace Fiddler With HAR

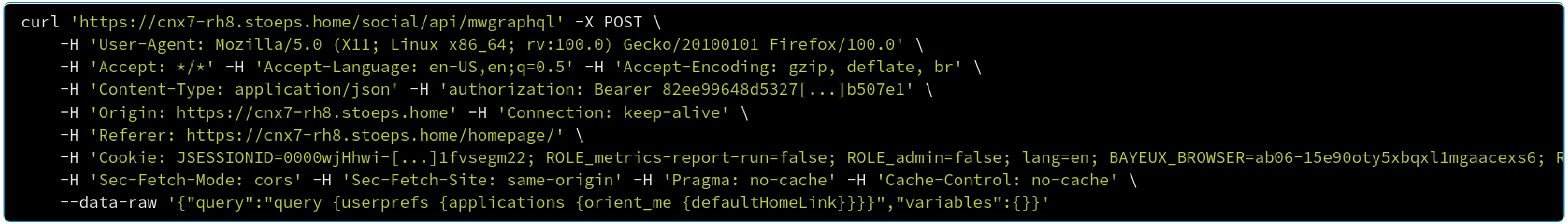
- Webdeveloper Tools > Network, Enable `persist logs`, Reload the page
- Right click > Save all as HAR
- To analyze a recorded HAR, just drag&drop into your network tab



Status	Method	Domain	File
200	GET	cnx7-rh8.stoeps.home	/homepage/login/
200	GET	cnx7-rh8.stoeps.home	_style?include=com.ibm.lconn.core.styles.oneui3/base/package3.css&etag=20220427.1135
200	GET		_style?include=com.ibm.lconn.core.styles.oneui3/sprites.css&etag=20220427.113548
200	GET		hikari.css?version=oneui3&rtl=false&etag=20220427.113548
200	GET		homepage.css?version=oneui3&rtl=false&etag=20220427.113548
200	GET		/connections/resources/web/_js/?include=dojo.main-&etag=20220427.113548&_proxyUR
200	GET		/connections/resources/web/_js/?include=lconn.core.bundle_common-&etag=20220427.
200	GET		blank.gif?etag=20220427.113548
200	GET		scloud_login_bg.jpg?etag=20220427.113548
200	GET		ckeditor.css
200	GET	cnx	blank.gif?etag=20220427.113548
200	GET	cnx7-rh8.stoeps.home	locale_en.json

Copy `curl` Command Line From WebDev Tools


200 POST cnx7-rh8.stoeps.h... mwgraphql /homepage/:114 (xhr) json 709 B 8...
200 GET cnx7-rh8.stoeps.h... /social/ html 15.51 KB 3...
200 GET cnx7-rh8.stoeps.h... _style?inclu css 39.60 KB 2...
200 GET cnx7-rh8.stoeps.h... _style?inclu css 30.57 KB 2...
200 GET cnx7-rh8.stoeps.h... hikari.css?v css 20.69 KB 1...
200 GET cnx7-rh8.stoeps.h... homepage. css 7.03 KB 2...
200 GET cnx7-rh8.stoeps.h... ic-orient-4. css 54.03 KB 3...
Copy
Save All As HAR
Resend
Edit and Resend
Block URL
Open in New Tab
Copy URL
Copy POST Data
Copy as cURL
Copy as Fetch
Copy Request Headers
Copy Response Headers

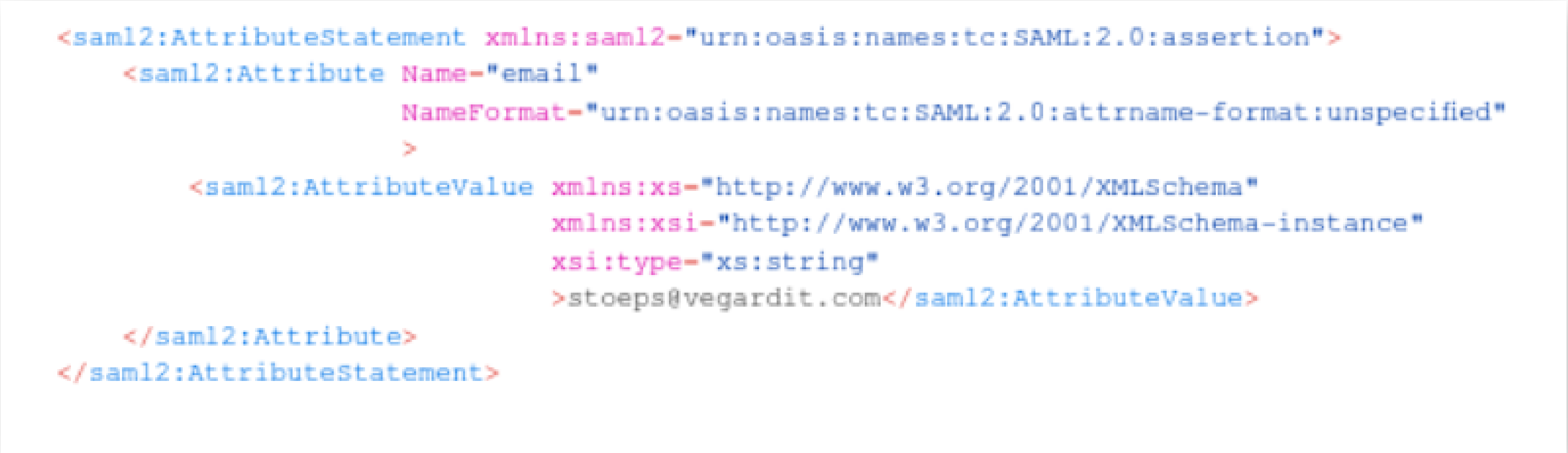


```
curl 'https://cnx7-rh8.stoeps.home/social/api/mwgraphql' -X POST \
    -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:100.0) Gecko/20100101 Firefox/100.0' \
    -H 'Accept: */*' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate, br' \
    -H 'Content-Type: application/json' -H 'authorization: Bearer 82ee99648d5327[...]b507e1' \
    -H 'Origin: https://cnx7-rh8.stoeps.home' -H 'Connection: keep-alive' \
    -H 'Referer: https://cnx7-rh8.stoeps.home/homepage/' \
    -H 'Cookie: JSESSIONID=0000wjHhwi-[...]1fvsegm22; ROLE_metrics-report-run=false; ROLE_admin=false; lang=en; BAYEUX_BROWSER=ab06-15e90oty5xbqxl1mgaacexs6; R
    -H 'Sec-Fetch-Mode: cors' -H 'Sec-Fetch-Site: same-origin' -H 'Pragma: no-cache' -H 'Cache-Control: no-cache' \
    --data-raw '{"query":"query {userprefs {applications {orient_me {defaultHomeLink}}}}","variables":{}}'
```

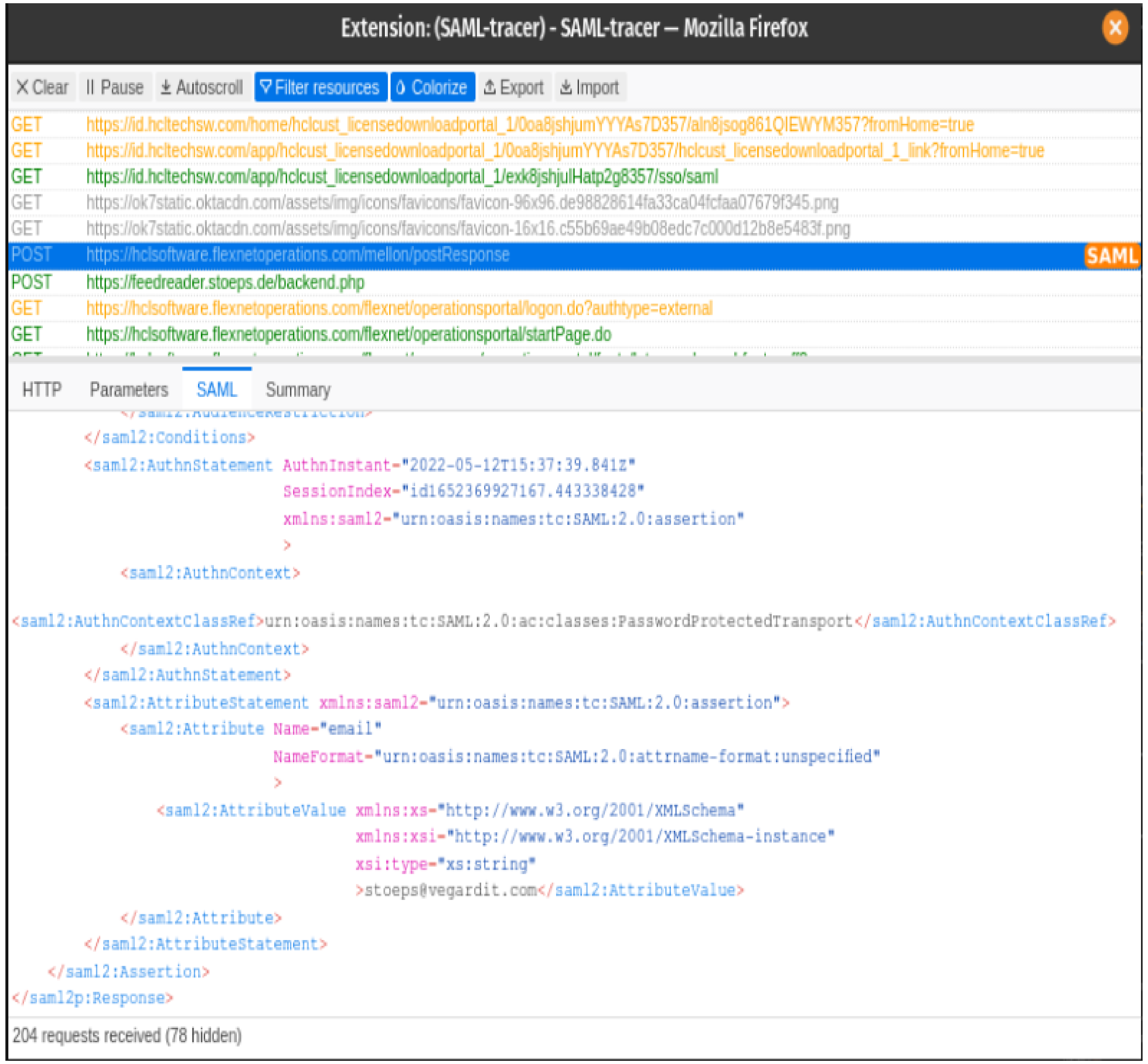
⚠ HAR and `curl` command include authorization tokens

SAML Tracer

- Decrypt the SAML data
- Check mappings (uid, mail addresses)



```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Attribute Name="email"
                     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                     >
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                              xsi:type="xs:string"
                              >stoeps@vegardit.com</saml2:AttributeValue>
    </saml2:Attribute>
</saml2:AttributeStatement>
```



```
GET   https://id.hcltechsw.com/home/hclcust_licensedownloadportal_1/0oa8jshjumYYYAs7D357/aln8jsog861QIEWYM357?fromHome=true
GET   https://id.hcltechsw.com/app/hclcust_licensedownloadportal_1/0oa8jshjumYYYAs7D357/hclcust_licensedownloadportal_1_link?fromHome=true
GET   https://id.hcltechsw.com/app/hclcust_licensedownloadportal_1/exk8jshjulHatp2g8357/sso/saml
GET   https://ok7static.oktacdn.com/assets/img/icons/favicons/favicon-96x96.de98828614fa33ca04fcfaa07679f345.png
GET   https://ok7static.oktacdn.com/assets/img/icons/favicons/favicon-16x16.c55b69ae49b08edc7c000d12b8e5483f.png
POST  https://hclsoftware.flexnetoperations.com/mellon/postResponse
POST  https://feedreader.stoeps.de/backend.php
GET   https://hclsoftware.flexnetoperations.com/flexnet/operationsportal/logon.do?authtype=external
GET   https://hclsoftware.flexnetoperations.com/flexnet/operationsportal/startPage.do
```

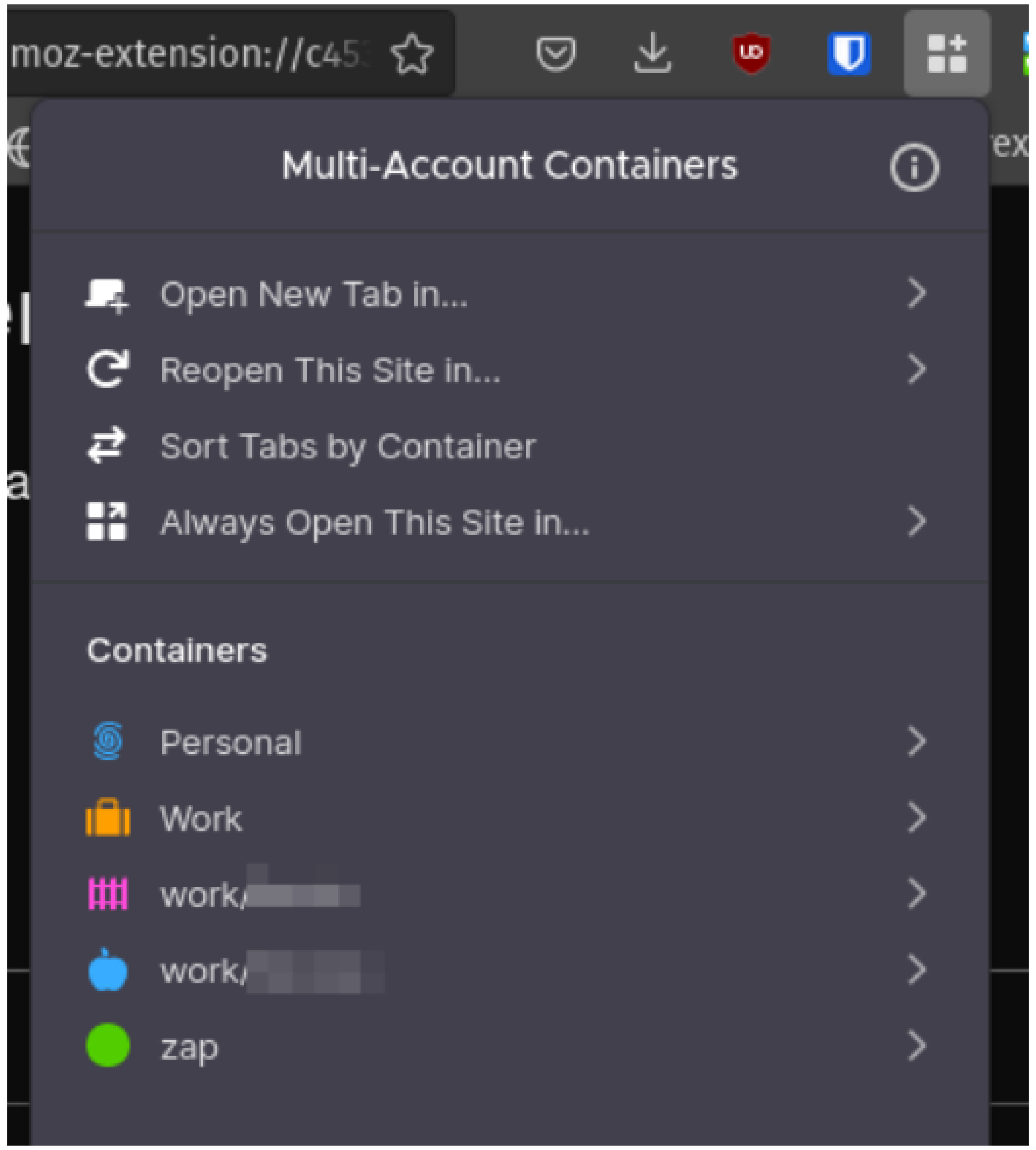
```
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2022-05-12T15:37:39.841Z"
                              SessionIndex="id1652369927167.443338428"
                              xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                              >
            <saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml2:Attribute Name="email"
                             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                             >
                <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                      xsi:type="xs:string"
                                      >stoeps@vegardit.com</saml2:AttributeValue>
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

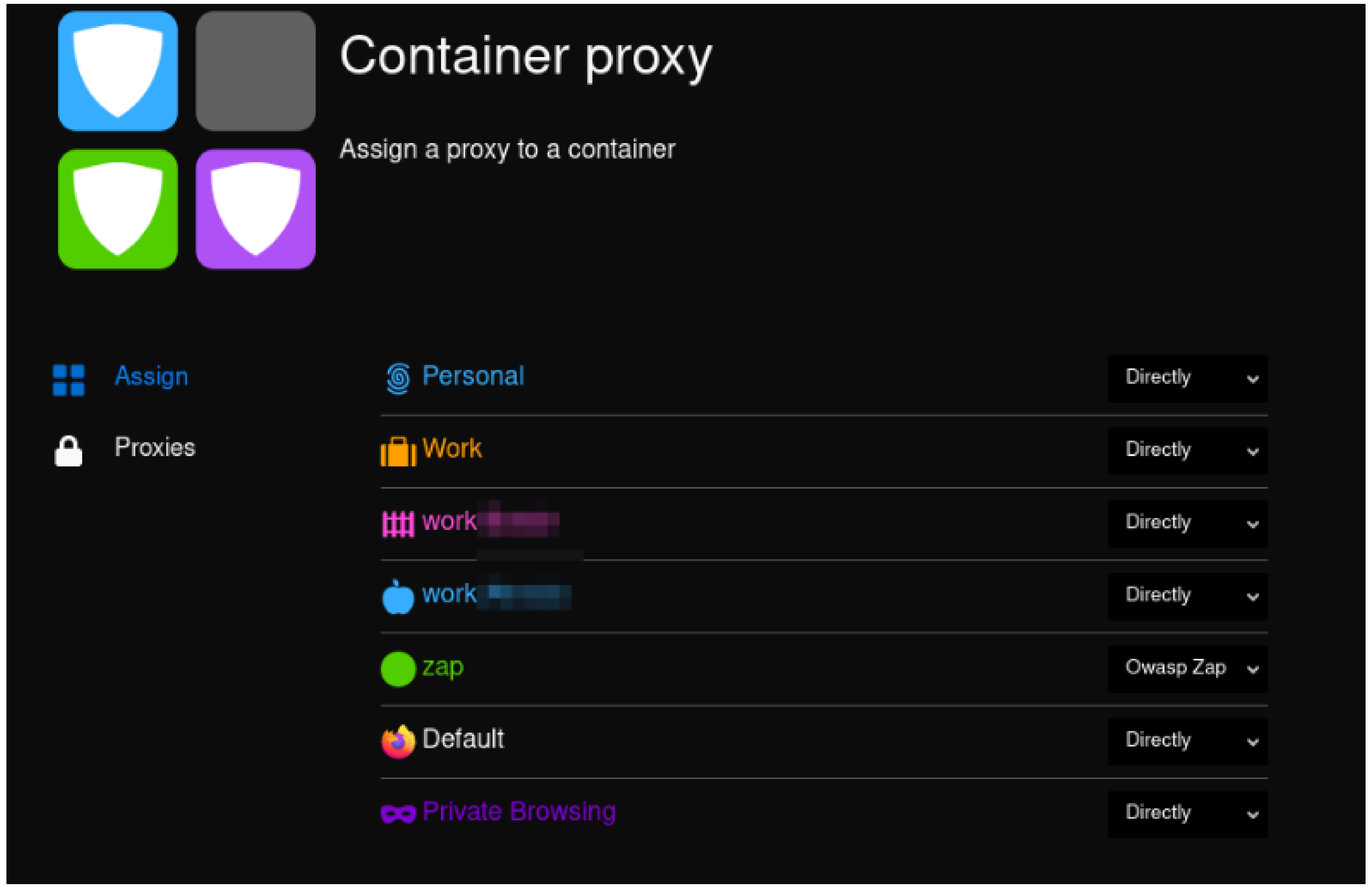
204 requests received (78 hidden)

Multi Account Container

- Very convenient to open ISC and Connections with different users
  - ISC as user wasadmin, Connections as normal user
- Test something with different users in one browser
  - e.g. create content and check notification
  - login with multiple accounts
- Shares Cookies with containers of the same class
- Private tab / window shares cookies of all private tabs
- Container Proxy is an additional add-on
  - set proxies for containers of one kind
  - e.g. Burp Suite for one class, Tor for another

Multi Account Container — Container Proxy





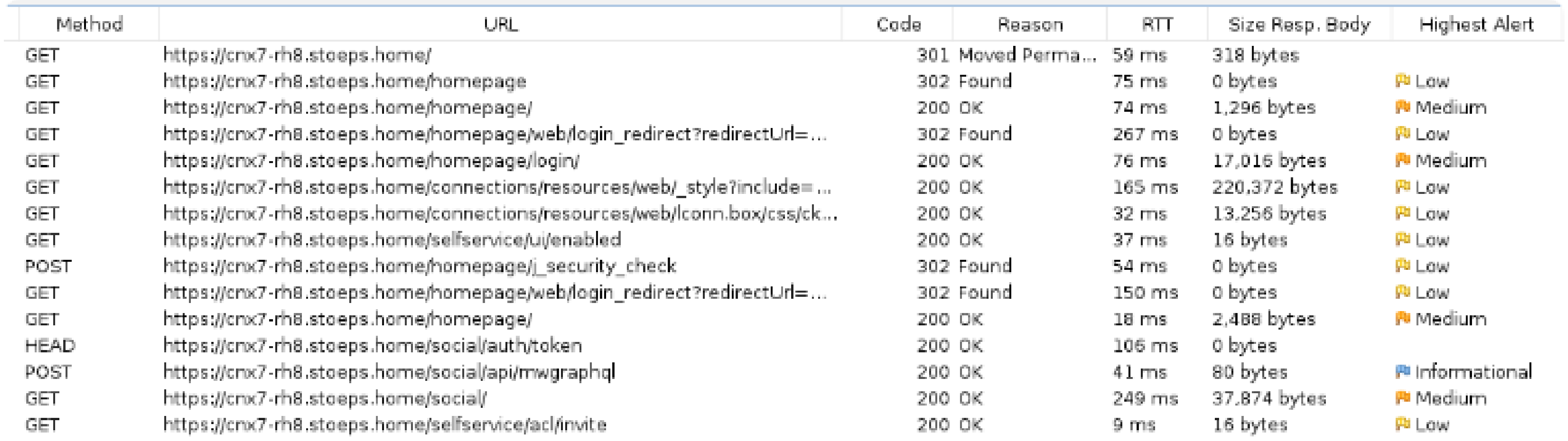
Container proxy

Assign a proxy to a container

Personal	Directly
Work	Directly
work [redacted]	Directly
work [redacted]	Directly
zap	Owasp Zap
Default	Directly
Private Browsing	Directly

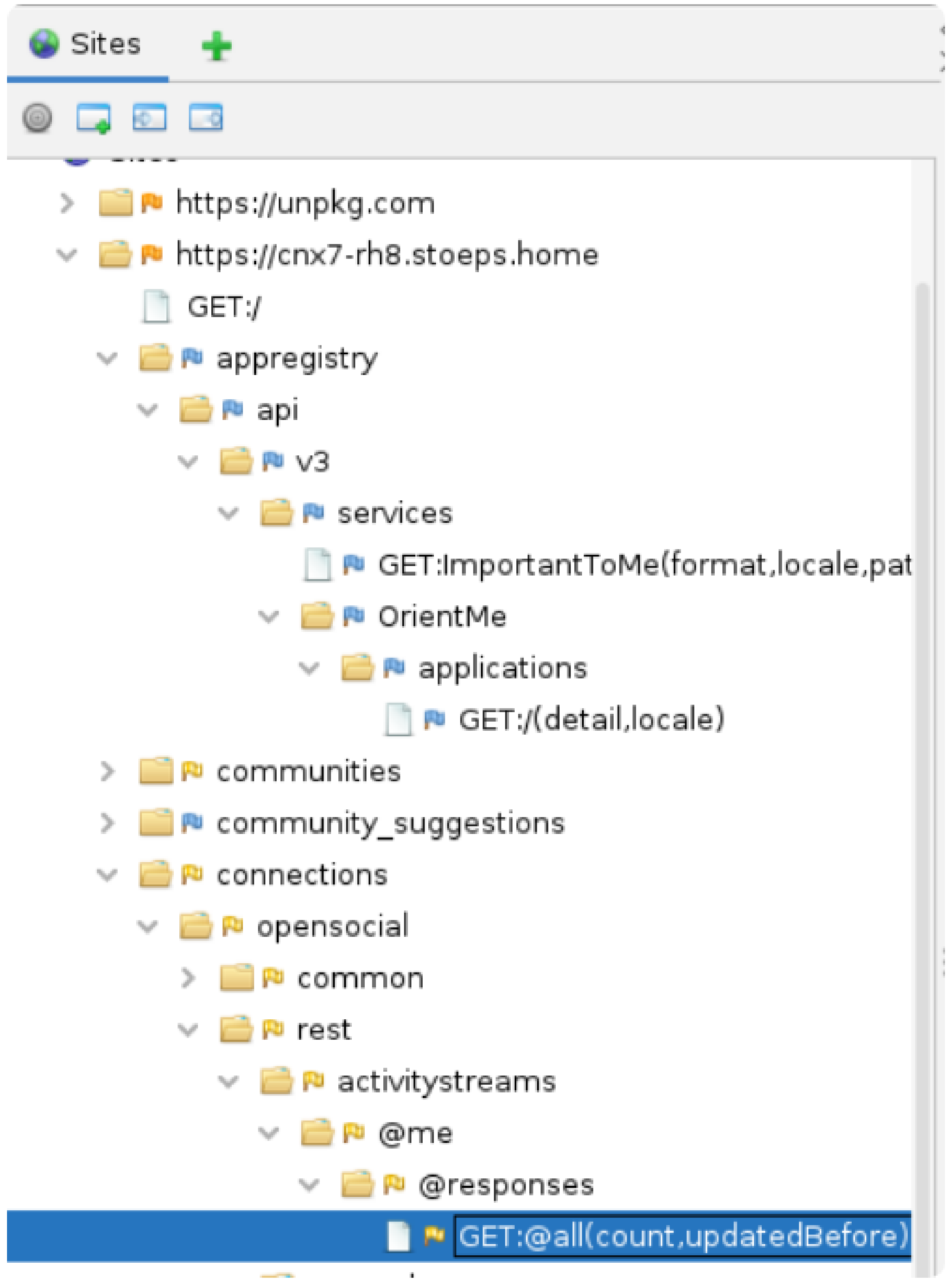
Intercept Proxies

- Often used in Bug Bounty
- Import HAR (ZAP)
- See requests and responses
- Bypass client side controls
- Brute Force and Fuzz API or Logins



Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert
GET	https://cnx7-rh8.stoeps.home/	301	Moved Perma...	59 ms	318 bytes	
GET	https://cnx7-rh8.stoeps.home/homepage	302	Found	75 ms	0 bytes	Low
GET	https://cnx7-rh8.stoeps.home/homepage/	200	OK	74 ms	1,296 bytes	Medium
GET	https://cnx7-rh8.stoeps.home/homepage/web/login_redirect?redirectUrl=...	302	Found	267 ms	0 bytes	Low
GET	https://cnx7-rh8.stoeps.home/homepage/login/	200	OK	76 ms	17,016 bytes	Medium
GET	https://cnx7-rh8.stoeps.home/connections/resources/web/_style?include=...	200	OK	165 ms	220,372 bytes	Low
GET	https://cnx7-rh8.stoeps.home/connections/resources/web/lconn.box/css/ck...	200	OK	32 ms	13,256 bytes	Low
GET	https://cnx7-rh8.stoeps.home/selfservice/ui/enabled	200	OK	37 ms	16 bytes	Low
POST	https://cnx7-rh8.stoeps.home/homepage/j_security_check	302	Found	54 ms	0 bytes	Low
GET	https://cnx7-rh8.stoeps.home/homepage/web/login_redirect?redirectUrl=...	302	Found	150 ms	0 bytes	Low
GET	https://cnx7-rh8.stoeps.home/homepage/	200	OK	18 ms	2,488 bytes	Medium
HEAD	https://cnx7-rh8.stoeps.home/social/auth/token	200	OK	106 ms	0 bytes	
POST	https://cnx7-rh8.stoeps.home/social/api/mwgraphql	200	OK	41 ms	80 bytes	Informational
GET	https://cnx7-rh8.stoeps.home/social/	200	OK	249 ms	37,874 bytes	Medium
GET	https://cnx7-rh8.stoeps.home/selfservice/acl/invite	200	OK	9 ms	16 bytes	Low

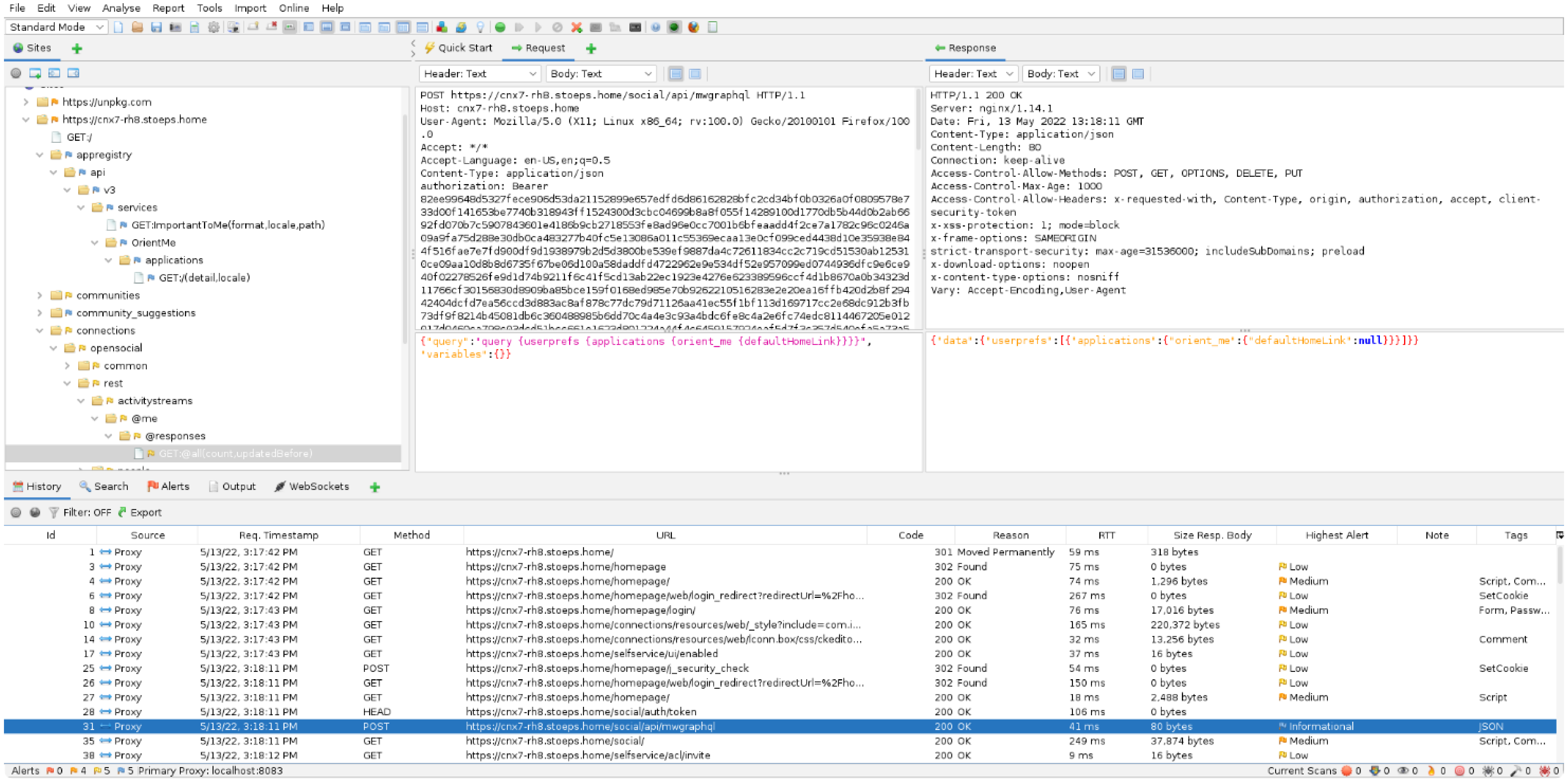
Figure 2. History



```
Sites
  https://unpkg.com
  https://cnx7-rh8.stoeps.home
    GET:/
    appregistry
      api
        v3
          services
            GET:ImportantToMe(format,locale,pat
          OrientMe
            applications
              GET:/(detail,locale)
    communities
    community_suggestions
    connections
      opensocial
        common
        rest
          activitystreams
            @me
              @responses
                GET:@all(count,updatedBefore)
```

Figure 3. Site tree

Intercept Proxies Example - OWASP ZAP



```
https://unpkg.com
https://cnx7-rh8.stoeps.home
  GET:/
  appregistry
    api
      v3
        services
          GET:ImportantToMe(format,locale,path)
        OrientMe
          applications
            GET:/(detail,locale)
  communities
  community_suggestions
  connections
    opensocial
      common
      rest
        activitystreams
          @me
            @responses
              GET:@all(count,updatedBefore)
```

```
POST https://cnx7-rh8.stoeps.home/social/api/mwgraphql HTTP/1.1
Host: cnx7-rh8.stoeps.home
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:100.0) Gecko/20100101 Firefox/100
.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
authorization: Bearer
82ee99648d5327fece906d53da21152899e657edfd6d86162828bfc2cd34bf0b0326a0f0809578e7
33d00f141653be7740b318943ff1524300d3cbc04699b8a8f055f14289100d1770db5b44d0b2ab66
92fd070b7c5907843601e4186b9cb2718553fe8ad96e0cc7001b6bfeaadd4f2ce7a1782c96c0246a
09a9fa75d288e30db0ca483277b40fc5e13086a011c55369ecaa13e0cf099ced4438d10e35938e84
4f516fae7e7fd900df9d1938979b2d5d3800be539ef9887da4c72611834cc2c719cd51530ab12531
0ce09aa10d8b8d6735f67be06d100a58daddfd4722962e9e534df52e957099ed0744936dfc9e6ce9
40f02278526fe9d1d74b9211f6c41f5cd13ab22ec1923e4276e623389596ccf4d1b8670a0b34323d
11766cf30156830d8909ba85bce159f0168ed985e70b92622105162838e2e20ea16ffb420d2b8f294
42404dcfd7ea56ccd3d883ac8af878c77dc79d71126aa41ec55f1bf113d169717cc2e68dc912b3fb
73df9f8214b45081db6c360488985b6dd70c4a4e3c93a4bdc6fe8c4a2e6fc74edc8114467205e012
```

```
{"query":"query {userprefs {applications {orient_me {defaultHomeLink}}}}",
"variables":{}}
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.1
Date: Fri, 13 May 2022 13:18:11 GMT
Content-Type: application/json
Content-Length: 80
Connection: keep-alive
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Access-Control-Max-Age: 1000
Access-Control-Allow-Headers: x-requested-with, Content-Type, origin, authorization, accept, client-
security-token
x-xss-protection: 1; mode=block
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-download-options: noopen
x-content-type-options: nosniff
Vary: Accept-Encoding,User-Agent
```

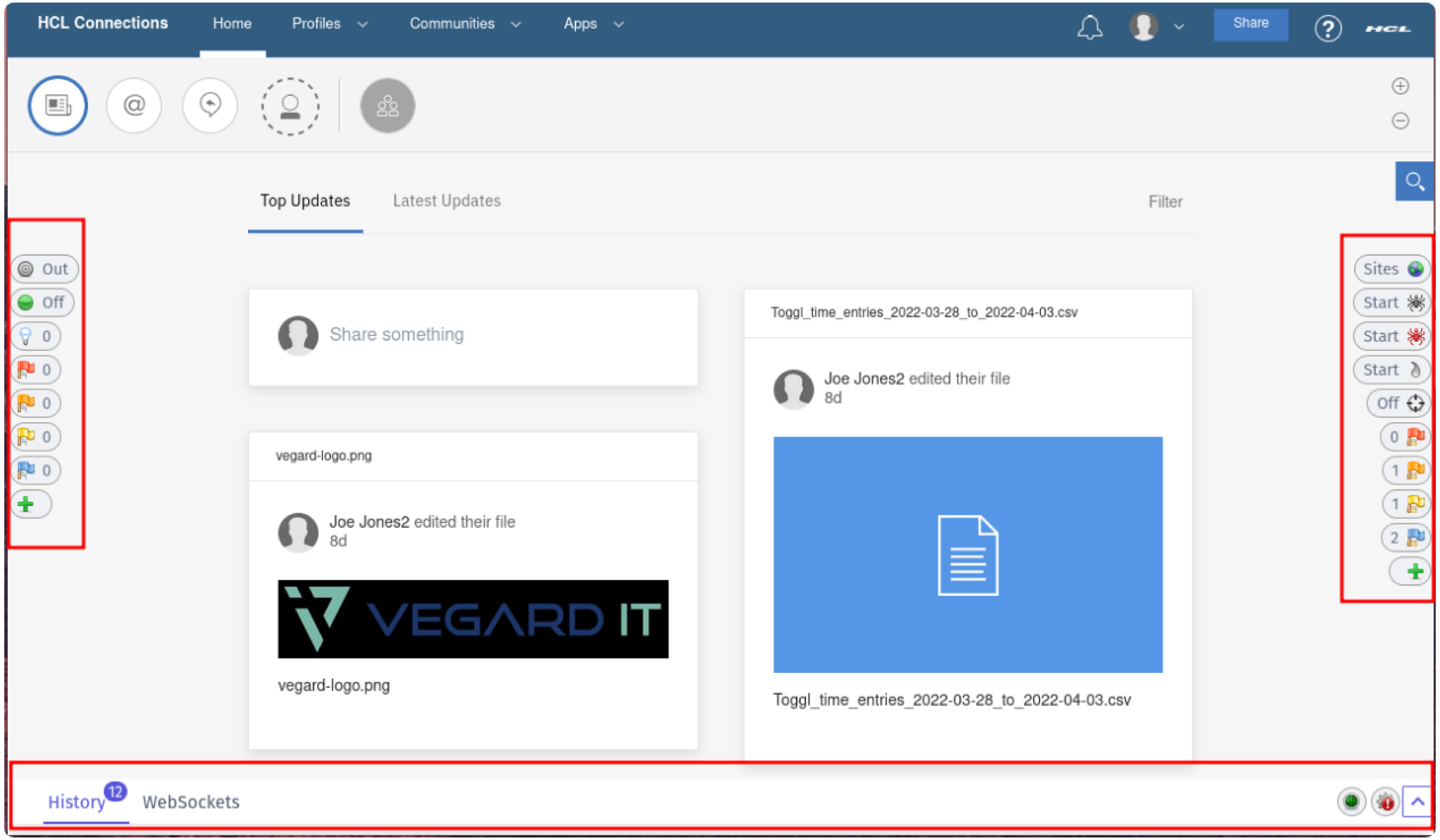
```
{"data":{"userprefs":[{"applications":{"orient_me":{"defaultHomeLink":null}}}]}}
```

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	⟷ Proxy	5/13/22, 3:17:42 PM	GET	https://cnx7-rh8.stoeps.home/	301	Moved Permanently	59 ms	318 bytes			
3	⟷ Proxy	5/13/22, 3:17:42 PM	GET	https://cnx7-rh8.stoeps.home/homepage	302	Found	75 ms	0 bytes	Low		
4	⟷ Proxy	5/13/22, 3:17:42 PM	GET	https://cnx7-rh8.stoeps.home/homepage/	200	OK	74 ms	1,296 bytes	Medium		Script, Com...
6	⟷ Proxy	5/13/22, 3:17:42 PM	GET	https://cnx7-rh8.stoeps.home/homepage/web/login_redirect?redirectUrl=%2Fho...	302	Found	267 ms	0 bytes	Low		SetCookie
8	⟷ Proxy	5/13/22, 3:17:43 PM	GET	https://cnx7-rh8.stoeps.home/homepage/login/	200	OK	76 ms	17,016 bytes	Medium		Form, Passw...
10	⟷ Proxy	5/13/22, 3:17:43 PM	GET	https://cnx7-rh8.stoeps.home/connections/resources/web/_style?include=com.i...	200	OK	165 ms	220,372 bytes	Low		
14	⟷ Proxy	5/13/22, 3:17:43 PM	GET	https://cnx7-rh8.stoeps.home/connections/resources/web/lconn.box/css/ckedito...	200	OK	32 ms	13,256 bytes	Low		Comment
17	⟷ Proxy	5/13/22, 3:17:43 PM	GET	https://cnx7-rh8.stoeps.home/selfservice/ui/enabled	200	OK	37 ms	16 bytes	Low		
25	⟷ Proxy	5/13/22, 3:18:11 PM	POST	https://cnx7-rh8.stoeps.home/homepage/j_security_check	302	Found	54 ms	0 bytes	Low		SetCookie
26	⟷ Proxy	5/13/22, 3:18:11 PM	GET	https://cnx7-rh8.stoeps.home/homepage/web/login_redirect?redirectUrl=%2Fho...	302	Found	150 ms	0 bytes	Low		
27	⟷ Proxy	5/13/22, 3:18:11 PM	GET	https://cnx7-rh8.stoeps.home/homepage/	200	OK	18 ms	2,488 bytes	Medium		Script
28	⟷ Proxy	5/13/22, 3:18:11 PM	HEAD	https://cnx7-rh8.stoeps.home/social/auth/token	200	OK	106 ms	0 bytes			
31	⟷ Proxy	5/13/22, 3:18:11 PM	POST	https://cnx7-rh8.stoeps.home/social/api/mwgraphql	200	OK	41 ms	80 bytes	Informational		JSON
35	⟷ Proxy	5/13/22, 3:18:11 PM	GET	https://cnx7-rh8.stoeps.home/social/	200	OK	249 ms	37,874 bytes	Medium		Script, Com...
38	⟷ Proxy	5/13/22, 3:18:12 PM	GET	https://cnx7-rh8.stoeps.home/selfservice/acl/invite	200	OK	9 ms	16 bytes	Low		

Alerts 0 4 5 5 Primary Proxy: localhost:8083

Current Scans 0 0 0 0 0 0 0 0

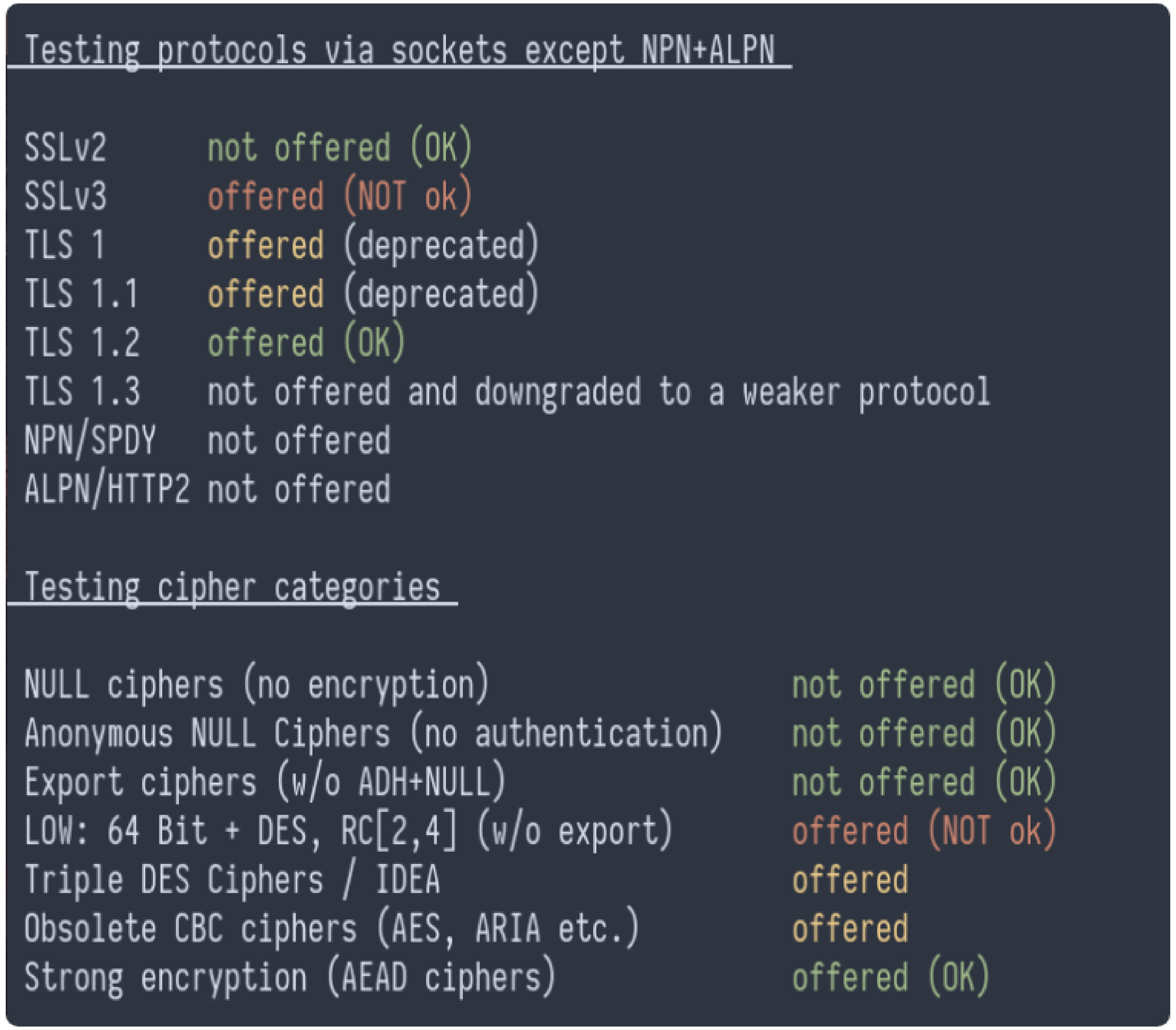
Intercept Proxies Example - OWASP ZAP HUD



SSL

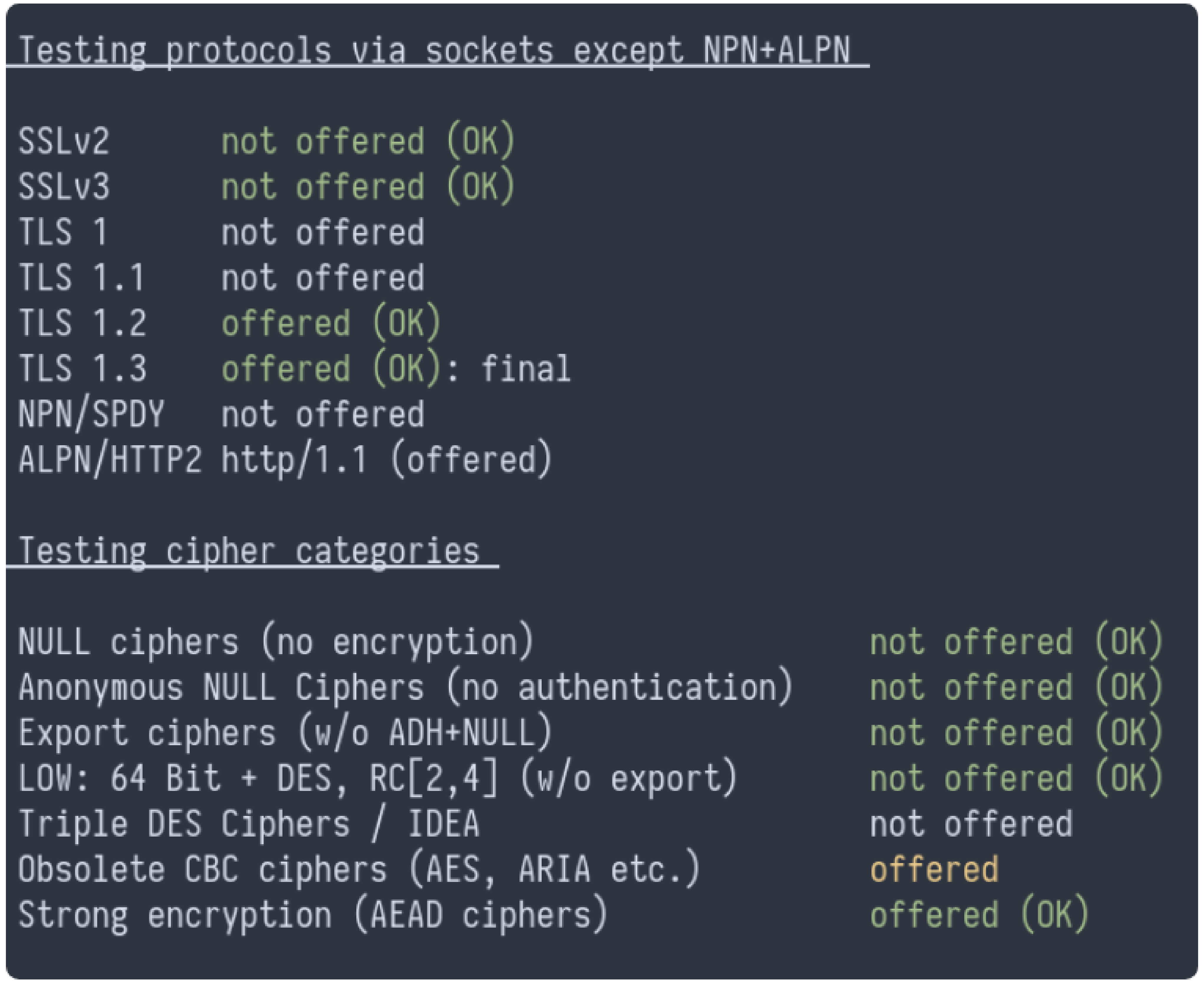
- `testssl.sh`
  - Check SSL certificates
  - Like SSL Server Test
    - But faster
    - No need to publish your site to public
- Keystore Explorer
  - Examine SSL
  - Import signer to TDI keystore
  - Convert certificates

testssl.sh — Protocols And Ciphers



```
 Testing protocols via sockets except NPN+ALPN 

 SSLv2      not offered (OK)
 SSLv3      offered (NOT ok)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories 

 NULL ciphers (no encryption)                    not offered (OK)
 Anonymous NULL Ciphers (no authentication)      not offered (OK)
 Export ciphers (w/o ADH+NULL)                   not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export)         offered (NOT ok)
 Triple DES Ciphers / IDEA                       offered
 Obsolete CBC ciphers (AES, ARIA etc.)           offered
 Strong encryption (AEAD ciphers)                offered (OK)
```

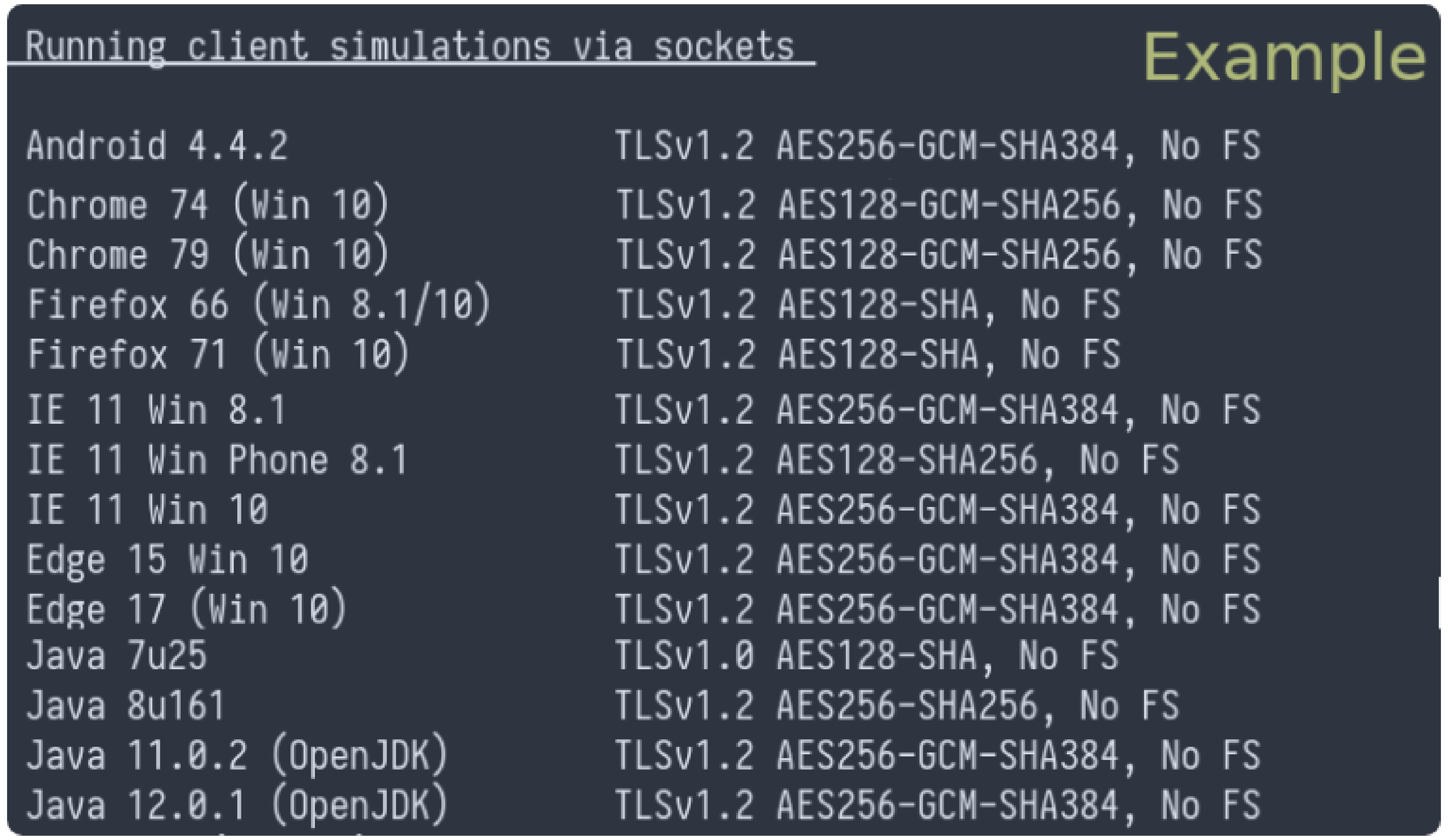
Figure 4. OpenLDAP



```
 Testing protocols via sockets except NPN+ALPN 

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 http/1.1 (offered)

 Testing cipher categories 

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export)           not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsolete CBC ciphers (AES, ARIA etc.)             offered
 Strong encryption (AEAD ciphers)                  offered (OK)
```

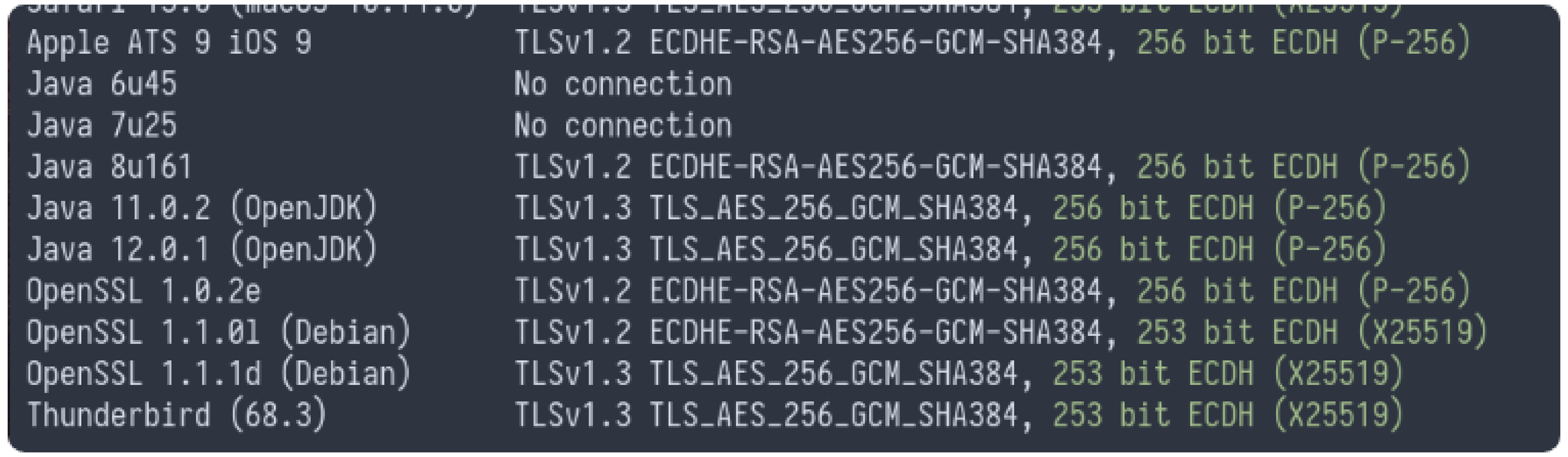
Figure 5. nginx

testssl.sh — Check Application Access



```
Running client simulations via sockets                    Example

Android 4.4.2                TLSv1.2 AES256-GCM-SHA384, No FS
Chrome 74 (Win 10)           TLSv1.2 AES128-GCM-SHA256, No FS
Chrome 79 (Win 10)           TLSv1.2 AES128-GCM-SHA256, No FS
Firefox 66 (Win 8.1/10)      TLSv1.2 AES128-SHA, No FS
Firefox 71 (Win 10)          TLSv1.2 AES128-SHA, No FS
IE 11 Win 8.1                TLSv1.2 AES256-GCM-SHA384, No FS
IE 11 Win Phone 8.1          TLSv1.2 AES128-SHA256, No FS
IE 11 Win 10                 TLSv1.2 AES256-GCM-SHA384, No FS
Edge 15 Win 10               TLSv1.2 AES256-GCM-SHA384, No FS
Edge 17 (Win 10)             TLSv1.2 AES256-GCM-SHA384, No FS
Java 7u25                    TLSv1.0 AES128-SHA, No FS
Java 8u161                   TLSv1.2 AES256-SHA256, No FS
Java 11.0.2 (OpenJDK)        TLSv1.2 AES256-GCM-SHA384, No FS
Java 12.0.1 (OpenJDK)        TLSv1.2 AES256-GCM-SHA384, No FS
```

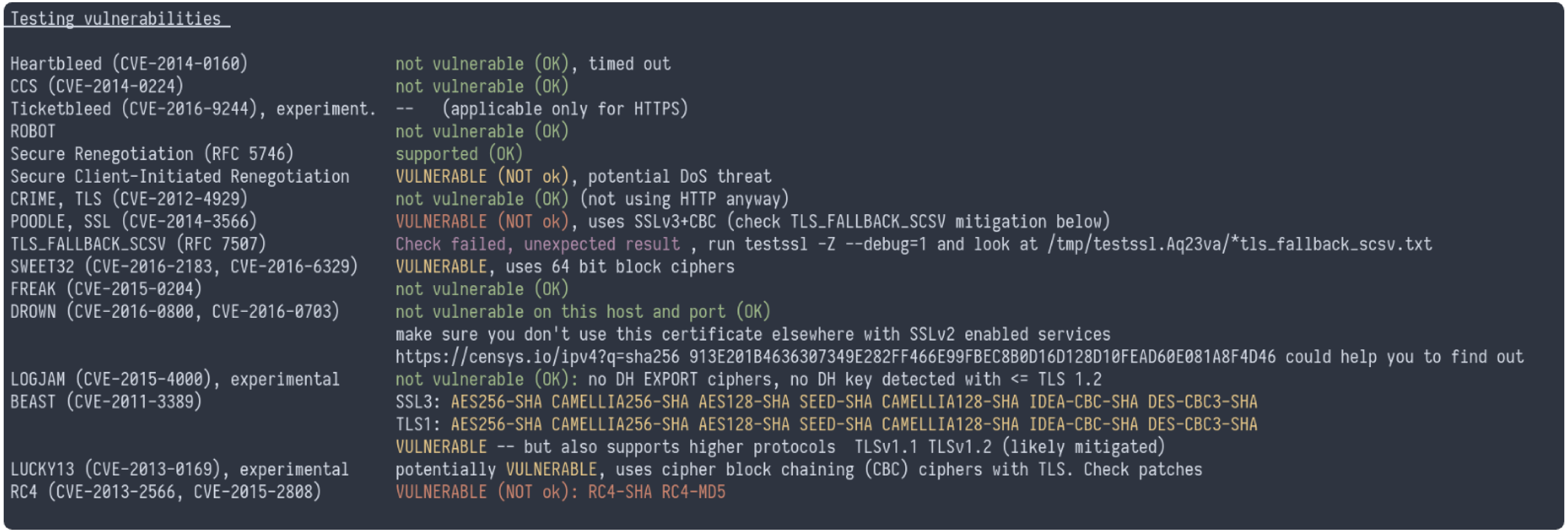
Figure 6. OpenLDAP



```
Safari 13.0 (macOS 10.14.6)  TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
Apple ATS 9 iOS 9            TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Java 6u45                    No connection
Java 7u25                    No connection
Java 8u161                   TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
Java 11.0.2 (OpenJDK)        TLSv1.3 TLS_AES_256_GCM_SHA384, 256 bit ECDH (P-256)
Java 12.0.1 (OpenJDK)        TLSv1.3 TLS_AES_256_GCM_SHA384, 256 bit ECDH (P-256)
OpenSSL 1.0.2e               TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256)
OpenSSL 1.1.0l (Debian)      TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 253 bit ECDH (X25519)
OpenSSL 1.1.1d (Debian)      TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
Thunderbird (68.3)           TLSv1.3 TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
```

Figure 7. nginx

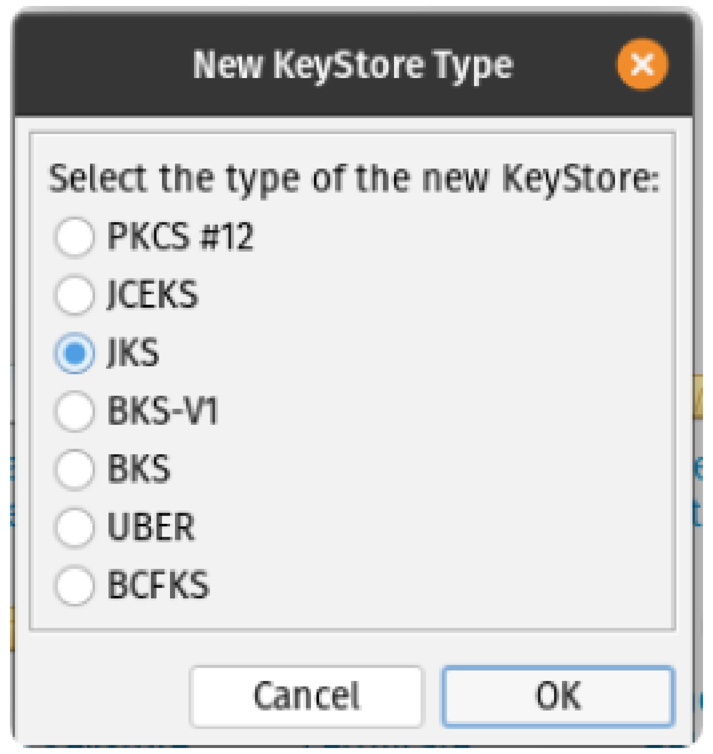
testssl.sh — Check For Vulnerabilities



```
Testing vulnerabilities 

Heartbleed (CVE-2014-0160)                not vulnerable (OK), timed out
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  --   (applicable only for HTTPS)
ROBOT                                     not vulnerable (OK)
Secure Renegotiation (RFC 5746)           supported (OK)
Secure Client-Initiated Renegotiation     VULNERABLE (NOT ok), potential DoS threat
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK) (not using HTTP anyway)
POODLE, SSL (CVE-2014-3566)               VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)              Check failed, unexpected result , run testssl -Z --debug=1 and look at /tmp/testssl.Aq23va/*tls_fallback_scsv.txt
SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                          make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                          https://censys.io/ipv4?q=sha256 913E201B4636307349E282FF466E99FBEC8B0D16D128D10FEAD60E081A8F4D46 could help you to find out
LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
BEAST (CVE-2011-3389)                     SSL3: AES256-SHA CAMELLIA256-SHA AES128-SHA SEED-SHA CAMELLIA128-SHA IDEA-CBC-SHA DES-CBC3-SHA
                                          TLS1: AES256-SHA CAMELLIA256-SHA AES128-SHA SEED-SHA CAMELLIA128-SHA IDEA-CBC-SHA DES-CBC3-SHA
                                          VULNERABLE -- but also supports higher protocols  TLSv1.1 TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5
```

Keystore Explorer — Import Signer For TDI

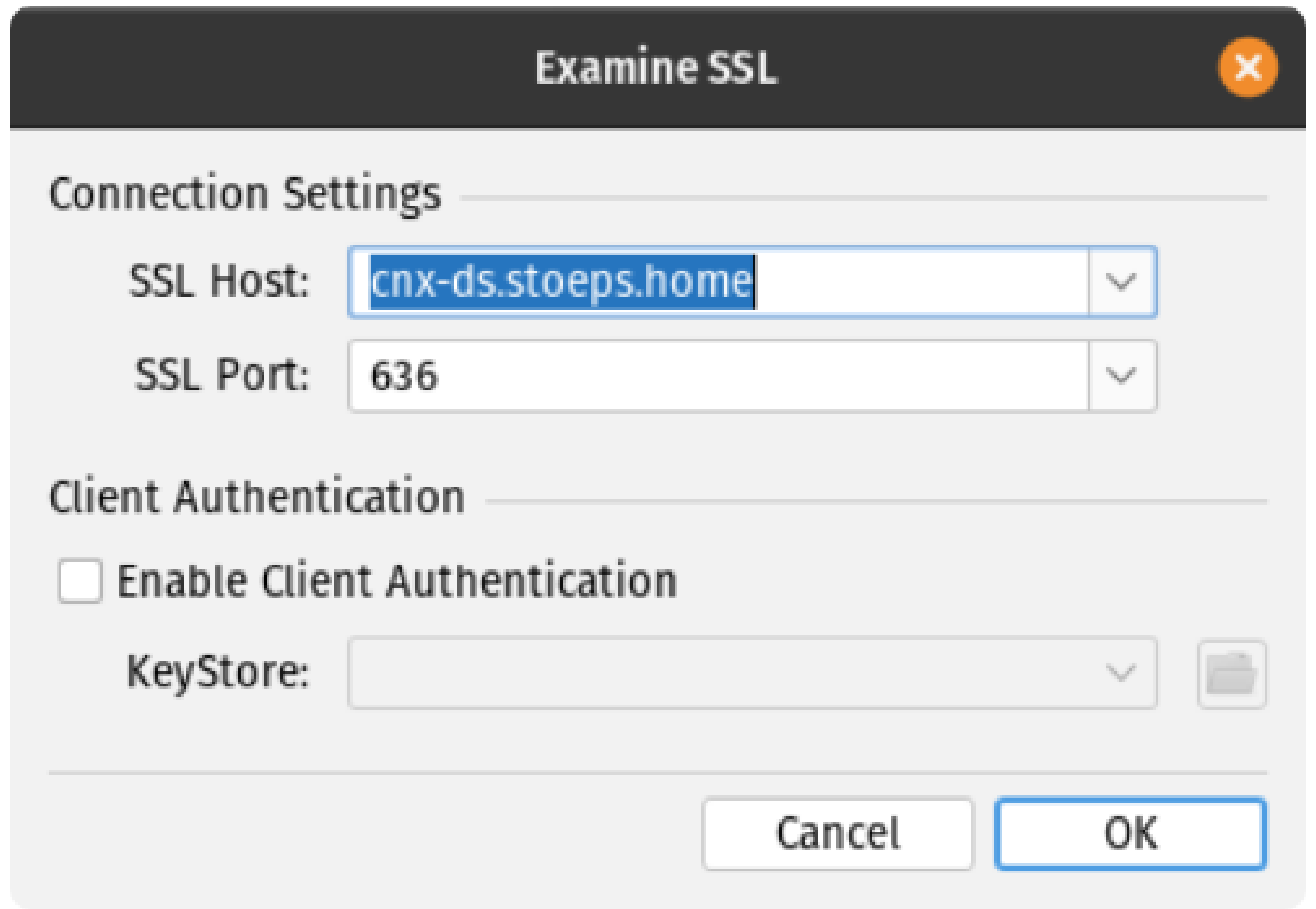
- Create Keystore (JKS)
- Examine > Examine SSL
  - Add hostname & port
  - Import



New KeyStore Type

Select the type of the new KeyStore:

○ PKCS #12
○ JCEKS
● JKS
○ BKS-V1
○ BKS
○ UBER
○ BCFKS



Examine SSL

Connection Settings

SSL Host: cnx-ds.stoeps.home

SSL Port: 636

Client Authentication

□ Enable Client Authentication

KeyStore:

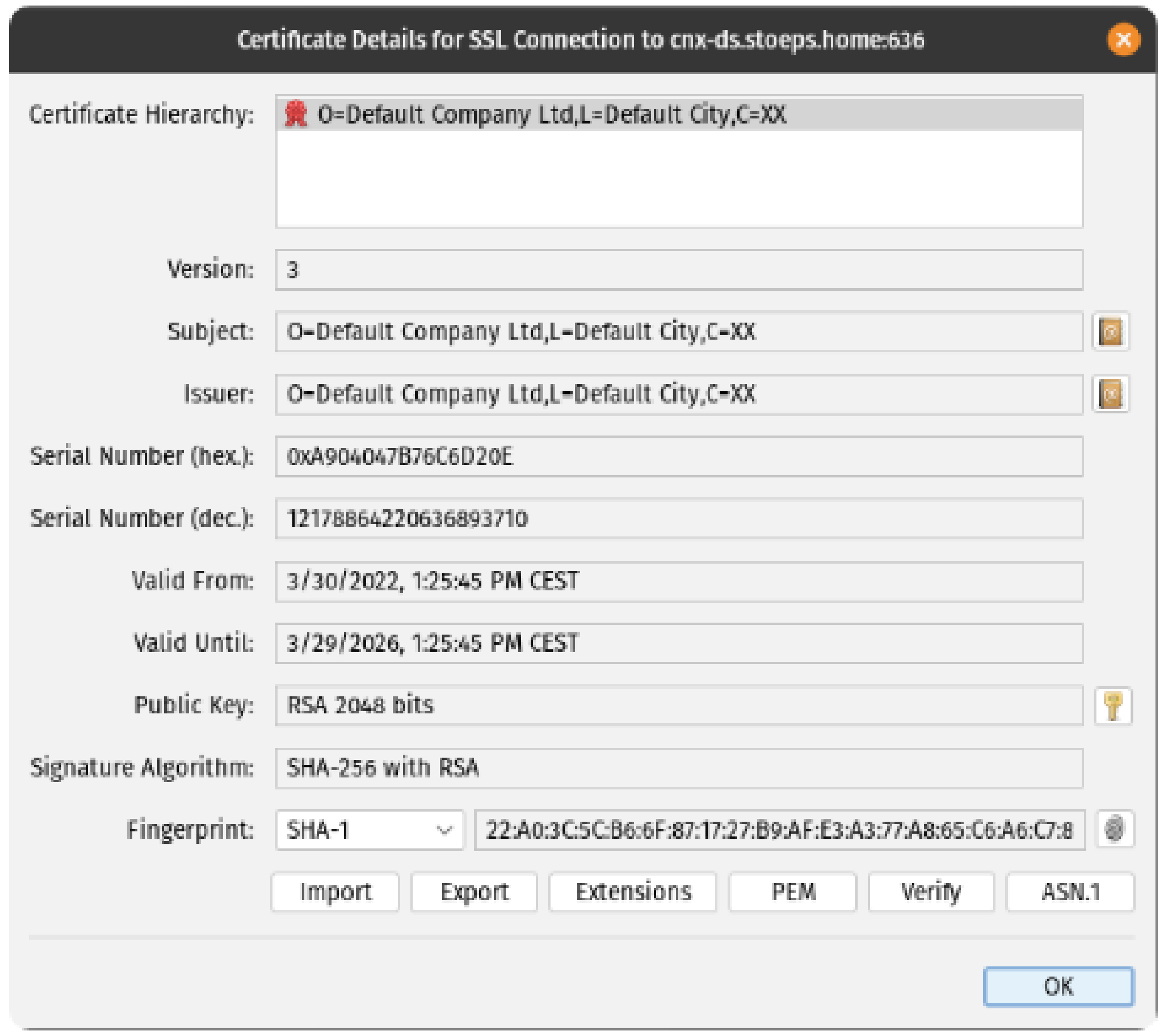
Keystore Explorer — Import Signer For TDI (2)

- Save Keystore (asks for password)
- Copy to your tdi solution directory
  - Add to `solution.properties`

```
javax.net.ssl.trustStore=tdi-keystore.jks
{protect}-javax.net.ssl.trustStorePassword=password
javax.net.ssl.trustStoreType=jks
```

- Enable SSL in `profiles_tdi.properties`

```
source_ldap_url=ldap://cnx-ds.stoeps.home:636
source_ldap_use_ssl=true
```



Certificate Details for SSL Connection to cnx-ds.stoeps.home:636

Certificate Hierarchy: O=Default Company Ltd,L=Default City,C=XX

Version: 3

Subject: O=Default Company Ltd,L=Default City,C=XX

Issuer: O=Default Company Ltd,L=Default City,C=XX

Serial Number (hex.): 0xA904047B76C6D20E

Serial Number (dec.): 12178864220636893710

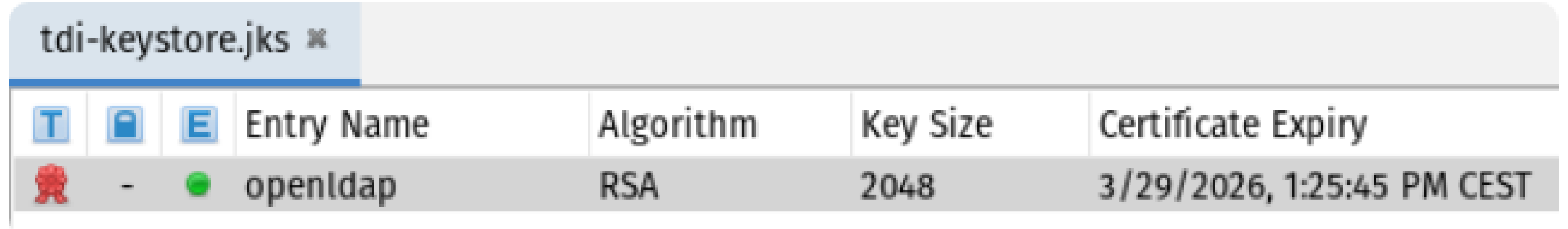
Valid From: 3/30/2022, 1:25:45 PM CEST

Valid Until: 3/29/2026, 1:25:45 PM CEST

Public Key: RSA 2048 bits

Signature Algorithm: SHA-256 with RSA

Fingerprint: SHA-1 22:A0:3C:5C:B6:6F:87:17:27:B9:AF:E3:A3:77:A8:65:C6:A6:C7:8



tdi-keystore.jks

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry
	-	●	openldap	RSA	2048	3/29/2026, 1:25:45 PM CEST

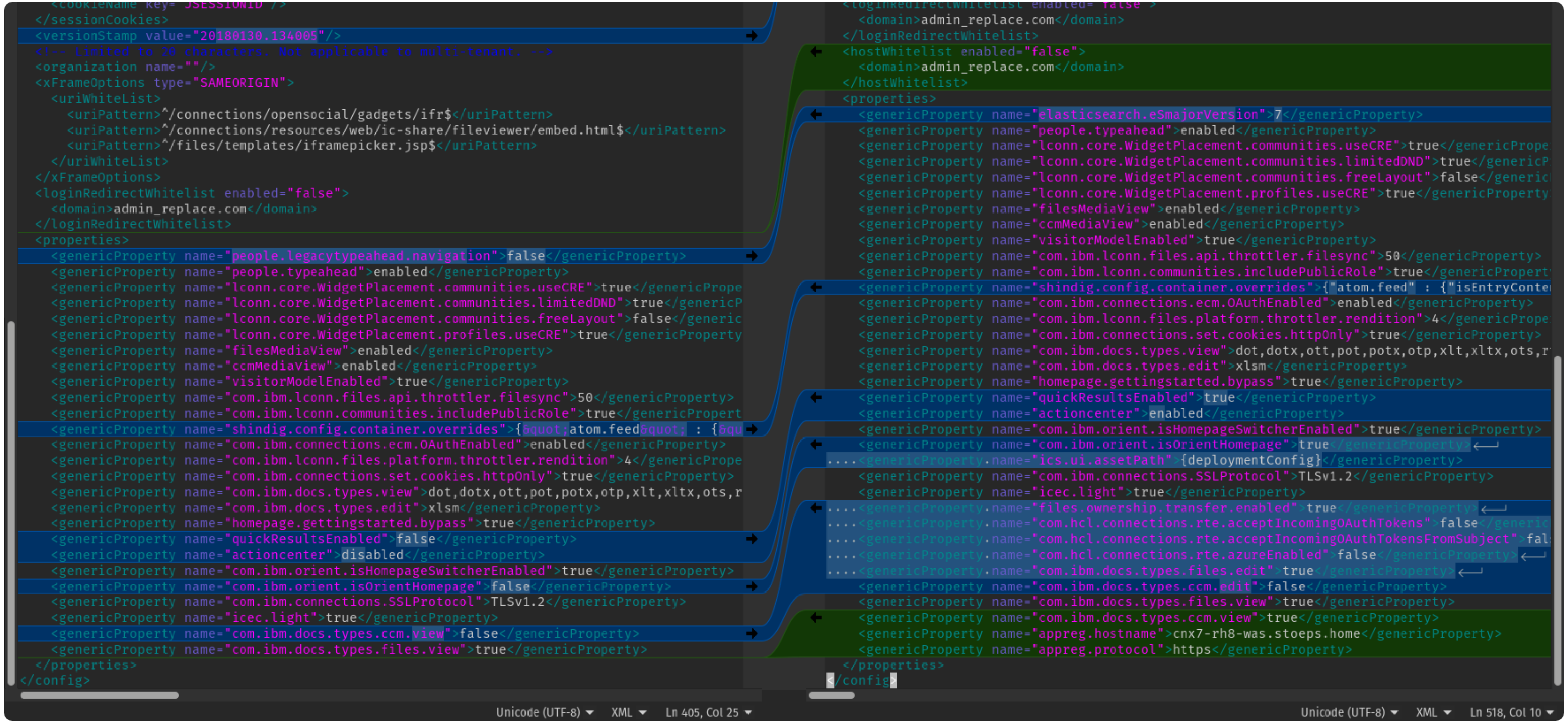
Version Control

- `git`
- Versioning for these directories
  - `Dmgr01/config/cells/<cellname>/LotusConnections-config/`
  - `<sharedDirectory>/customization`
  - tdisol
- `.gitignore`
  - `*.jar`
  - `*.xsd`
- Branches for new features
  - Switching branches to test a feature, merge to keep
- Linux / Windows format conversion on the fly

Compare Files

- Compare files between production and testing
- Side by side migration, compare directory trees
  - NEVER trust your documentation to find all changes
- Software
  - Meld (GPL v2)
  - Git
  - Beyond Compare
    - 30$
    - Trial

Meld



```
    <cookieName key="JSESSIONID"/>
  </sessionCookies>
  <versionStamp value="20180130.134005"/>
  <!-- Limited to 20 characters. Not applicable to multi-tenant. -->
  <organization name=""/>
  <xFrameOptions type="SAMEORIGIN">
    <uriWhiteList>
      <uriPattern>^/connections/opensocial/gadgets/ifr$</uriPattern>
      <uriPattern>^/connections/resources/web/ic-share/fileviewer/embed.html$</uriPattern>
      <uriPattern>^/files/templates/iframepicker.jsp$</uriPattern>
    </uriWhiteList>
  </xFrameOptions>
  <loginRedirectWhitelist enabled="false">
    <domain>admin_replace.com</domain>
  </loginRedirectWhitelist>
  <properties>
    <genericProperty name="people.legacytypeahead.navigation">false</genericProperty>
    <genericProperty name="people.typeahead">enabled</genericProperty>
    <genericProperty name="lconn.core.WidgetPlacement.communities.useCRE">true</genericPrope
    <genericProperty name="lconn.core.WidgetPlacement.communities.limitedDND">true</genericP
    <genericProperty name="lconn.core.WidgetPlacement.communities.freeLayout">false</generic
    <genericProperty name="lconn.core.WidgetPlacement.profiles.useCRE">true</genericProperty
    <genericProperty name="filesMediaView">enabled</genericProperty>
    <genericProperty name="ccmMediaView">enabled</genericProperty>
    <genericProperty name="visitorModelEnabled">true</genericProperty>
    <genericProperty name="com.ibm.lconn.files.api.throttler.filesync">50</genericProperty>
    <genericProperty name="com.ibm.lconn.communities.includePublicRole">true</genericPropert
    <genericProperty name="shindig.config.container.overrides">{&quot;atom.feed&quot; : {&qu
    <genericProperty name="com.ibm.connections.ecm.OAuthEnabled">enabled</genericProperty>
    <genericProperty name="com.ibm.lconn.files.platform.throttler.rendition">4</genericPrope
    <genericProperty name="com.ibm.connections.set.cookies.httpOnly">true</genericProperty>
    <genericProperty name="com.ibm.docs.types.view">dot,dotx,ott,pot,potx,otp,xlt,xltx,ots,r
    <genericProperty name="com.ibm.docs.types.edit">xlsm</genericProperty>
    <genericProperty name="homepage.gettingstarted.bypass">true</genericProperty>
    <genericProperty name="quickResultsEnabled">false</genericProperty>
    <genericProperty name="actioncenter">disabled</genericProperty>
    <genericProperty name="com.ibm.orient.isHomepageSwitcherEnabled">true</genericProperty>
    <genericProperty name="com.ibm.orient.isOrientHomepage">false</genericProperty>
    <genericProperty name="com.ibm.connections.SSLProtocol">TLSv1.2</genericProperty>
    <genericProperty name="icec.light">true</genericProperty>
    <genericProperty name="com.ibm.docs.types.ccm.view">false</genericProperty>
    <genericProperty name="com.ibm.docs.types.files.view">true</genericProperty>
  </properties>
</config>
```

Unicode (UTF-8) ▾ XML ▾ Ln 405, Col 25 ▾

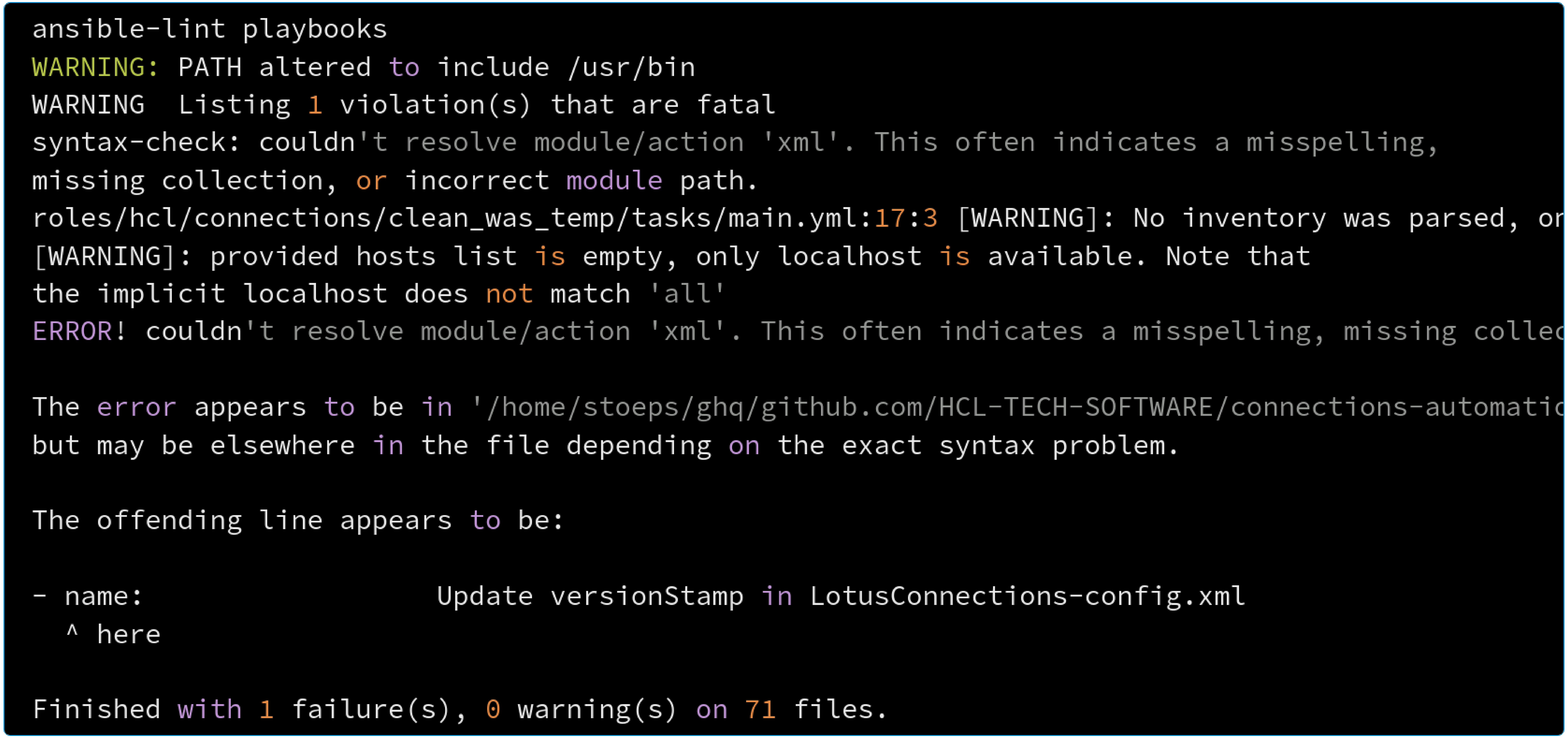
```
  <loginRedirectWhitelist enabled="false">
    <domain>admin_replace.com</domain>
  </loginRedirectWhitelist>
  <hostWhitelist enabled="false">
    <domain>admin_replace.com</domain>
  </hostWhitelist>
  <properties>
    <genericProperty name="elasticsearch.eSmajorVersion">7</genericProperty>
    <genericProperty name="people.typeahead">enabled</genericProperty>
    <genericProperty name="lconn.core.WidgetPlacement.communities.useCRE">true</genericPrope
    <genericProperty name="lconn.core.WidgetPlacement.communities.limitedDND">true</genericP
    <genericProperty name="lconn.core.WidgetPlacement.communities.freeLayout">false</generic
    <genericProperty name="lconn.core.WidgetPlacement.profiles.useCRE">true</genericProperty
    <genericProperty name="filesMediaView">enabled</genericProperty>
    <genericProperty name="ccmMediaView">enabled</genericProperty>
    <genericProperty name="visitorModelEnabled">true</genericProperty>
    <genericProperty name="com.ibm.lconn.files.api.throttler.filesync">50</genericProperty>
    <genericProperty name="com.ibm.lconn.communities.includePublicRole">true</genericPropert
    <genericProperty name="shindig.config.container.overrides">{"atom.feed" : {"isEntryConte
    <genericProperty name="com.ibm.connections.ecm.OAuthEnabled">enabled</genericProperty>
    <genericProperty name="com.ibm.lconn.files.platform.throttler.rendition">4</genericPrope
    <genericProperty name="com.ibm.connections.set.cookies.httpOnly">true</genericProperty>
    <genericProperty name="com.ibm.docs.types.view">dot,dotx,ott,pot,potx,otp,xlt,xltx,ots,r
    <genericProperty name="com.ibm.docs.types.edit">xlsm</genericProperty>
    <genericProperty name="homepage.gettingstarted.bypass">true</genericProperty>
    <genericProperty name="quickResultsEnabled">true</genericProperty>
    <genericProperty name="actioncenter">enabled</genericProperty>
    <genericProperty name="com.ibm.orient.isHomepageSwitcherEnabled">true</genericProperty>
    <genericProperty name="com.ibm.orient.isOrientHomepage">true</genericProperty>⟵
....<genericProperty.name="ics.ui.assetPath">{deploymentConfig}</genericProperty>
    <genericProperty name="com.ibm.connections.SSLProtocol">TLSv1.2</genericProperty>
    <genericProperty name="icec.light">true</genericProperty>
....<genericProperty.name="files.ownership.transfer.enabled">true</genericProperty>⟵
....<genericProperty.name="com.hcl.connections.rte.acceptIncomingOAuthTokens">false</generic
....<genericProperty.name="com.hcl.connections.rte.acceptIncomingOAuthTokensFromSubject">fal
....<genericProperty.name="com.hcl.connections.rte.azureEnabled">false</genericProperty>⟵
....<genericProperty.name="com.ibm.docs.types.files.edit">true</genericProperty>⟵
    <genericProperty name="com.ibm.docs.types.ccm.edit">false</genericProperty>
    <genericProperty name="com.ibm.docs.types.files.view">true</genericProperty>
    <genericProperty name="com.ibm.docs.types.ccm.view">true</genericProperty>
    <genericProperty name="appreg.hostname">cnx7-rh8-was.stoeps.home</genericProperty>
    <genericProperty name="appreg.protocol">https</genericProperty>
  </properties>
</config>
```

Unicode (UTF-8) ▾ XML ▾ Ln 518, Col 10 ▾

Linter

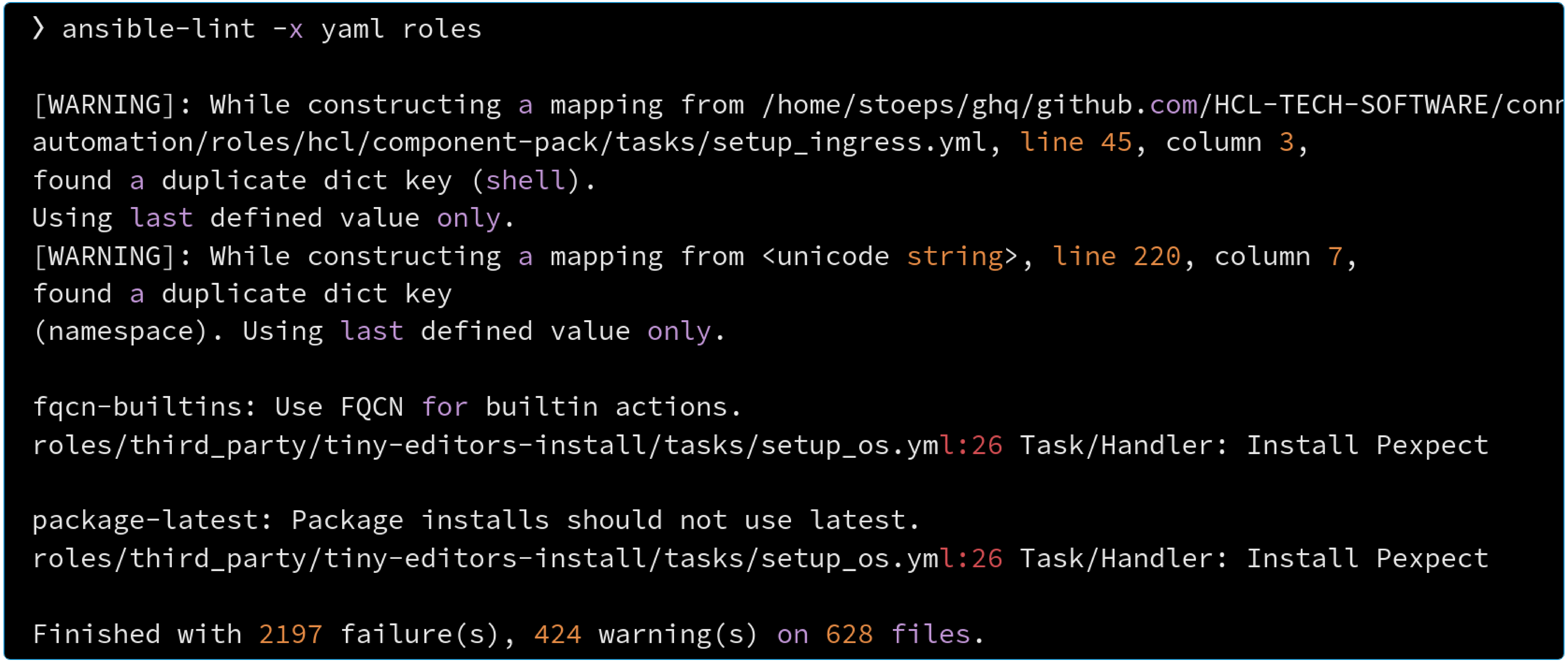
- As standalone tools, or integrated into your favorite editor
  - VIM, Emacs
  - VS Code, notepad++
- Examples
  - Ansible-lint
    - Ansible: Linting playbooks, roles and collections
  - yamllint
    - Kubernetes, Ansible
    - Autocomplete in editors, test in CI/CD pipeline
  - config-lint
    - Validates: Terraform, Kubernetes, LintRules, YAML, JSON
  - LanguageTool
    - Spellchecker, Grammar, Standalone, integrated in editor, browser add-on

Ansible Lint



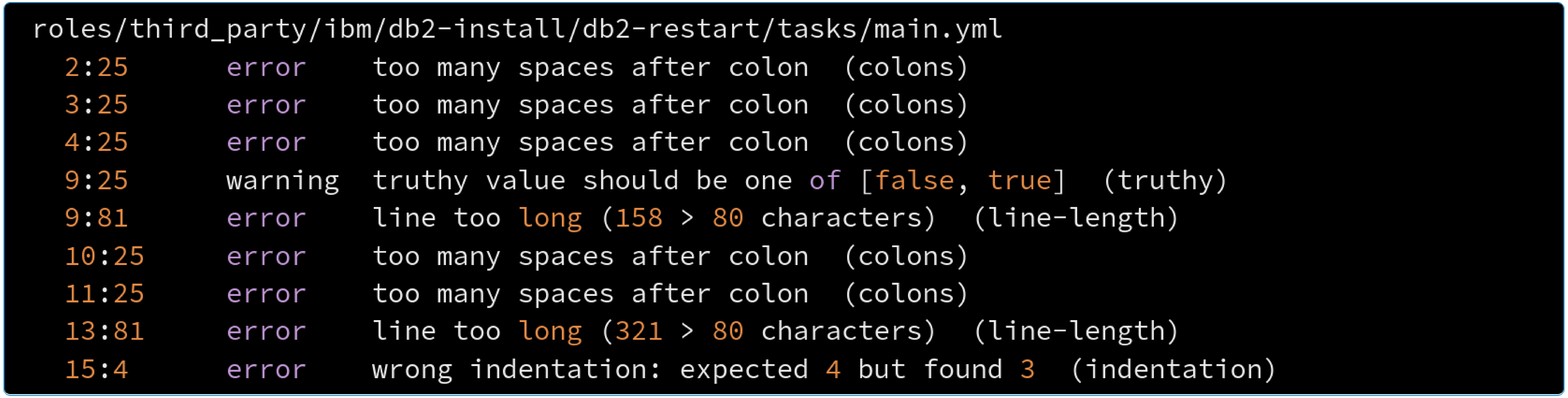
```
ansible-lint playbooks
WARNING: PATH altered to include /usr/bin
WARNING  Listing 1 violation(s) that are fatal
syntax-check: couldn't resolve module/action 'xml'. This often indicates a misspelling,
missing collection, or incorrect module path.
roles/hcl/connections/clean_was_temp/tasks/main.yml:17:3 [WARNING]: No inventory was parsed, or
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'
ERROR! couldn't resolve module/action 'xml'. This often indicates a misspelling, missing collec

The error appears to be in '/home/stoeps/ghq/github.com/HCL-TECH-SOFTWARE/connections-automatic
but may be elsewhere in the file depending on the exact syntax problem.

The offending line appears to be:

- name:                  Update versionStamp in LotusConnections-config.xml
  ^ here

Finished with 1 failure(s), 0 warning(s) on 71 files.
```

Ansible Lint



```
❯ ansible-lint -x yaml roles

[WARNING]: While constructing a mapping from /home/stoeps/ghq/github.com/HCL-TECH-SOFTWARE/conn
automation/roles/hcl/component-pack/tasks/setup_ingress.yml, line 45, column 3,
found a duplicate dict key (shell).
Using last defined value only.
[WARNING]: While constructing a mapping from <unicode string>, line 220, column 7,
found a duplicate dict key
(namespace). Using last defined value only.

fqcn-builtins: Use FQCN for builtin actions.
roles/third_party/tiny-editors-install/tasks/setup_os.yml:26 Task/Handler: Install Pexpect

package-latest: Package installs should not use latest.
roles/third_party/tiny-editors-install/tasks/setup_os.yml:26 Task/Handler: Install Pexpect

Finished with 2197 failure(s), 424 warning(s) on 628 files.
```

Yamllint



```
roles/third_party/ibm/db2-install/db2-restart/tasks/main.yml
  2:25      error    too many spaces after colon  (colons)
  3:25      error    too many spaces after colon  (colons)
  4:25      error    too many spaces after colon  (colons)
  9:25      warning  truthy value should be one of [false, true]  (truthy)
  9:81      error    line too long (158 > 80 characters)  (line-length)
  10:25     error    too many spaces after colon  (colons)
  11:25     error    too many spaces after colon  (colons)
  13:81     error    line too long (321 > 80 characters)  (line-length)
  15:4      error    wrong indentation: expected 4 but found 3  (indentation)
```

Extract Fixes And Jars

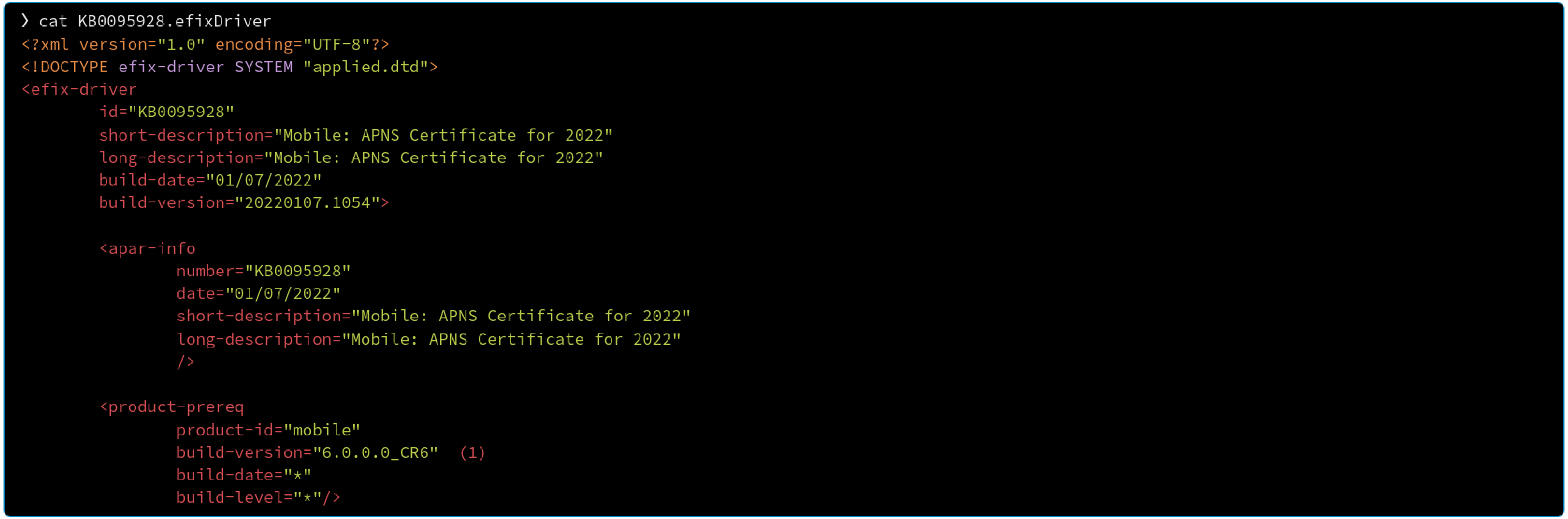
- 7-zip
- Check fixes jar for version and replaced files/paths
- Extract jars (Java bundles, CFixes)
  - get customization files, check for changes
  - remove classes (Log4Shell workaround)

Decompiler (Find Issues)

- `jd-gui`
  - Java Decompiler
- Ghidra
  - A software reverse engineering (SRE) suite of tools developed by NSA

Check Product Version Of A Fix

- Extract `jar`-file and Search efixDriver file

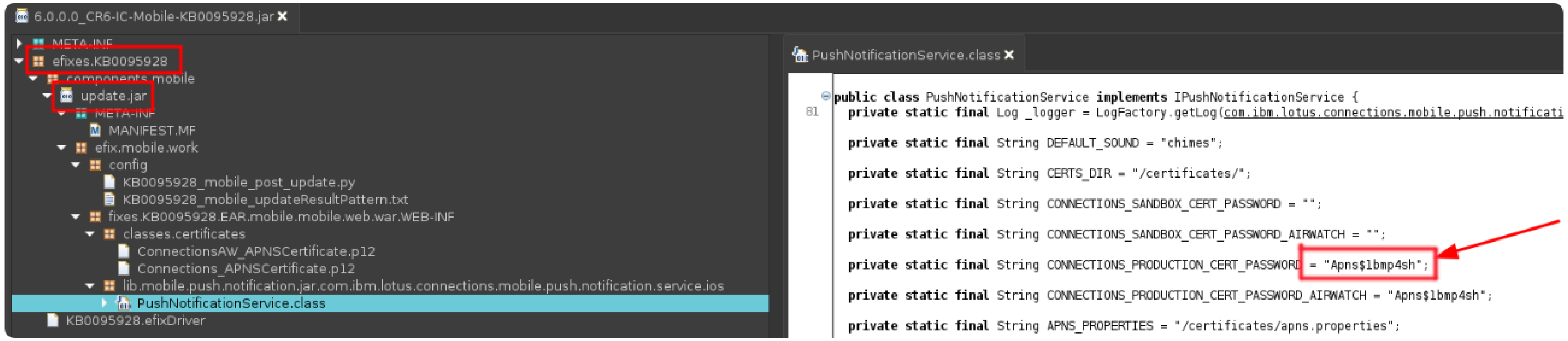


```
❯ cat KB0095928.efixDriver
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE efix-driver SYSTEM "applied.dtd">
<efix-driver
        id="KB0095928"
        short-description="Mobile: APNS Certificate for 2022"
        long-description="Mobile: APNS Certificate for 2022"
        build-date="01/07/2022"
        build-version="20220107.1054">

        <apar-info
                number="KB0095928"
                date="01/07/2022"
                short-description="Mobile: APNS Certificate for 2022"
                long-description="Mobile: APNS Certificate for 2022"
                />

        <product-prereq
                product-id="mobile"
                build-version="6.0.0.0_CR6"  (1)
                build-date="*"
                build-level="*"/>
```

1 Check build version

jd-gui

- Example check Mobile APNS update file

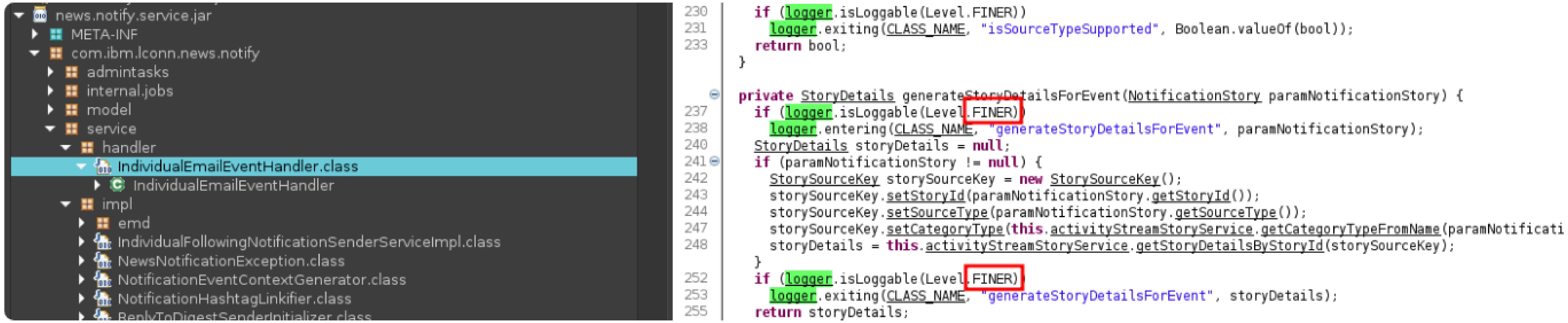


```
6.0.0.0_CR6-IC-Mobile-KB0095928.jar
▸ META-INF
▾ efixes.KB0095928
  ▾ components.mobile
    ▾ update.jar
      ▾ META-INF
          MANIFEST.MF
      ▾ efix.mobile.work
        ▾ config
            KB0095928_mobile_post_update.py
            KB0095928_mobile_updateResultPattern.txt
        ▾ fixes.KB0095928.EAR.mobile.mobile.web.war.WEB-INF
          ▾ classes.certificates
              ConnectionsAW_APNSCertificate.p12
              Connections_APNSCertificate.p12
          ▾ lib.mobile.push.notification.jar.com.ibm.lotus.connections.mobile.push.notification.service.ios
            ▸ PushNotificationService.class
    KB0095928.efixDriver
```

PushNotificationService.class

```java
public class PushNotificationService implements IPushNotificationService {
  private static final Log _logger = LogFactory.getLog(com.ibm.lotus.connections.mobile.push.notificati

  private static final String DEFAULT_SOUND = "chimes";

  private static final String CERTS_DIR = "/certificates/";

  private static final String CONNECTIONS_SANDBOX_CERT_PASSWORD = "";

  private static final String CONNECTIONS_SANDBOX_CERT_PASSWORD_AIRWATCH = "";

  private static final String CONNECTIONS_PRODUCTION_CERT_PASSWORD = "Apns$1bmp4sh";

  private static final String CONNECTIONS_PRODUCTION_CERT_PASSWORD_AIRWATCH = "Apns$1bmp4sh";

  private static final String APNS_PROPERTIES = "/certificates/apns.properties";
```

- Check ear-files, find trace settings

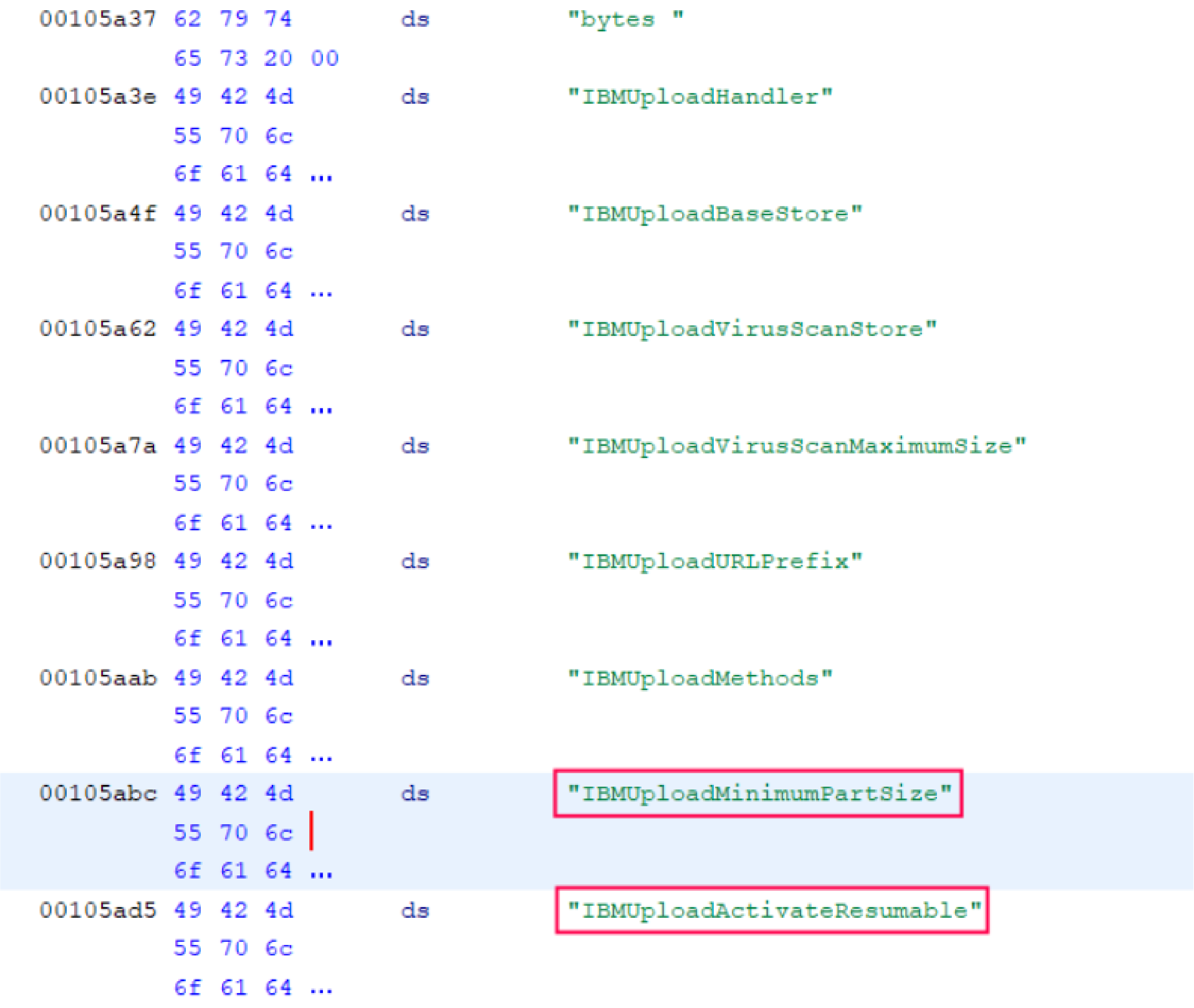


```
▾ news.notify.service.jar
  ▸ META-INF
  ▾ com.ibm.lconn.news.notify
    ▸ admintasks
    ▸ internal.jobs
    ▸ model
    ▾ service
      ▾ handler
        ▾ IndividualEmailEventHandler.class
          ▸ IndividualEmailEventHandler
      ▾ impl
        ▸ emd
        ▸ IndividualFollowingNotificationSenderServiceImpl.class
        ▸ NewsNotificationException.class
        ▸ NotificationEventContextGenerator.class
        ▸ NotificationHashtagLinkifier.class
        ▸ ReplyToDigestSenderInitializer.class
```

```java
    if (logger.isLoggable(Level.FINER))
      logger.exiting(CLASS_NAME, "isSourceTypeSupported", Boolean.valueOf(bool));
    return bool;
  }

  private StoryDetails generateStoryDetailsForEvent(NotificationStory paramNotificationStory) {
    if (logger.isLoggable(Level.FINER))
      logger.entering(CLASS_NAME, "generateStoryDetailsForEvent", paramNotificationStory);
    StoryDetails storyDetails = null;
    if (paramNotificationStory != null) {
      StorySourceKey storySourceKey = new StorySourceKey();
      storySourceKey.setStoryId(paramNotificationStory.getStoryId());
      storySourceKey.setSourceType(paramNotificationStory.getSourceType());
      storySourceKey.setCategoryType(this.activityStreamStoryService.getCategoryTypeFromName(paramNotificati
      storyDetails = this.activityStreamStoryService.getStoryDetailsByStoryId(storySourceKey);
    }
    if (logger.isLoggable(Level.FINER))
      logger.exiting(CLASS_NAME, "generateStoryDetailsForEvent", storyDetails);
    return storyDetails;
```

Ghidra

- Decompiler
- Check binaries for configuration strings
- Example shows mod_ibm_upload.so
  - Analyzed configuration parameters
  - Documentation missing
  - Article of this story



```
00105a37 62 79 74        ds         "bytes "
         65 73 20 00
00105a3e 49 42 4d        ds         "IBMUploadHandler"
         55 70 6c
         6f 61 64 ...
00105a4f 49 42 4d        ds         "IBMUploadBaseStore"
         55 70 6c
         6f 61 64 ...
00105a62 49 42 4d        ds         "IBMUploadVirusScanStore"
         55 70 6c
         6f 61 64 ...
00105a7a 49 42 4d        ds         "IBMUploadVirusScanMaximumSize"
         55 70 6c
         6f 61 64 ...
00105a98 49 42 4d        ds         "IBMUploadURLPrefix"
         55 70 6c
         6f 61 64 ...
00105aab 49 42 4d        ds         "IBMUploadMethods"
         55 70 6c
         6f 61 64 ...
00105abc 49 42 4d        ds         "IBMUploadMinimumPartSize"
         55 70 6c
         6f 61 64 ...
00105ad5 49 42 4d        ds         "IBMUploadActivateResumable"
         55 70 6c
         6f 61 64 ...
```

Database (JDBC) Client — DBeaver Community

- Supports DB2 and Elasticsearch

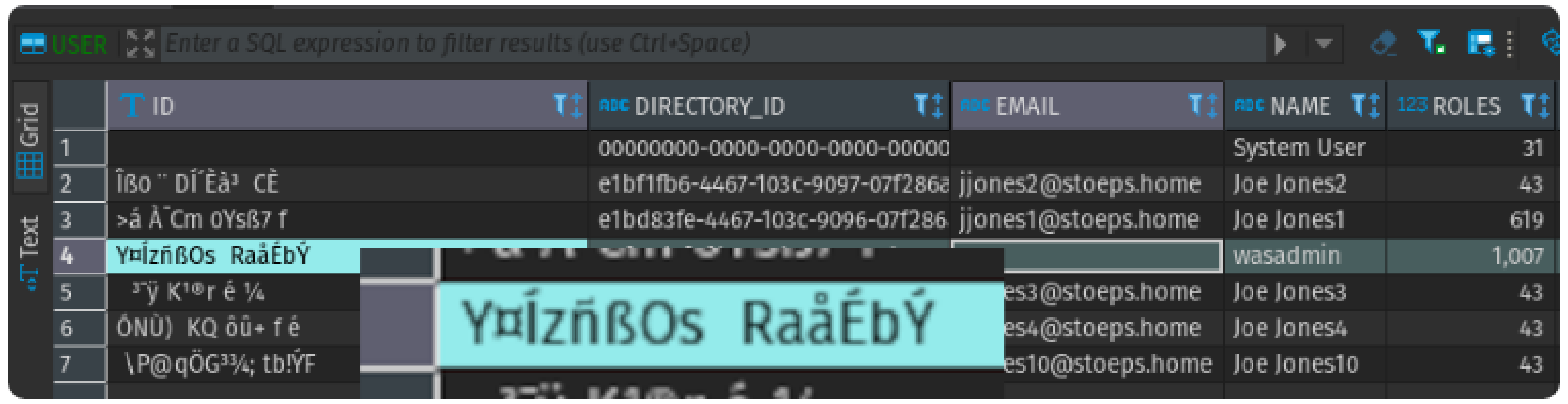
Elasticsearch

Open Distro Elasticsearch

DB2 iSeries/ AS 400

DB2 LUW

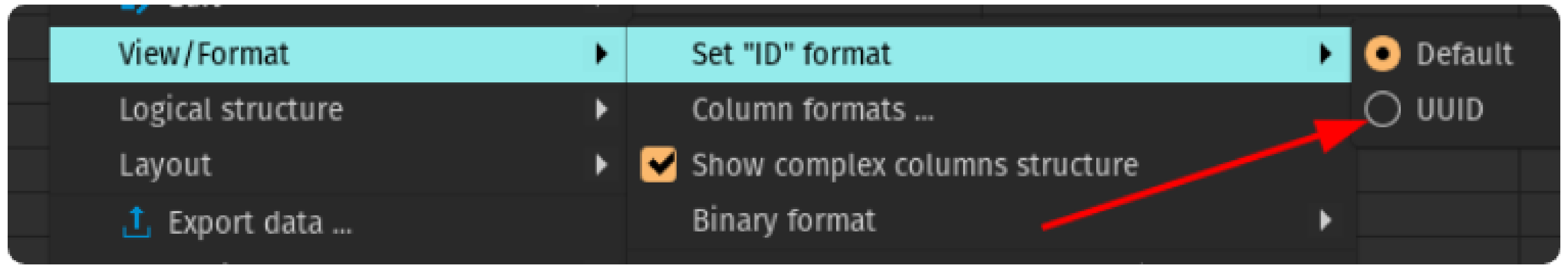
- Converts binary ids (Files, Wikis) to UUID format for better readability

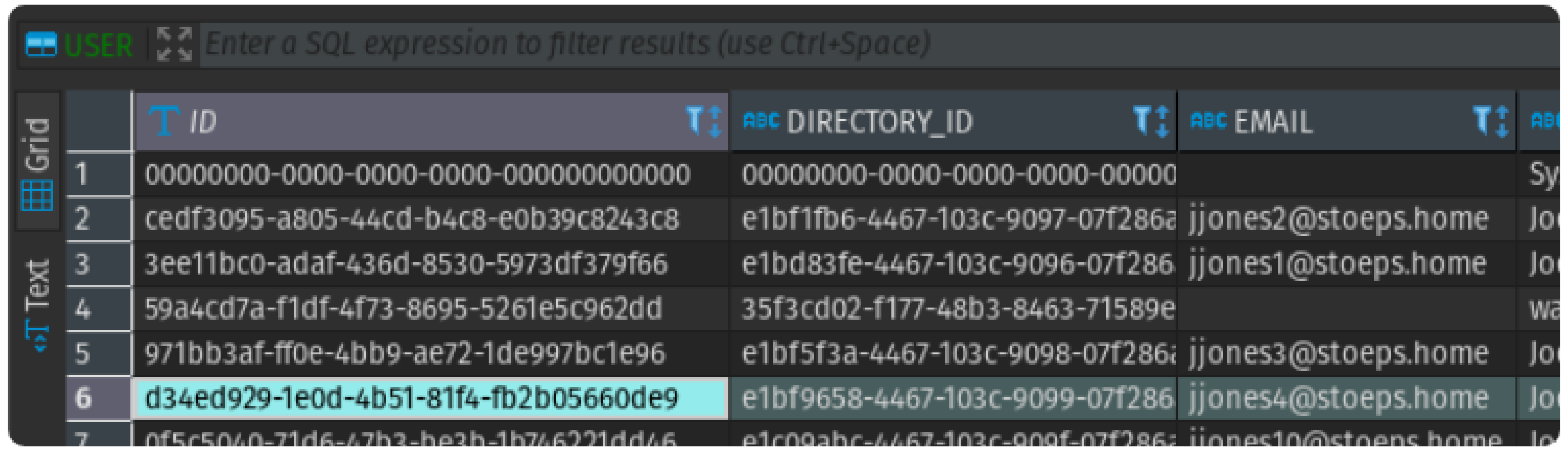


USER Enter a SQL expression to filter results (use Ctrl+Space)

	ID	DIRECTORY_ID	EMAIL	NAME	ROLES
1		00000000-0000-0000-0000-00000		System User	31
2	Îßo ¨ DÍ´Èà³ CÈ	e1bf1fb6-4467-103c-9097-07f286a	jjones2@stoeps.home	Joe Jones2	43
3	>á Å¯Cm 0Ysß7 f	e1bd83fe-4467-103c-9096-07f286	jjones1@stoeps.home	Joe Jones1	619
4	Y¤ÍzñßOs RaåÉbÝ			wasadmin	1,007
5	³ÿ K¹®r é ¼		es3@stoeps.home	Joe Jones3	43
6	ÔNÙ) KQ ôû+ f é		es4@stoeps.home	Joe Jones4	43
7	\P@qÖG³¾; tb!ÝF		es10@stoeps.home	Joe Jones10	43

Y¤ÍzñßOs RaåÉbÝ





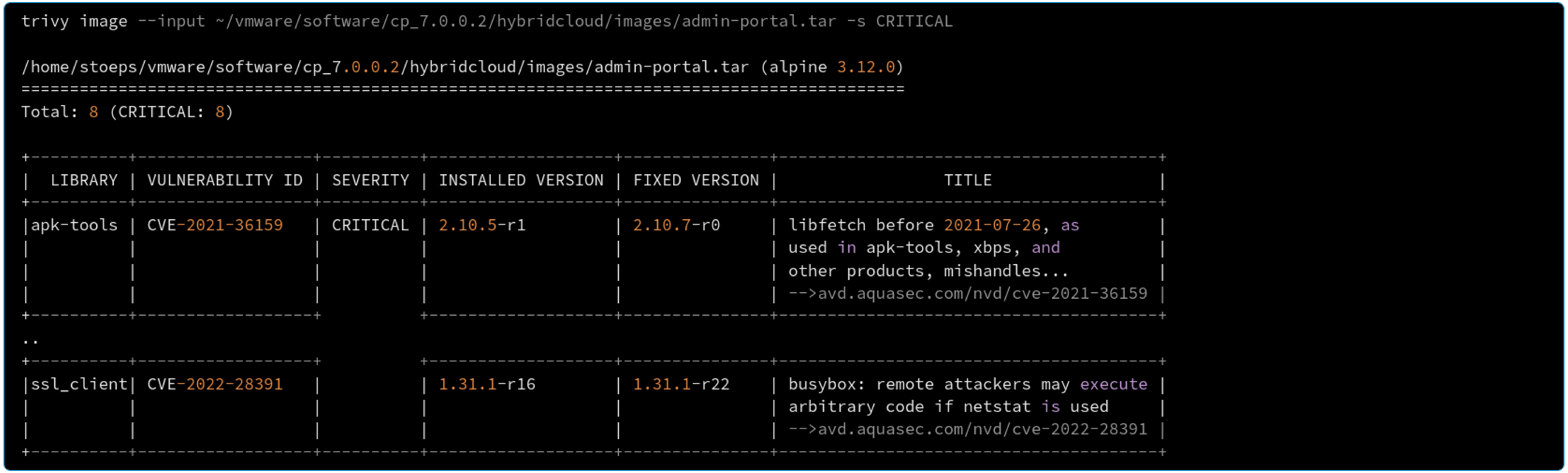
USER Enter a SQL expression to filter results (use Ctrl+Space)

	ID	DIRECTORY_ID	EMAIL	
1	00000000-0000-0000-0000-000000000000	00000000-0000-0000-0000-00000		Sy
2	cedf3095-a805-44cd-b4c8-e0b39c8243c8	e1bf1fb6-4467-103c-9097-07f286a	jjones2@stoeps.home	Jo
3	3ee11bc0-adaf-436d-8530-5973df379f66	e1bd83fe-4467-103c-9096-07f286	jjones1@stoeps.home	Jo
4	59a4cd7a-f1df-4f73-8695-5261e5c962dd	35f3cd02-f177-48b3-8463-71589e		wa
5	971bb3af-ff0e-4bb9-ae72-1de997bc1e96	e1bf5f3a-4467-103c-9098-07f286a	jjones3@stoeps.home	Jo
6	d34ed929-1e0d-4b51-81f4-fb2b05660de9	e1bf9658-4467-103c-9099-07f286	jjones4@stoeps.home	Jo
7	0f5c5040-71d6-47b3-be3b-1b746221dd46	e1c09abc-4467-103c-909f-07f286a	jjones10@stoeps.home	Jo

Security

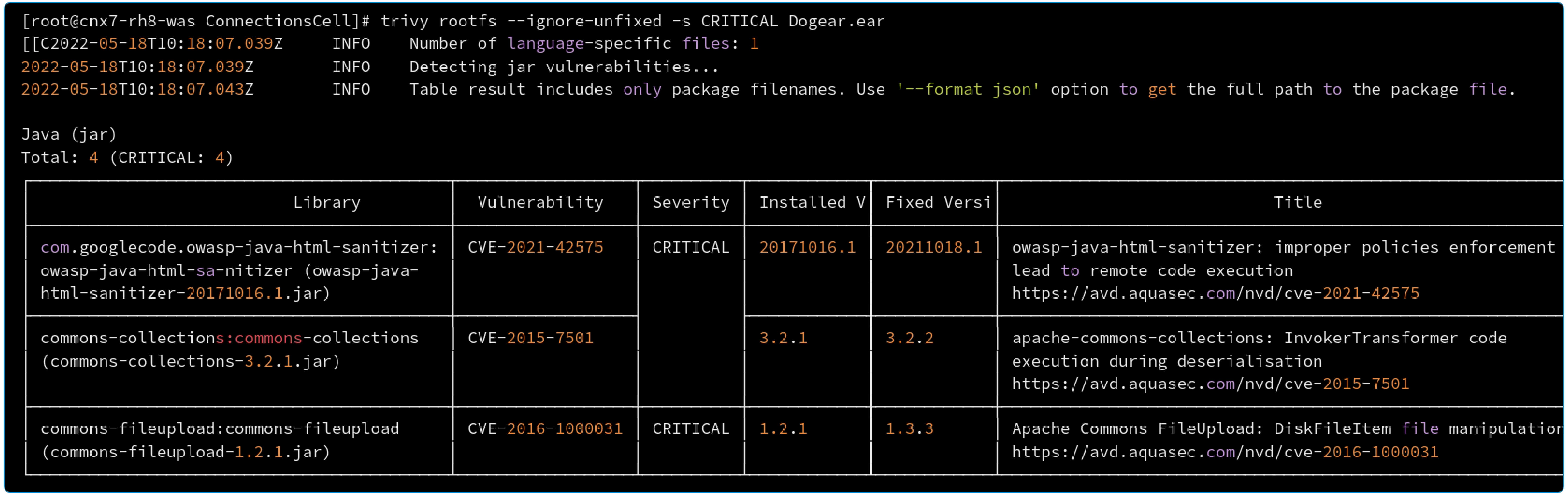
- trivy
  - File System
  - Registry (Container)
- Popeye
  - Scans live Kubernetes cluster
  - Detects misconfigurations
  - Helps you to ensure that best practices are in place

Trivy — Container Images



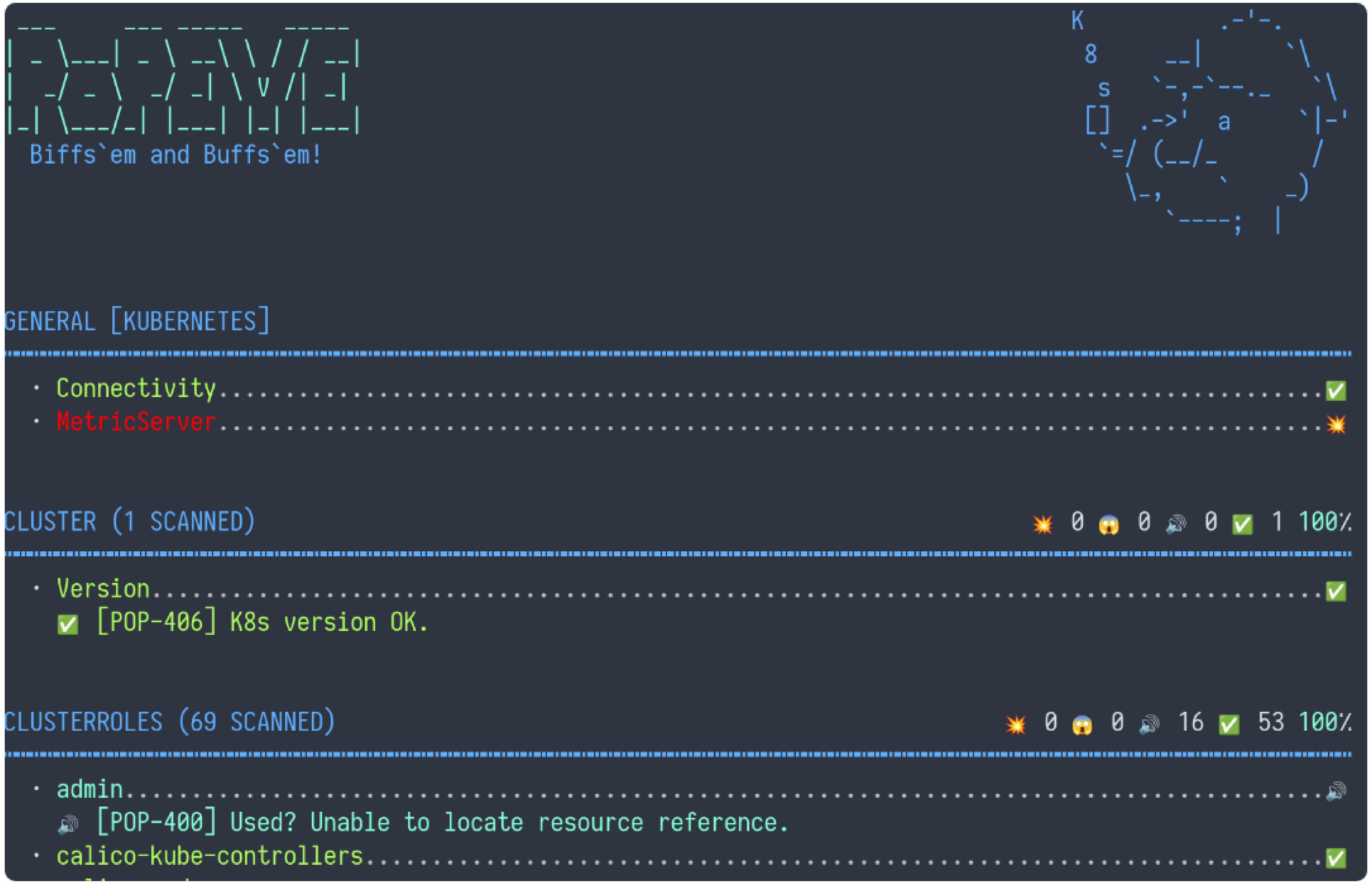
```
trivy image --input ~/vmware/software/cp_7.0.0.2/hybridcloud/images/admin-portal.tar -s CRITICAL

/home/stoeps/vmware/software/cp_7.0.0.2/hybridcloud/images/admin-portal.tar (alpine 3.12.0)
===========================================================================================
Total: 8 (CRITICAL: 8)

+----------+------------------+----------+-------------------+---------------+---------------------------------------+
|  LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |                 TITLE                 |
+----------+------------------+----------+-------------------+---------------+---------------------------------------+
|apk-tools | CVE-2021-36159   | CRITICAL | 2.10.5-r1         | 2.10.7-r0     | libfetch before 2021-07-26, as        |
|          |                  |          |                   |               | used in apk-tools, xbps, and          |
|          |                  |          |                   |               | other products, mishandles...         |
|          |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2021-36159 |
+----------+------------------+          +-------------------+---------------+---------------------------------------+
..
+----------+------------------+          +-------------------+---------------+---------------------------------------+
|ssl_client| CVE-2022-28391   |          | 1.31.1-r16        | 1.31.1-r22    | busybox: remote attackers may execute |
|          |                  |          |                   |               | arbitrary code if netstat is used     |
|          |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-28391 |
+----------+------------------+----------+-------------------+---------------+---------------------------------------+
```

Trivy — Filesystem



```
[root@cnx7-rh8-was ConnectionsCell]# trivy rootfs --ignore-unfixed -s CRITICAL Dogear.ear
[[C2022-05-18T10:18:07.039Z     INFO    Number of language-specific files: 1
2022-05-18T10:18:07.039Z        INFO    Detecting jar vulnerabilities...
2022-05-18T10:18:07.043Z        INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

Java (jar)
Total: 4 (CRITICAL: 4)

┌───────────────────────────────────────────┬──────────────────┬──────────┬────────────┬────────────┬────────────────────────────────────────────────────────
│                  Library                  │  Vulnerability   │ Severity │ Installed V│ Fixed Versi│                         Title
├───────────────────────────────────────────┼──────────────────┼──────────┼────────────┼────────────┼────────────────────────────────────────────────────────
│ com.googlecode.owasp-java-html-sanitizer: │ CVE-2021-42575   │ CRITICAL │ 20171016.1 │ 20211018.1 │ owasp-java-html-sanitizer: improper policies enforcement
│ owasp-java-html-sa-nitizer (owasp-java-   │                  │          │            │            │ lead to remote code execution
│ html-sanitizer-20171016.1.jar)            │                  │          │            │            │ https://avd.aquasec.com/nvd/cve-2021-42575
├───────────────────────────────────────────┼──────────────────┤          ├────────────┼────────────┼────────────────────────────────────────────────────────
│ commons-collections:commons-collections   │ CVE-2015-7501    │          │ 3.2.1      │ 3.2.2      │ apache-commons-collections: InvokerTransformer code
│ (commons-collections-3.2.1.jar)           │                  │          │            │            │ execution during deserialisation
│                                           │                  │          │            │            │ https://avd.aquasec.com/nvd/cve-2015-7501
├───────────────────────────────────────────┼──────────────────┼──────────┼────────────┼────────────┼────────────────────────────────────────────────────────
│ commons-fileupload:commons-fileupload     │ CVE-2016-1000031 │ CRITICAL │ 1.2.1      │ 1.3.3      │ Apache Commons FileUpload: DiskFileItem file manipulation
│ (commons-fileupload-1.2.1.jar)            │                  │          │            │            │ https://avd.aquasec.com/nvd/cve-2016-1000031
└───────────────────────────────────────────┴──────────────────┴──────────┴────────────┴────────────┴────────────────────────────────────────────────────────
```

popeye



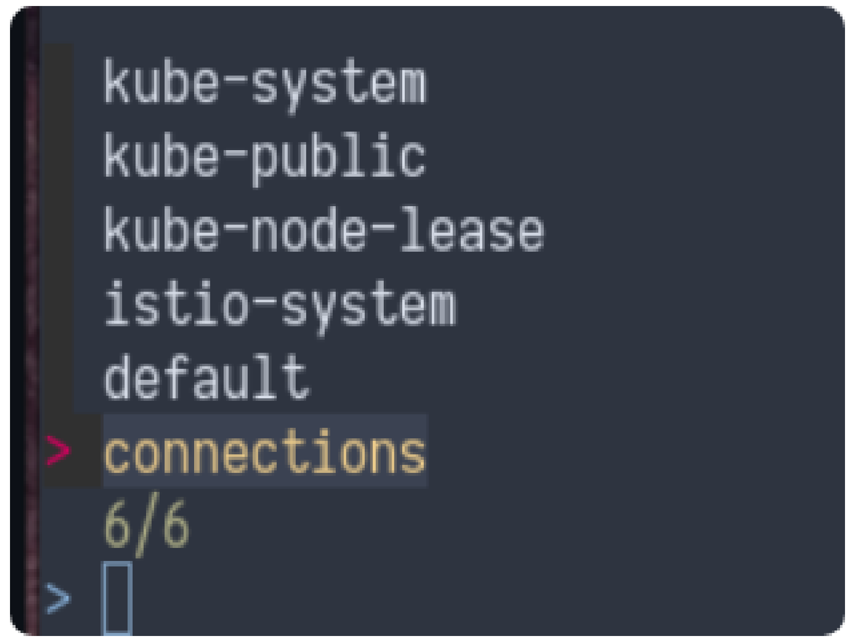
```
 ___     ___ _____   _____                                                  K          .-'-.
| _ \___| _ \ __\ \ / / __|                                                  8     __|      `\
|  _/ _ \  _/ _| \ V /| _|                                                    s   `-,-`--._   `\
|_| \___/_| |___| |_| |___|                                                  []  .->'  a     `|-'
  Biffs`em and Buffs`em!                                                      `=/ (__/_       /
                                                                                \_,    `    _)
                                                                                   `----;  |


GENERAL [KUBERNETES]
┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅
  · Connectivity.......................................................................✅
  · MetricServer.......................................................................💥


CLUSTER (1 SCANNED)                                                     💥 0 😱 0 🔊 0 ✅ 1 100٪
┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅
  · Version............................................................................✅
    ✅ [POP-406] K8s version OK.


CLUSTERROLES (69 SCANNED)                                              💥 0 😱 0 🔊 16 ✅ 53 100٪
┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅┅
  · admin..............................................................................🔊
    🔊 [POP-400] Used? Unable to locate resource reference.
  · calico-kube-controllers............................................................✅
```

Kubernetes

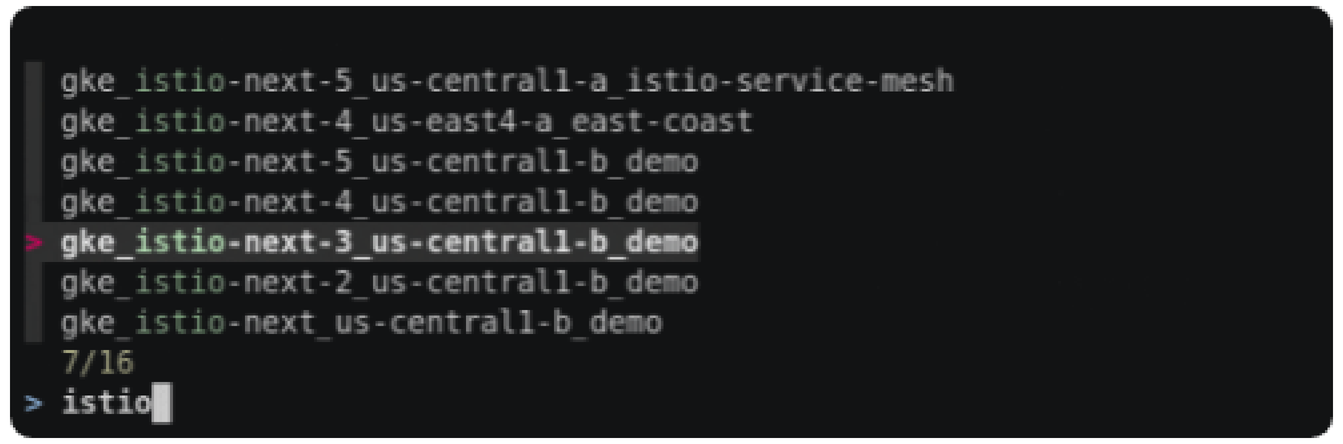
- Some tools to work faster on the console
  - kubectx, kubens
  - `fzf` for `kubectl`, `kubectx`
- Get logs from running pods
  - kubetail or stern
- Speed up the most used tasks with `kubectl`
  - K9s — (Win, Mac, Lnx)
- Get some insights of the blackbox Kubernetes
  - Linkerd, Istio

`kubectx`, `kubens`

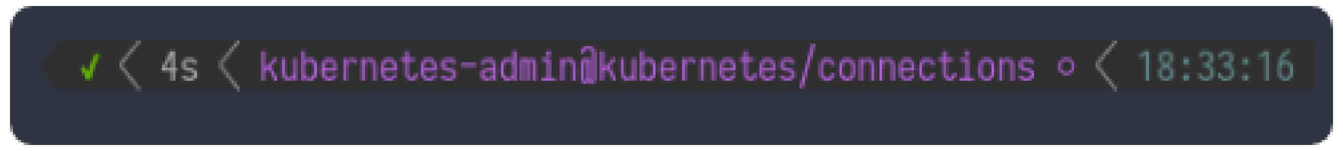
- Change context or namespace for `kubectl`
- `kubectl ns` shows all namespaces
  - select the namespace to set a new default
- Speed up `kubectl`
  - no need to type `-n connections` over and over again
- `kubectx` or `kubectl ctx`
  - set Kubernetes master and user to connect with `kubectl`
  - useful if you administrate multiple Kubernetes clusters from one host



```
  kube-system
  kube-public
  kube-node-lease
  istio-system
  default
> connections
  6/6
>
```



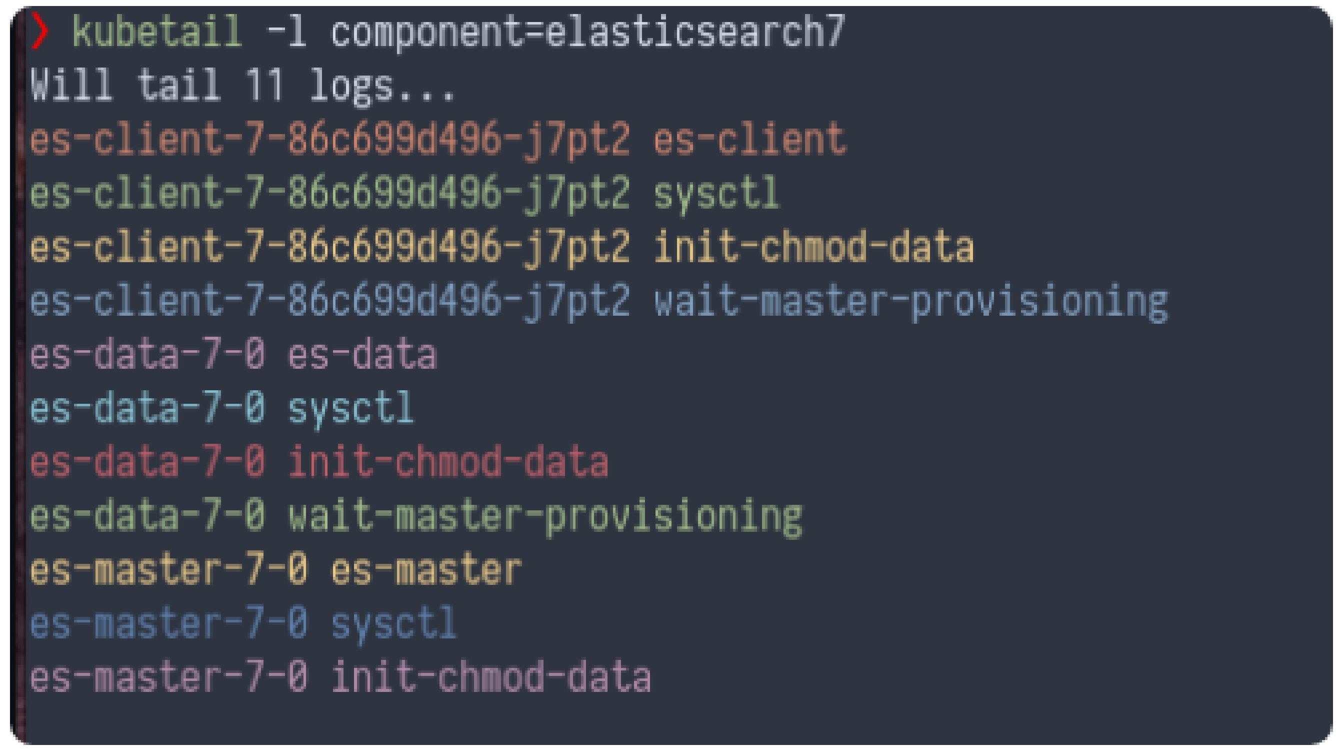
```
  gke_istio-next-5_us-central1-a_istio-service-mesh
  gke_istio-next-4_us-east4-a_east-coast
  gke_istio-next-5_us-central1-b_demo
  gke_istio-next-4_us-central1-b_demo
> gke_istio-next-3_us-central1-b_demo
  gke_istio-next-2_us-central1-b_demo
  gke_istio-next_us-central1-b_demo
  7/16
> istio
```



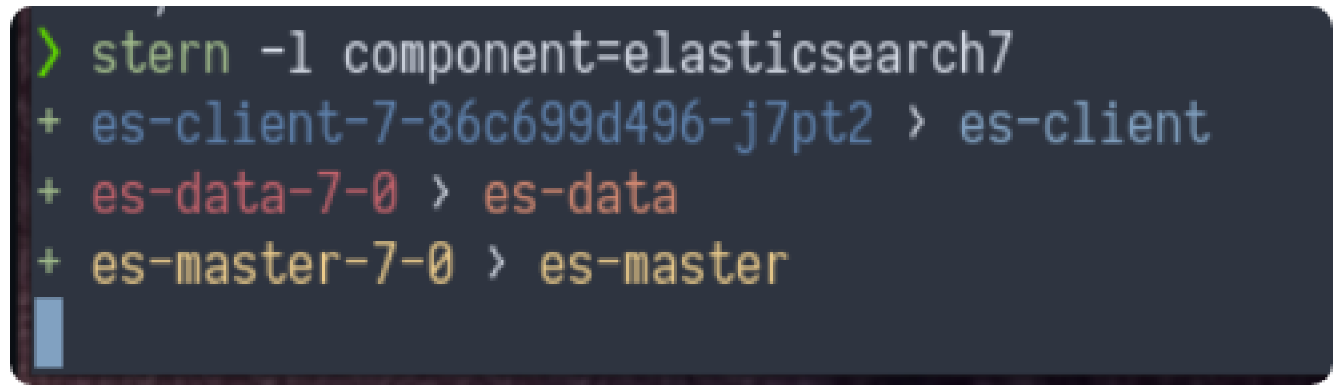
```
✓ ❮ 4s ❮ kubernetes-admin@kubernetes/connections ∘ ❮ 18:33:16
```

kubetail, stern

- kubetail
  - Display logs from multiple containers/pods
  - Regular Expression or label to select
- stern
  - Shows running container, not all
  - -c selects container



```
❯ kubetail -l component=elasticsearch7
Will tail 11 logs...
es-client-7-86c699d496-j7pt2 es-client
es-client-7-86c699d496-j7pt2 sysctl
es-client-7-86c699d496-j7pt2 init-chmod-data
es-client-7-86c699d496-j7pt2 wait-master-provisioning
es-data-7-0 es-data
es-data-7-0 sysctl
es-data-7-0 init-chmod-data
es-data-7-0 wait-master-provisioning
es-master-7-0 es-master
es-master-7-0 sysctl
es-master-7-0 init-chmod-data
```



```
❯ stern -l component=elasticsearch7
+ es-client-7-86c699d496-j7pt2 › es-client
+ es-data-7-0 › es-data
+ es-master-7-0 › es-master
```

k9s

- Replaces `watch kubectl get pods` for me
- Check logs of pods and containers from the terminal ui
- No complicated cli commands necessary

Istio

- Componentpack is somehow a black box
- No documentation on dependencies
  - Which pods should I check when for example Orient Me isn’t working
  - Which pods can you restart without affecting Customizer?
- Istio
  - Service Mesh
    - Traffic Management
    - Observability
    - Security

Istio Checking ComponentPack — Installation

Fast, but unsecure

```
curl -L https://istio.io/downloadIstio | ISTIO_VERSION=1.13.4 TARGET_ARCH=x86_64 sh -
cd istio-1.13.4
export PATH=$PWD/bin:$PATH
istioctl install --set profile=demo
istioctl manifest apply --set components.cni.enabled=true

kubectl get pods -n istio-system

NAME                                   READY   STATUS    RESTARTS   AGE
istio-cni-node-fgrhx                   1/1     Running   0          168m
istio-ingressgateway-76dcc86449-5z9rd  1/1     Running   0          168m
istiod-7664dfcb67-5wsgz                1/1     Running   0          168m
```

Istio Checking ComponentPack — Sidecar

Enable sidecars for namespace connections

```
kubectl label namespace connections istio-injection=enabled
```

Disable sidecar for Elasticsearch

```
kubectl edit statefulsets.apps/es-data-7
kubectl edit statefulsets.apps/es-master-7
kubectl edit deployment es-client-7
```

```
spec:
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
```

- Restart all statefulsets and deployments

Install Kiali On Top Of Istio

- Kiali is an observability console for Istio
  - With service mesh configuration and validation capabilities
- Helps you understand the structure and health of your service mesh

```
kubectl apply -f \
https://raw.githubusercontent.com/istio/istio/release-1.13/samples/addons/kiali.yaml

kubectl apply -f \
https://raw.githubusercontent.com/istio/istio/release-1.13/samples/addons/prometheus.yaml
```

Documentation

- I write most documention in
  - asciidoctor
  - markdown
  - LaTeX
- `pandoc` converts from any of these formats to (e.g.)
  - HTML
  - PDF
  - MS Word
  - …
- txt based formats can be version controlled in `git`

Container

- Work with local container
  - Use tools
  - Test
  - Change images
- Podman
- Docker
- Dive
  - Analyze container layer and changes

Some More Useful Tools For Daily Work

- JSON
  - gron
    - Gron the JSON flattener
  - JQ
- Ansible
  - Install tools on all servers with same paths and aliases
  - Commands on your fingertips in all environments

Session Slides

- PDF version at https://engage.ug/engage2.nsf/Pages/sessionagenda2022
- HTML version with embedded videos

Thank You!

Your feedback is important

stoeps@vegardit.com

VEGARD IT

Links For All Tools

- K6: https://k6.io
- Selenium: https://www.selenium.dev
- JMeter: https://jmeter.apache.org
- IBM TMDA: https://www.ibm.com/support/pages/ibm-thread-and-monitor-dump-analyzer-java-tmda
- GoAccess: https://github.com/allinurl/goaccess
- SAML-tracer: https://github.com/SimpleSAMLphp/SAML-tracer/
- Multi-Account Container: https://github.com/mozilla/multi-account-containers#readme
- Container Proxy: https://github.com/bekh6ex/firefox-container-proxy

Links For All Tools (2)

- OWASP Zed Attack Proxy (ZAP): https://www.zaproxy.org/
- Burp Suite: https://portswigger.net/burp
- mitmproxy: https://mitmproxy.org/
- Charles: https://www.charlesproxy.com/
- `testssl.sh`: https://testssl.sh/
- Keystore Explorer: https://keystore-explorer.org/
- Git: https://git-scm.com/
- Beyond Compare: https://www.scootersoftware.com/features.php?zz=features_focused
- Ansible-lint: https://ansible-lint.readthedocs.io/en/latest/

Links For All Tools (3)

- yamllint: https://github.com/adrienverge/yamllint
- config-linthttps://stelligent.github.io/config-lint/#/running[]
- LanguageTool: https://languagetool.org
- 7-zip: https://www.7-zip.org
- Ghidra: https://ghidra-sre.org/
- trivy: https://aquasecurity.github.io/trivy/v0.27.1/
- Popeye: https://popeyecli.io
- kubectx, kubens: https://github.com/ahmetb/kubectx

Links For All Tools (4)

- kubetail: https://github.com/johanhaleby/kubetail
- stern: https://github.com/wercker/stern
- K9s: https://github.com/derailed/k9s
- Linkerd: https://linkerd.io/
- Istio: https://istio.io/
- Asciidoctor: https://asciidoctor.org
- Markdown: https://daringfireball.net/projects/markdown/
- LaTeX: https://www.latex-project.org/
- Podman: https://podman.io

Links For All Tools (5)

- Docker: https://docker.io
- Dive: https://github.com/wagoodman/dive
- gron: https://github.com/tomnomnom/gron
- Gron the JSON flattener: https://www.datafix.com.au/BASHing/2022-03-23.html
- JQ: https://stedolan.github.io/jq/
- Session slides with Videos: https://share.stoeps.de/engage2022-admintoolbox.html