Hydra Infrastructure Management Guide

Student Container Platform Administration

Computer Science Department
SUNY New Paltz

Last Updated: January 2025

Contents

1 System O er iew

Hydra is a contain riz d d v lopm nt platform providing p rsist nt d v lopm nt nvironm nts for Comput r Sci nc stud nts and faculty at SUNY N w Paltz. Th syst m us s SAML 2.0 Singl Sign-On via Azur AD and Dock r for contain r orch stration.

1.1 Key Features

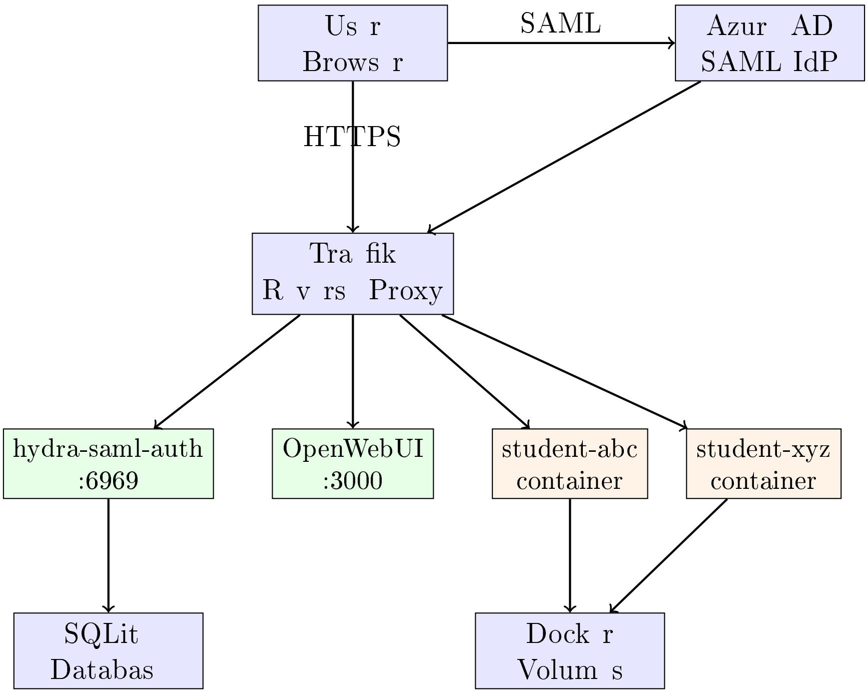
- **SSO Authentication:** Azur AD SAML 2.0 with automatic us r provisioning
- **Persistent Containers:** On d v lopm nt nvironm nt p r stud nt with data p rsist nc
- **Built-in Services:** VS Cod (cod -s rv r), Jupyt r Not book, Dock r-in-Dock r
- **Dynamic Routing:** Tra fik-bas d routing for custom w b applications
- **Resource Management:** P r-contain r CPU and m mory limits
- **Integration:** Op nW bUI (GPT) and n8n account manag m nt

1.2 Access URLs

Service	URL	Description
Dashboard	`https://hydr .newp ltz.edu/d shbo rd`	Main us r int rfac
Op nW bUI	`https://gpt.hydr .newp ltz.edu/`	AI chat int rfac
VS Cod	`https://hydr .newp ltz.edu/students/{user}/vscode`	Brows r IDE
Jupyt r	`https://hydr .newp ltz.edu/students/{user}/jupyter`	Not books

2 System Architecture

2.1 Architecture Diagram



2.2 Component Overview

Component	Port	Description
Tra fik	80, 443	R v rs proxy, TLS t rmination, routing
hydra-saml-auth	6969	SAML auth, dashboard, contain r manag m nt
Op nW bUI	3000	AI chat int rfac (Ollama front nd)
Stud nt Contain rs	Dynamic	P r-us r d v lopm nt nvironm nts

2.3 Network Architecture

Stud nt contain rs op rat on an isolat d Dock r n twork (`hydr _students_net`) with:

- No dir ct int rn t acc ss (configurabl)
- Int rnal DNS r solution
- Tra fik-m diat d xt rnal acc ss via ForwardAuth

3 Authentication System

3.1 SAML 2.0 SSO Flow

1. User visits https://hydra.newpaltz.edu/login

2. Hydra redirects to Azure AD with SAML AuthnRequest

3. User authenticates with New Paltz credentials

4. Azure AD returns signed SAML assertion

5. Hydra validates signature, extracts: email, groups, displayName

6. Session created, JWT cookie issued

7. User redirected to /dashboard

3.2 Session Management

S ssions ar manag d via:

- **Express Session:** S rv r-sid s ssion storag in SQLit
- **JWT Cookie:** Sit -wid auth ntication cooki for cross-s rvic SSO

- **JWKS Endpoint:** Public k y ndpoint for JWT v rification by oth r s rvic s

JWT Configuration:

- TTL: Configurabl via `JWT_TTL_SECONDS` (d fault: 86400)
- Algorithm: RS256
- Cooki Domain: `.newp ltz.edu`

4 Container System

4.1 Student Container Features

Each stud nt r c iv s a singl p rsist nt contain r with:

Feature	Details
Nod .js	Lat st LTS via nvm
Python	3.11+ with pip, v nv, Jupyt r
Java	Op nJDK 21
Dock r	Full Dock r-in-Dock r support (privil g d mod)
VS Cod	cod -s rv r brows r IDE
Jupyt r	Not book and Jupyt rLab
Tools	Git, curl, wg t, build- ss ntial, tc.

4.2 Resource Limits

Resource	Limit
RAM	4GB p r contain r
CPU	2 cor s p r contain r
Storag	Unlimit d (host disk limit d)

Security Note: Stud nt contain rs run in privil g d mod to support Dock r-in-Dock r. This grants l vat d acc ss. Monitor for abus and consid r disabling for untrust d us rs.

4.3 Port Routing

Stud nts can xpos w b applications through custom rout s:

- D fault rout s: `/students/{usern me}/vscode`, `/students/{usern me}/jupyter`
- Custom rout s add d via dashboard UI
- R s rv d ports: 8443 (cod -s rv r), 8888 (Jupyt r)
- All rout s prot ct d by ForwardAuth

5 File Structure

```
hydra-saml-auth/
|-- index.js              # Main entry: SAML, JWT/JWKS, routes,
   WebSocket
|-- db.js                 # SQLite database initialization
|-- routes/
|   |-- containers.js     # Container lifecycle, services, ports, logs
|   |-- webui-api.js      # OpenWebUI account proxy
|   |-- n8n-api.js        # n8n account management
|   |-- servers-api.js    # Cluster status endpoints
|   |-- admin.js          # Admin panel routes
|-- services/
|   |-- activity-logger.js    # Activity tracking
|   |-- email-notifications.js # Email alerts
|-- views/                # EJS templates
|-- student-container/
|   |-- Dockerfile        # Ubuntu 22.04 + dev tools
|   |-- supervisord.conf  # Process manager config
|   |-- entrypoint.sh     # Container startup
|-- docker-compose.yaml   # Production stack
|-- docs/                 # Documentation
```

6 Common Operations

6.1 View Running Containers

```
docker ps --filter "name=student-"
```

6.2 Access Container Shell

```
docker exec -it student-<username> /bin/bash
```

6.3 View Container Logs

```
docker logs -f student-<username> --tail=100
```

6.4 Restart a Container

```
docker restart student-<username>
```

6.5 Remove a Stuck Container

```
docker rm -f student-<username>
```

6.6 Rebuild Student Container Image

```
cd student-container
docker build -t hydra-student-container:latest .
```

Note: Stud nts with xisting contain rs must r cr at th m to us updat d imag s.

7 Ser ice Management

7.1 Restart Main Service

```
docker compose restart hydra-saml-auth
```

7.2 Rebuild and Redeploy

```
docker compose build hydra-saml-auth
docker compose up -d hydra-saml-auth
```

7.3 View Service Logs

```
docker compose logs -f hydra-saml-auth
```

7.4 Check Traefik Routing

```
docker compose logs traefik | grep -i error
curl -I https://hydra.newpaltz.edu/
```

8 Troubleshooting

8.1 Authentication Issues

Symptom	Solution
SAML ass rtion invalid	V rify `METADATA_URL` and `SAML_SP_ENTITY_ID` match Azur config xactly
Cooki not s t	Ch ck `COOKIE_DOMAIN`, nsur HTTPS, ch ck brows r s ttings
JWT v rification fails	V rify JWKS ndpoint acc ssibl , ch ck k y rotation

8.2 Container Issues

Symptom	Solution
Contain r won't initializ	V rify `hydr -student-cont iner:l test` imag xists
Contain r 404	Ch ck contain r is on `hydr _students_net`, Tra fik running
S rvic won't start	Ch ck sup rvisord logs insid contain r
Port routing fails	V rify port not r s rv d (8443, 8888) and not in us

8.3 Service-Specific Issues

- **VS Code not loading:** Ch ck cod -s rv r proc ss, ForwardAuth working
- **Jupyter issues:** V rify `NotebookApp.b se_url` s tting
- **Docker-in-Docker fails:** Contain r must hav privil g d mod
- **Files not persisting:** Only `/home/student/` is p rsist d

9 Backup and Reco ery

9.1 Database Backup

```
# Backup SQLite database
sqlite3 /app/data/webui.db ".backup ’/backups/hydra-$(date +%Y%m%d).db
   ’"

# Automated daily backup (add to crontab)
0 2 * * * sqlite3 /app/data/webui.db ".backup ’/backups/hydra-$(date
   +\%Y\%m\%d).db’"
```

9.2 Volume Backup

```
# List student volumes
docker volume ls | grep student-

# Backup a volume
docker run --rm -v student-<user>-data:/data -v $(pwd):/backup \
    alpine tar cvf /backup/student-<user>-backup.tar /data
```

10 En ironment Configuration

10.1 Required Variables

Variable	Description
BASE_URL	Ext rnal URL (https://hydra.n wpaltz. du)
METADATA_URL	Azur AD f d ration m tadata URL
SAML_SP_ENTITY_ID	SP Entity ID (must match Azur xactly)
COOKIE_DOMAIN	Cooki scop (.n wpaltz. du)
PORT	S rvic port (d fault: 6969)
DB_PATH	Databas path (/app/data/w bui.db)

10.2 Optional Variables

Variable	Description
PUBLIC_STUDENTS_BASE	Stud nt URL bas (https://hydra.n wpaltz. du/stud nts)
JWT_TTL_SECONDS	JWT tok n lif tim
JWT_PRIVATE_KEY_FILE	Path to JWT signing k y
JWT_PUBLIC_KEY_FILE	Path to JWT v rification k y

11 References

- Dock r Docum ntation: https://docs.docker.com/
- Tra fik Docum ntation: https://doc.tr efik.io/tr efik/
- SAML 2.0 Sp cification: https://docs.o sis-open.org/security/s ml/v2.0/
- Azur AD SAML: https://docs.microsoft.com/en-us/ zure/ ctive-directory/develop/single-sign-on-s ml-protocol
- cod -s rv r: https://coder.com/docs/code-server/l test
- Jupyt r: https://jupyter.org/document tion