TIER Grouper Packaging – What/Why?

- Grouper components packages in containers
- Easier Configuration, Deployment, and Adoption
- DevOps Practices and Methodologies
- Share knowledge and collect artifacts
Package Options for TIER Grouper

- Appliances (first offering)
  - VirtualBox VMs
  - AMIs (for AWS)
  - Pull containers from Dockerhub
- Source Code (github.internet2.edu/docker/grouper)
  - Build, and run in Docker Swarm
  - Includes all components to compose to a functional Grouper ecosystem:
    - Grouper Loader, Grouper UI, Grouper WS, Shibboleth IDP, Shibboleth SP, LDAP, MariaDB, RabbitMQ
- Standalone Container (dockerhub.com/tier/grouper)
  - Pushed to Dockerhub
  - Includes all Grouper subcomponents in container (UI, WS, Loader, SCIM)
  - Based on CMD flag in Dockerfile, can assume any role (chameleon)
Deployment Options

- Docker Swarm
  - Test-compose directory
  - Secrets
  - Compose
- Standalone container
  - FROM tier/grouper:latest
  - Layer in local configs
    - DB settings, sources, loader jobs, etc.
  - Build and push to a private Docker Repo
  - Run in AWS, Openshift, K8s
  - It’s what Internet2 is doing for Comanage environment (AWS ECS)
FROM tier/grouper:2.3.0-a103-u42-w12-p16

ENV CONFIG_BUCKET=s3://comanage-dev-host-configs/grouper.at.internet2.edu

RUN yum update -y &&
    yum -y install epel-release &&
    yum -y install awscli

RUN aws s3 cp $CONFIG_BUCKET/shib/sp-cert.pem /etc/shibboleth &&
    aws s3 cp $CONFIG_BUCKET/shib/sp-key.pem /etc/shibboleth &&
    aws s3 cp $CONFIG_BUCKET/shib/attribute-map.xml /etc/shibboleth &&
    aws s3 cp s3://comanage-dev-host-configs/general_metadata/login.at.internet2.edu-metadata.xml /etc/shibboleth

RUN aws s3 cp $CONFIG_BUCKET/grouper/grouper.hibernate.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/ldap.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/grouper.client.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/grouper.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/subject.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/sources.xml /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/log4j.properties /opt/grouper/conf/ &&
    aws s3 cp $CONFIG_BUCKET/grouper/grouper-loader.properties /opt/grouper/conf/

CMD ["ui"]
Change Management for Grouper Container?

• Branch (in Internet2 github) and Tag (in TIER Dockerhub) naming convention based on patch level of components
  - Should make change management of container easier and to avoid drift between dev and prod instead of pulling from :LATEST
  - E.g. 2.3.0-a104-u42-w12-p16, 2.3.0-a103-u42-w12-p16
  - 2.3.0 = Base version of Grouper
  - A = API patch version
  - U = UI patch version
  - W = Web Services patch version
  - P = PSPNG patch version
You don’t have to go to Stack Overflow to figure this out…
There are no stupid questions.....

Email Lists

- tier-packaging@internet2.edu
- tier-pack-grouper@internet2.edu
- grouper-study@internet2.edu

Slack Channels (internet2.slack.com)

- #tier-packaging
- #tier-grouper
- #tier-devops-discuss

Links

- github.internet2.edu/docker/grouper
- spaces.internet2.edu/display/TPD
Wednesday Showcases – 8:45AM Grand Ballroom

- Provisioning Architecture, and data flows
- Provisioning De-provisioning
  - midPoint as provisioning engine
  - Grouper as a group and privilege management system
  - Canvas as provisioning target (perhaps other apps if time)
- TIER Packaging - Overview of Containers and GitHub Repository
  - Shibboleth IdP
  - Grouper
  - COmanage
  - RabbitMQ
  - midPoint