What's new with SLATE?

Lincoln Bryant

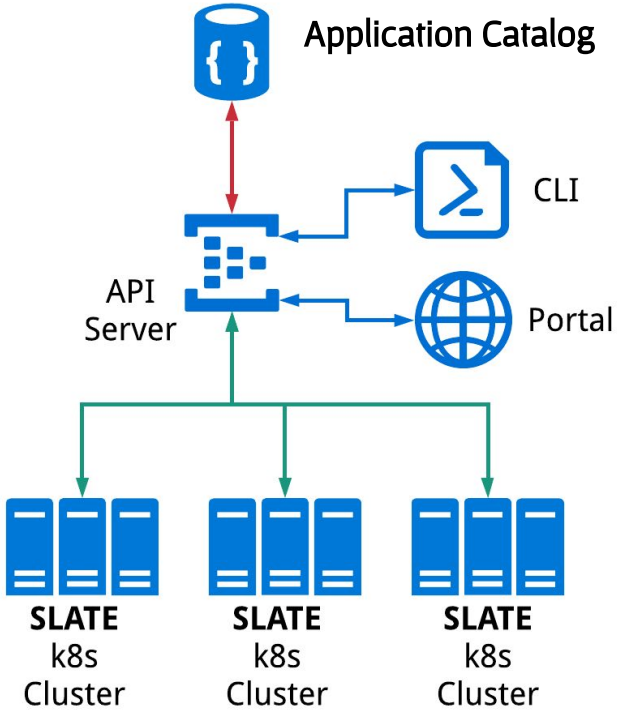
2nd IRIS-HEP K8S Meetup (Dec 1 - 2, 2020)

SLATE in a nutshell

- Services Layer At The Edge
- Platform for programmatically deploying applications to sites in a secure and easy-to-use way
  - SLATE implements a secure operations model to scope user privileges, i.e. **Federated Operations** (c.f. CHEP2019 article)
- Three fundamental pieces:
  - Centralized service to manage users, groups, clusters, and authorization thereof
  - REST API with a fully supported web portal and commandline client
  - Curated catalog of applications, a la 'the App Store'

SLATE Architecture

- Lightweight federation and application catalog layer on top of Kubernetes
  - Security-conscious, site autonomous
  - Sites retain administrative control
- Single entrypoint using institutional identity
- Simple UNIX-like permissions model (Users + Groups)
- Application catalog abstracts away much of the Kubernetes details, let's users think about the important parts of their deployment



Applications

Why build a curated catalog?

Docker Hub is a good place to publicly put images, but its security is sketchy!

- Does not enforce Dockerfile sources with images
- Release tags are not immutable
- Images themselves are static, do not get updated with security patches

This is to say nothing of poorly crafted K8S YAMLs

Docker | dä-kər
A tool for running untrusted code from random people on the internet as root!

DevOps to DevOops: Docker Hub proves so secure that 430 Docker images out of 2,500 have no vulnerabilities

As for the rest, you're on your own

Thomas Claburn in San Francisco Mon 15 Jun 2020 // 10:45 UTC SHARE

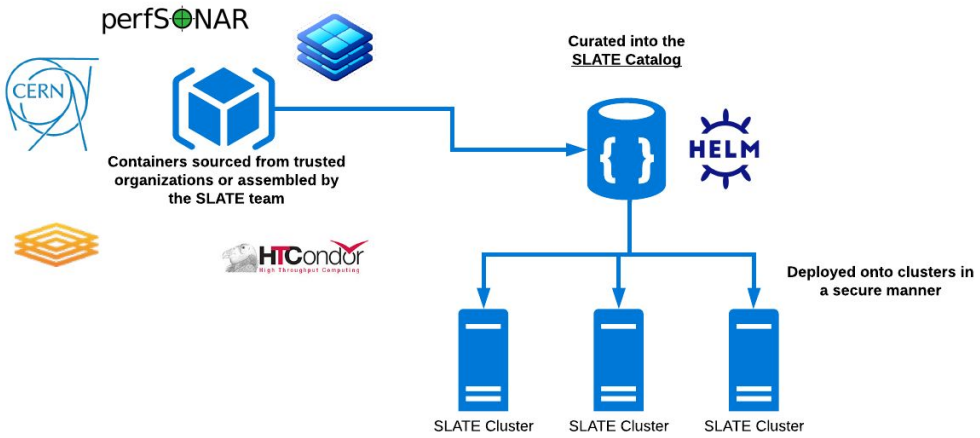
Back in 2015, security biz BanyanOps found that about 40 per cent of Docker images distributed through Docker Hub had high-priority vulnerabilities. That was when the Docker Hub repository stored about 95,000 Docker images.

// MOST READ

AWS reveals it broke itself by exceeding OS thread limits, sysadmins weren't familiar with some

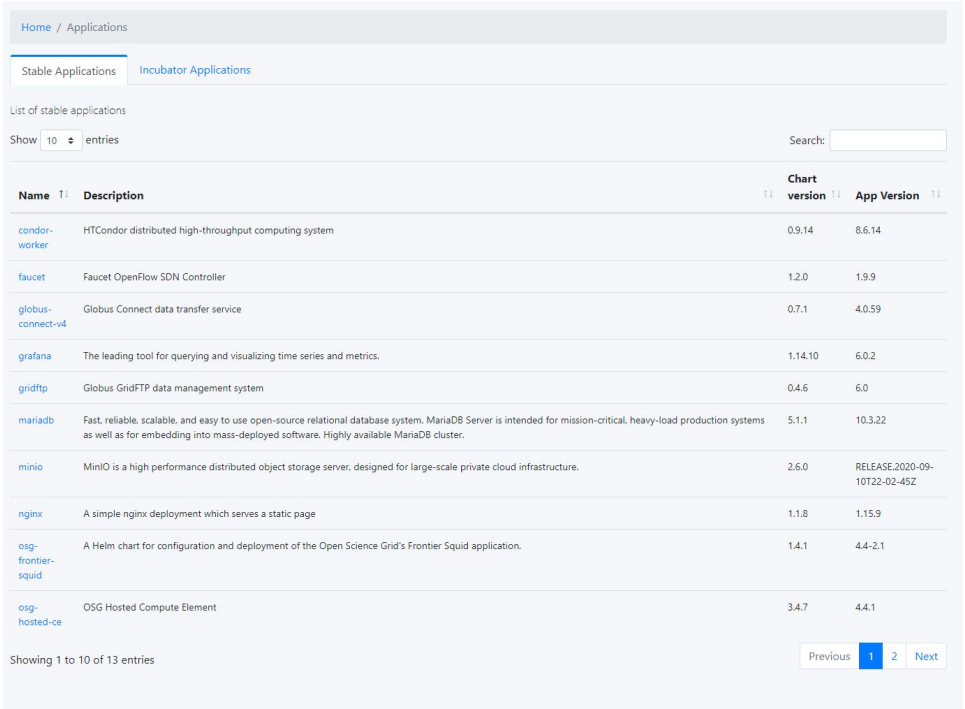
SLATE Catalog

- The SLATE Catalog is centrally managed to ensure quality and cut back on the 'wild west' of Docker containers
- Helm Charts in the SLATE Catalog refer to container images in trusted repositories, such as those operated by SLATE, OSG, CERN, etc.



Catalog Updates

- Helm 3 across the board
- Applications in the catalog should now generally support network policies
- Actively working on:
  - **Open OnDemand w/ KeyCloak**
  - **CMS XCache**
  - **HTCondor Submit, Central Manager, Worker updates**
- Software that has been stabilized and in production since Jan:
  - **MinIO**
  - **OSG Hosted CE**
  - **Jupyter**
  - **MariaDB**



Opportunities for Collaboration

- All SLATE applications are vanilla Helm applications
- Can be used outside of SLATE:
  - `helm repo add slate` https://jenkins.slateci.io/catalog/stable/
- We want to collaborate with you!
  - I think we have an opportunity as a community to build
    - **a catalog of Kubernetes / Helm applications**
    - **a registry of containers that are trusted by the community, regularly updated, fully sourced**

Updates since the last meeting

New SLATE Clusters in 2020

- New SLATE Clusters registered:
  - Great Plains Network
  - Georgia Tech
  - New Mexico State University
  - University of Wisconsin-Madison
  - South Pole Telescope (at the south pole!)
  - Institute of Physics (FZU) in the Czech Republic
  - Texas Advanced Computing Center at the University of Texas at Austin
  - University of Texas - Arlington
  - Boston University

Georgia Institute of Technology

GPN GREAT PLAINS NETWORK

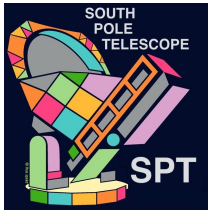
NM STATE

FZU Institute of Physics of the Czech Academy of Sciences

WISCONSIN UNIVERSITY OF WISCONSIN-MADISON

TACC TEXAS ADVANCED COMPUTING CENTER

BOSTON UNIVERSITY



UNIVERSITY OF TEXAS ARLINGTON

New SLATE Feature - Volumes

- SLATE now supports Kubernetes Volumes as first class objects
  - (scheduled for production roll out on Wednesday, December 9)

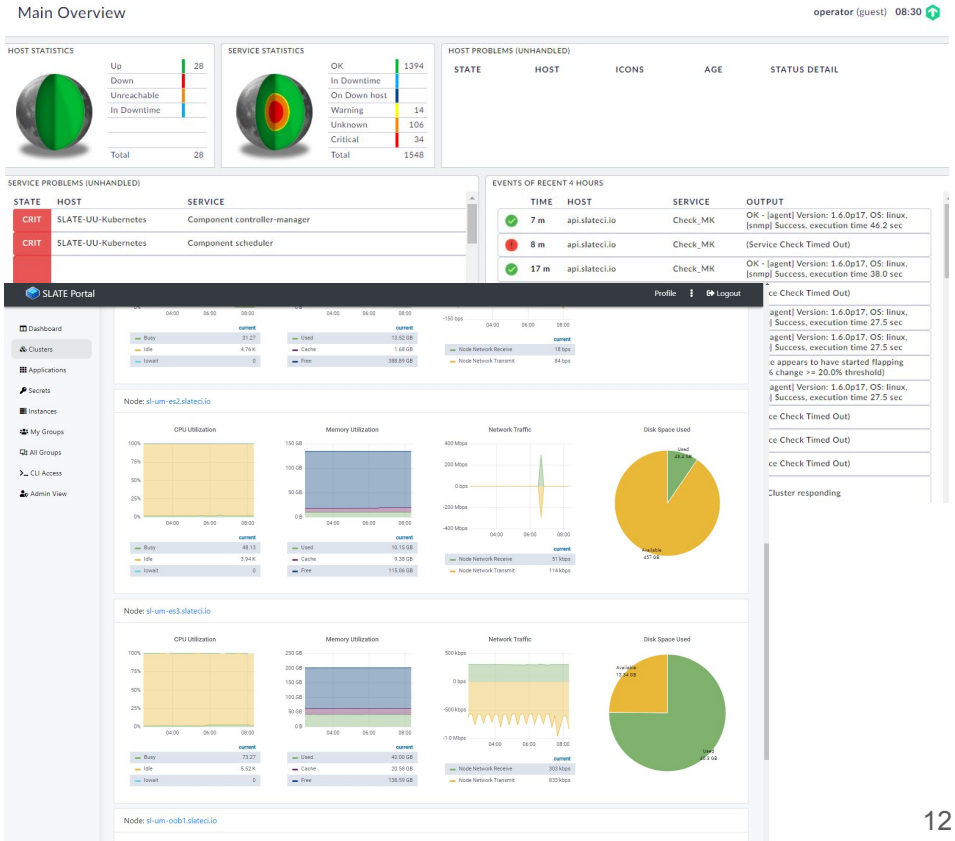
```
[muhammad@utah-dev1 ~]$ slate volume create htcondor-logs --group slate-dev --cluster utah-dev --size 10G --storageClass local-path
...
Creating volume...
...
...
...
Successfully created volume htcondor-logs with ID volume_FPOhgu3Chjg
[muhammad@utah-dev1 ~]$ slate volume info volume_FPOhgu3Chjg
Name          Created                          Group     Cluster  ID
htcondor-logs 2020-Dec-01 21:11:33.858843 UTC slate-dev utah-dev volume_FPOhgu3Chjg

Details:
Storage Request Access Mode   Volume Mode Storage Class
10G             ReadWriteOnce Filesystem  local-path

Status:
Status
Pending
```

New SLATE Feature - Monitoring

- Cluster operators can now opt-in to have SLATE collect metrics and forward it to the central dashboard
- Also actively working on our alerting capabilities with check_mk



Federated Operations Updates

- One of the broad goals of the SLATE project is to proliferate technology and policies behind the idea of **Federated Operations**
- In US ATLAS we are using SLATE to deploy & operate a collection of XCaches at a number of **LHC Tier2 centers** used to develop caching model for PanDA and Rucio ("Virtual Placement")
  - MWT2 (Chicago), ALGT2 (Michigan), Boston, SWT2 (UTA), Prague, LRZ (Munich)
  - Operated by one person (Ilija Vukotic) who frequently updates the software and monitoring
- Leverages SLATE's privilege model implementation that guarantees:
  - **Only** specific users can deploy **specific, curated applications** (e.g. those passing **OSG SecOps**)
  - All under control of the cluster administrator who can revoke access at any time
  - The application administrator obviously can also be an employee of the same organization as the cluster administrator (therefore requiring no "special" privileges)
- To express these principles the SLATE team (with the help of cybersecurity experts) over the past year has formalized a set of **security policies**
- This work can be generalized to help inform WLCG (SCv2) sec. policies for fedops

Final Thoughts

Other musings, thoughts for discussion

- We want to align with the security work that others are doing.
- Foresee SLATE requiring all Charts to have:
  - Pod Security Policies
  - Ingress/Egress rules
  - Denying Rootly containers
- Seems essential for SLATE to work seamlessly with products like OpenShift.
  - We've done a lot of work to make SLATE work with Kubeadm, K3S, Singularity CRI.
  - I would personally like to consider a highly opinionated K8S distribution for SLATE clusters.

Summary

- SLATE community growing, several new sites added this year.
  - Use cases have primarily been XCaches, OSG CEs, Globus..
  - Growing interest in things like Jupyter, HTCondor (workers + submit)
- Strong relationship with our friends in OSG who have contributed many contributions to the catalog, feature requests, patches, etc.
- Want to more closely collaborate with others:
  - to develop and support the Federated Operations model
  - to build trustworthy and reliable packages for Kubernetes applications in our community