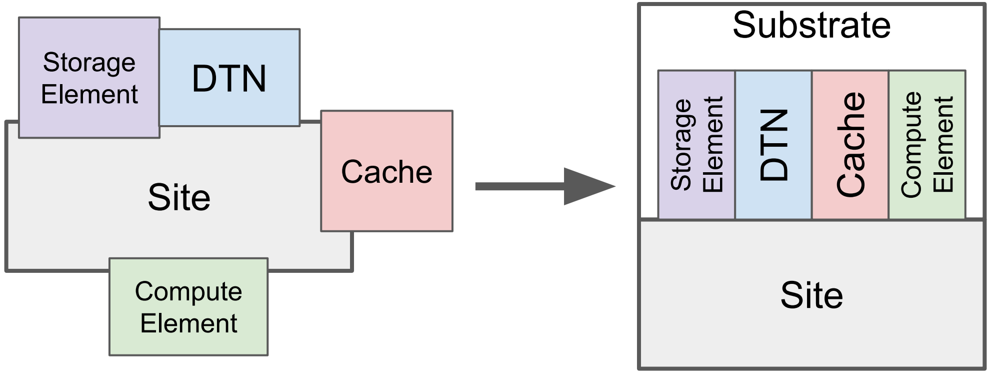
Applying SCI to SLATE

Chris Weaver for the SLATE Team

WISE Meeting
April 21, 2020

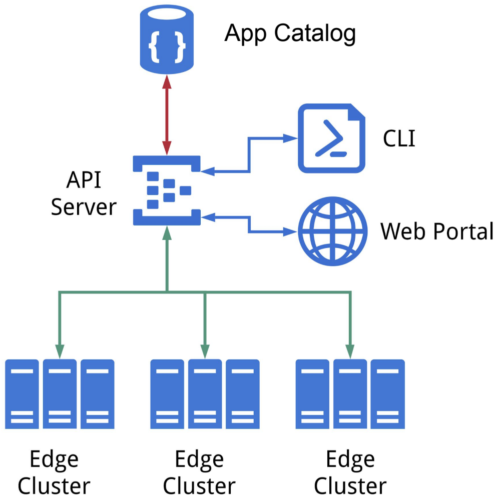
Purpose of SLATE

- Many distributed infrastructures find it difficult to roll out and maintain new services
- By adding a **consistent edge substrate** that is common to sites and modular service components which use it, labor can be reduced
- Offers possibility federated operation
  - or a mix of local and federated



The SLATE Platform for Edge Services

- SLATE (Services Layer at the Edge) provides a substrate for this type of infrastructure
- Docker, Kubernetes, and Helm are used to package and deploy service applications
- A central server component is used to mediate user requests being sent to participating edge Kubernetes clusters
- Command line and web interfaces are provided



slateci.io

Roles in the SLATE Federation

- Platform Administrator
  - Operates the central parts of the federation
- Edge (Cluster) Administrator
  - Runs a cluster which participates in the federation
- Application Administrator
  - Runs one or more services on one or more participating clusters
- Application Developer
  - Maintains an application used on the platform
- Application Reviewer
  - Checks applications for consistency with policy, quality standards

Expectations Between Roles:

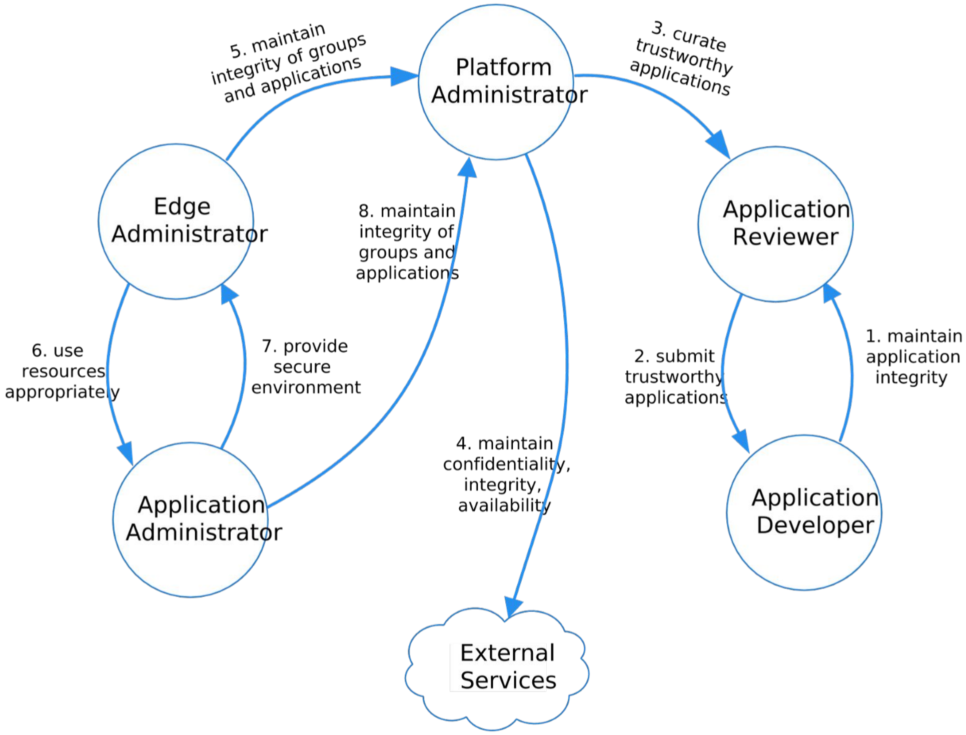

Platform Administrator
Edge Administrator
Application Reviewer
Application Administrator
Application Developer
External Services
1. maintain application integrity
2. submit trustworthy applications
3. curate trustworthy applications
4. maintain confidentiality, integrity, availability
5. maintain integrity of groups and applications
6. use resources appropriately
7. provide secure environment
8. maintain integrity of groups and applications

Diagram courtesy of Kay Avila

Plans

- To be useful, SLATE needs to be trusted by several cyberinfrastructure/e-infrastructure groups, such as the WLCG, OSG, ATLAS and CMS
- Adopting a set of policies which conform to a widely understood standard, like SCI seems like a good step in building that trust

Initial feedback on SCIv2

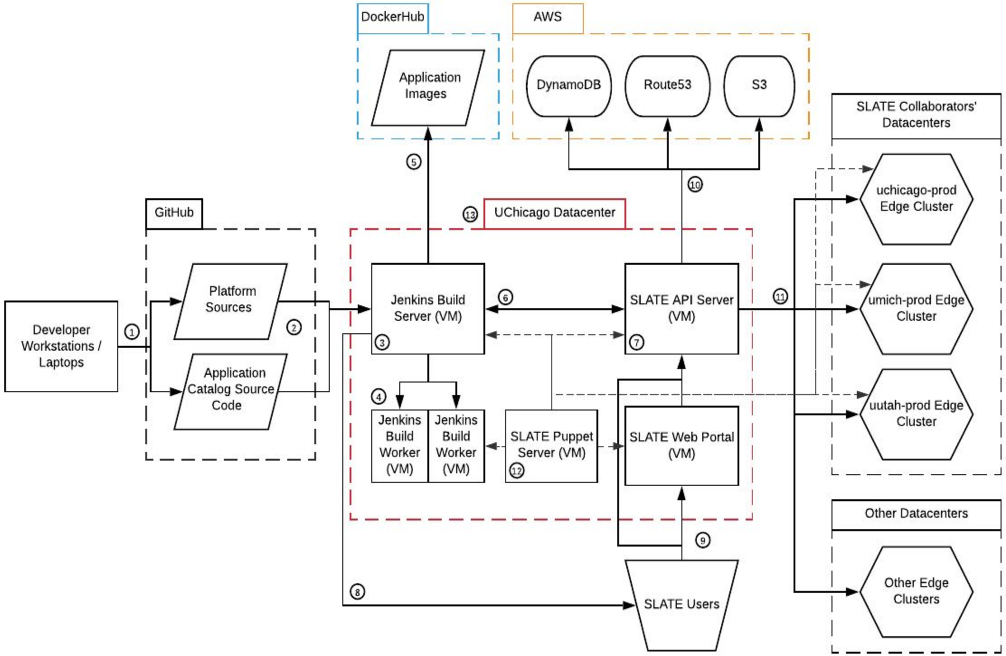
- Broadly, everything makes sense and most aspects seem to be covered
- Good starting point to be responsive to supporting infrastructures' (sites') policies
- Some aspects of SLATE's federated operations model are not entirely addressed by SCI v2:
    - Application development, review, and containerization ([OS10] is meager)
    - Shared responsibility across the federated operation for things like vulnerability management, IDS, traceability, incident response
- In order to make the SLATE platform a secure, coherent whole across the multiple participating organizations, possibilities:
    - Role-specific agreements to be followed by role occupants
    - SCI include a new specification that to apply to a federated system, each organization participating in the federation must agree to implement the SCI framework (kinda like Sirtfi)

Questions?

Thanks!

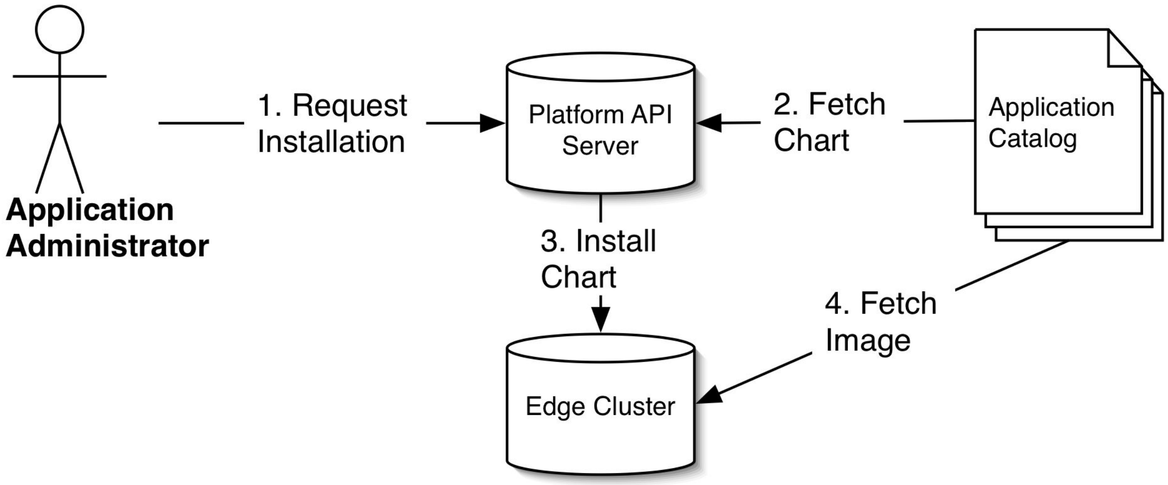
extra slides follow

Further Information about SLATE



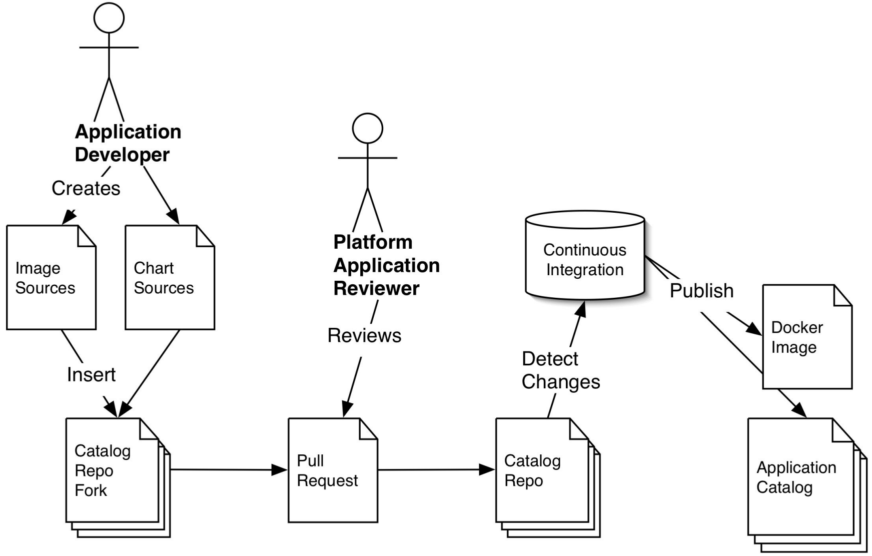
- Design of the SLATE platform, and security considerations:
  - https://drive.google.com/file/d/1eJR4vqo9wfT45bM3ENlwt6xfKPrq1_Ei/view?usp=sharing
- Previous paper on security ideas:
  - https://drive.google.com/file/d/10ASE-be8XTzw5J4qGnTpK50L4BJLJBFc/view?usp=sharing

Application Install Process



- The SLATE API server mediates requests to install applications
  - Fetches applications only from the curated catalog
  - Enforces rules set by the administrators of the target cluster

Application Curation



- Much of the value of the centralized application catalog derives from the overesight applied to the applications added to it
- Some amount of human attention is required, but maximizing automation is highly desirable