WLCG Federated Operations Security Survey

Rob Gardner
University of Chicago

Romain Wartel
CERN

GDB
March 11, 2020

Federated Operations Security Survey

WLCG Federated Operations Security Working Group survey - 60 responses thru Feb 10

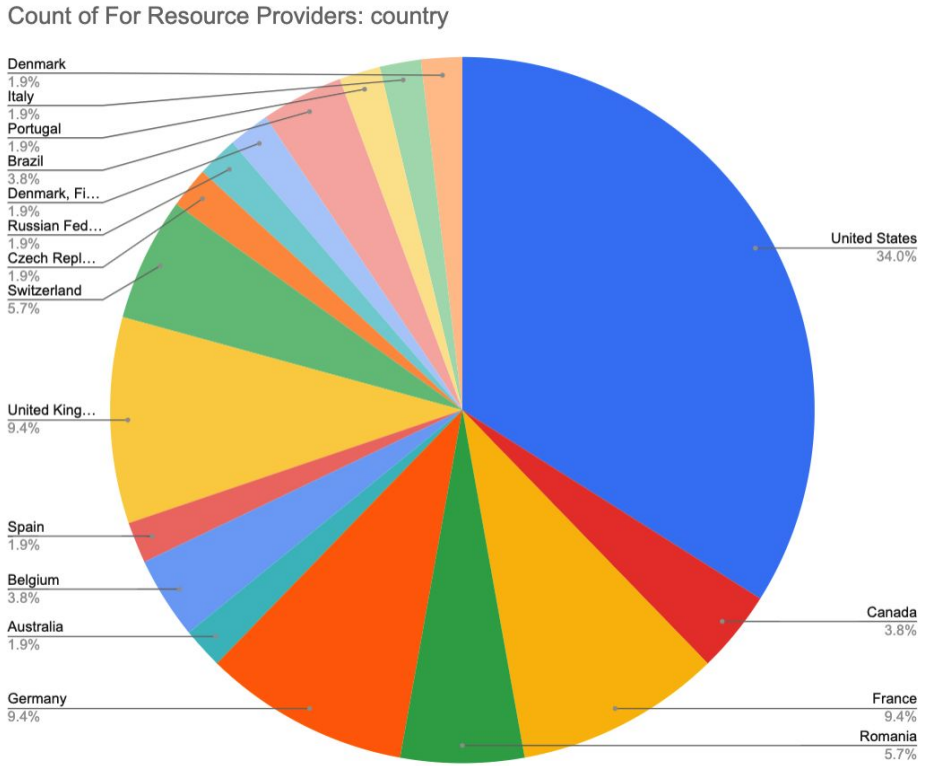
Section 1 of 3

Trust, Security & Federated Operation Models

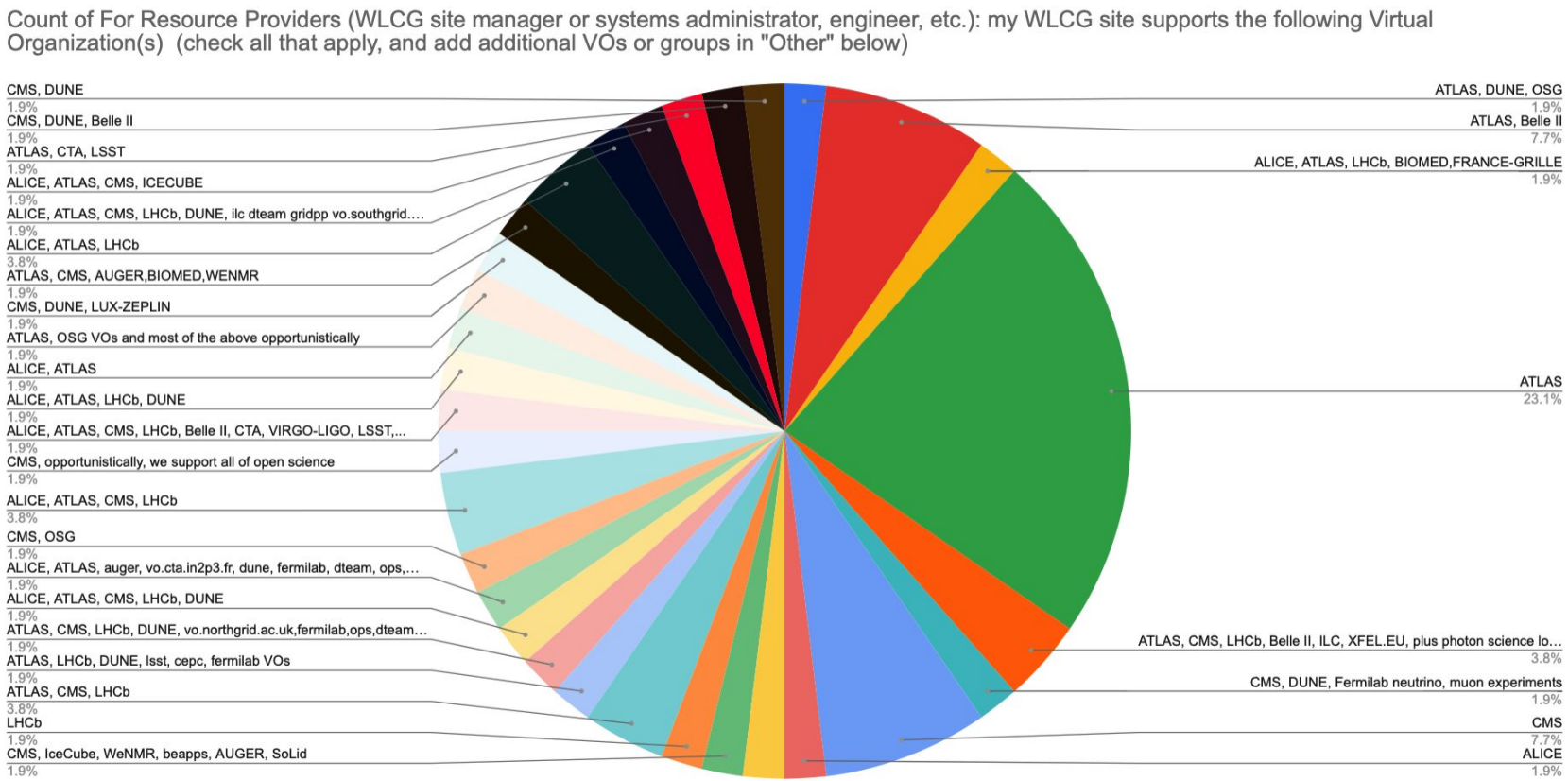
The purpose of this survey is to collect perspectives on trust & security from the community regarding federated operation of services across WLCG sites by trusted third parties. The input collected here will inform the activity of the WLCG Federation Operations Security working group (https://twiki.cern.ch/twiki/bin/view/LCG/WLCGFederatedOperationsSecurityWG).

The primary goal of the Working Group is to develop a trust model for centralized service orchestration across WLCG centers, an approach being explored by the SLATE project (http://slateci.io) and others. The aim is improving the operational efficiency of WLCG computing services, promote innovation of new computing platforms in support of HL-LHC software development, whilst maintaining a similar level of trust and operational security capabilities across the infrastructure.

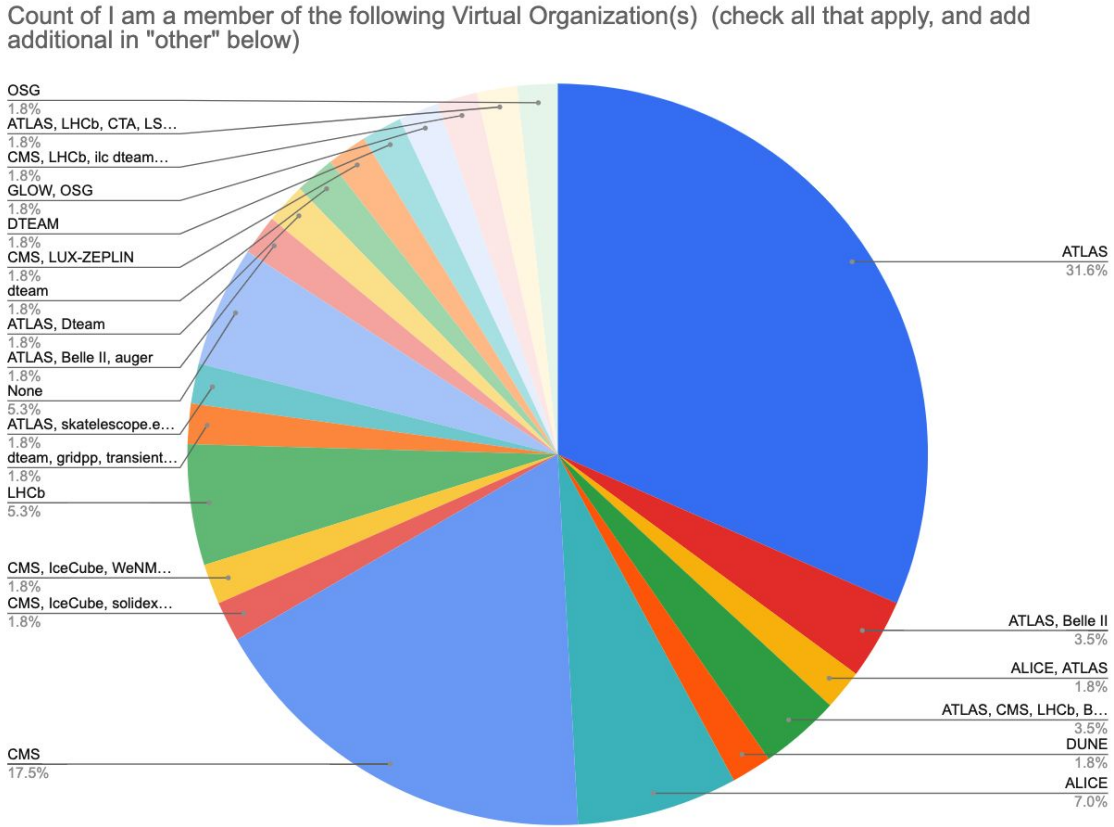
In practice, federated operations involve:
- Reviewing images and containers provided by collaborating research infrastructures (e.g. compute element software)
- Establishing a security baseline and ensuring compliance with security policies (e.g. traceability)
- Deploying and operating service infrastructure centrally



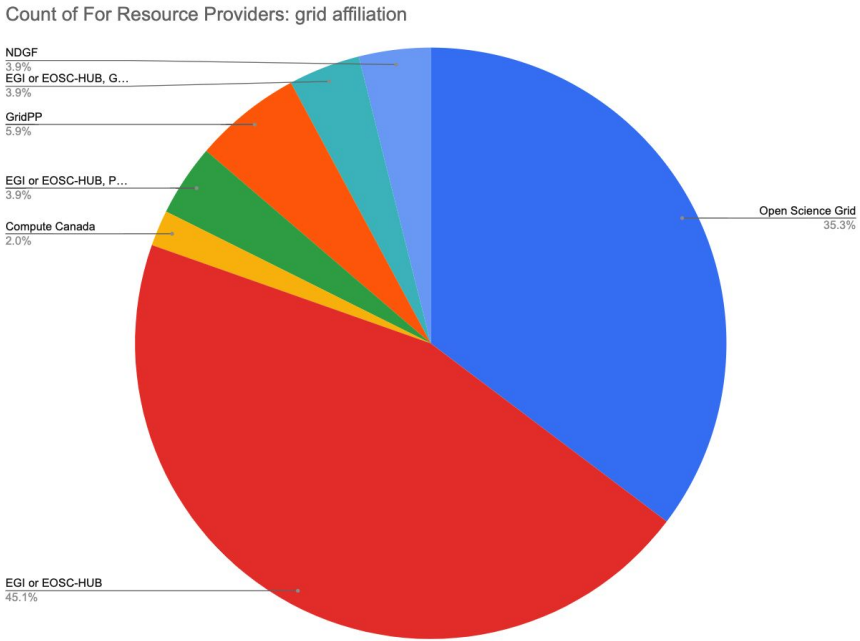
VOs supported by Resource Providers

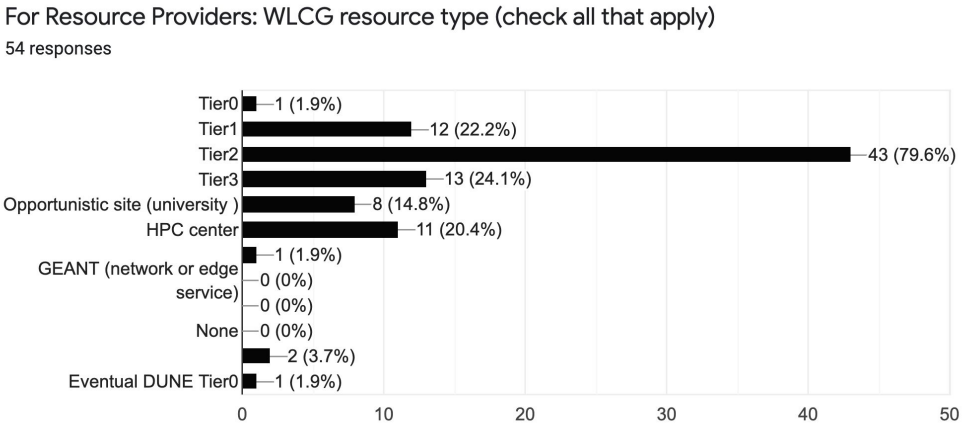


Response from Experiments

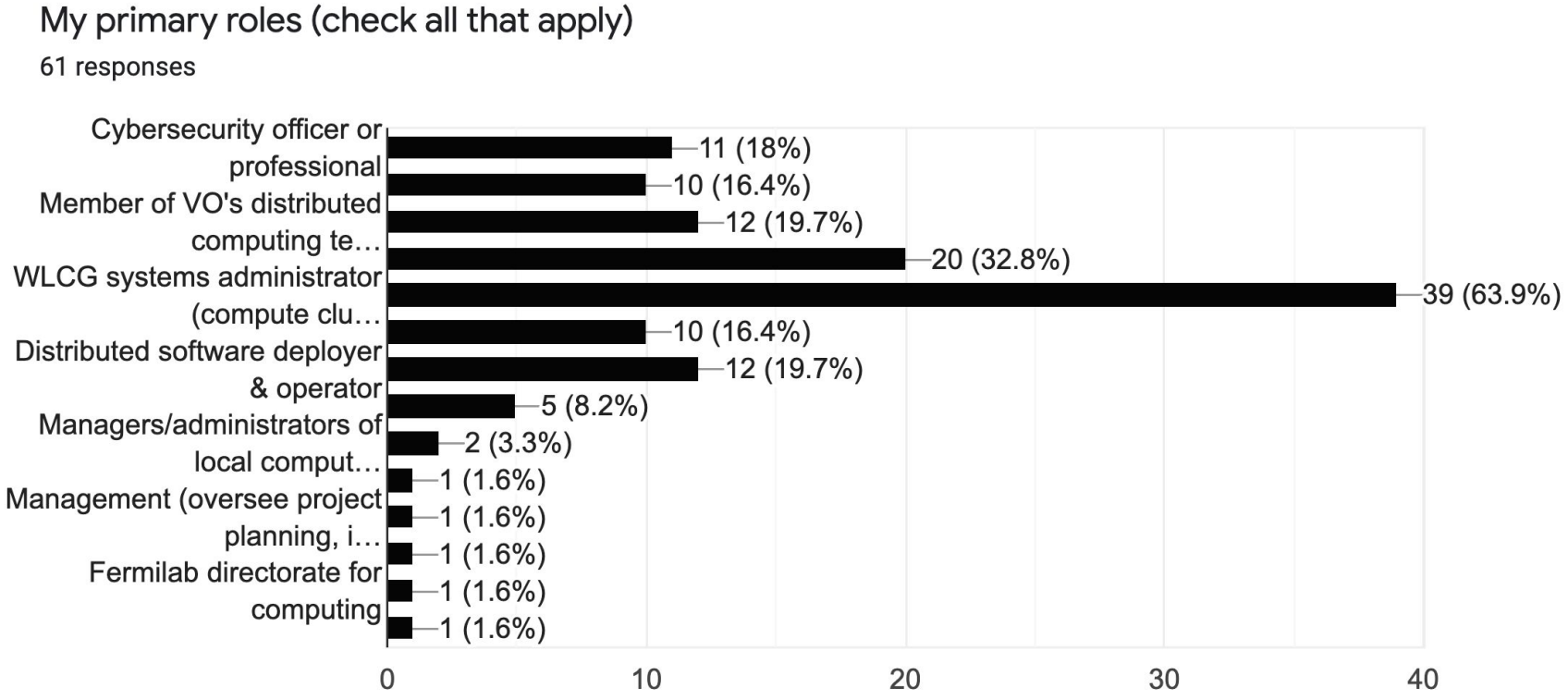


by Grid & Provider Type





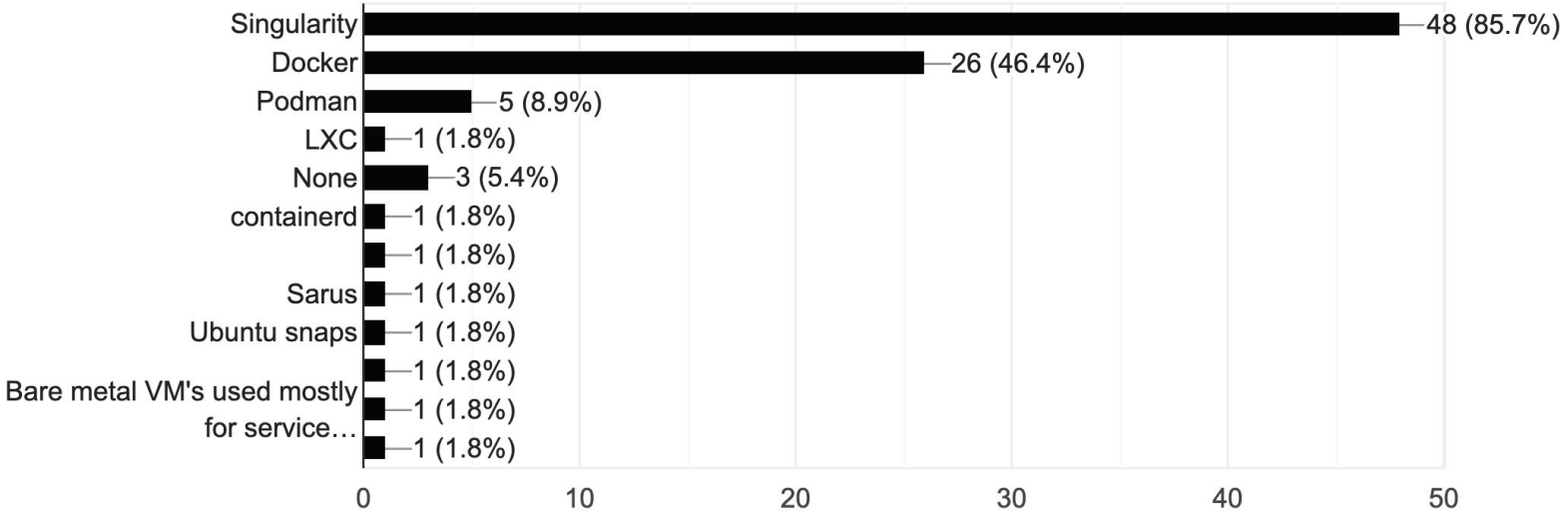
Roles of Respondents



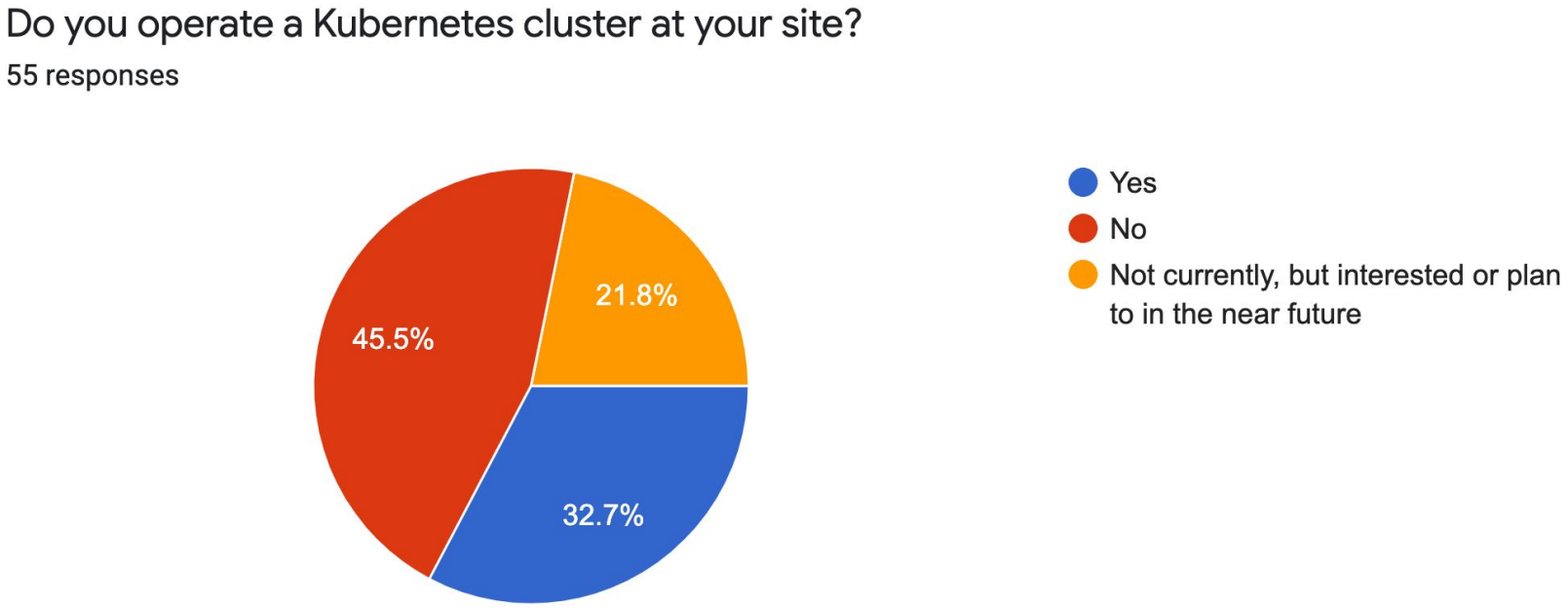
Use of Containers

Are you currently using, or planning to use, any of the following Linux containerization technologies at your site? Especially from a services perspective.

56 responses



Kubernetes Use



Summary of Comments

Primary security concerns

Traceability	21
Trust	20
Delegation	3
Roles & responsibilities	10
Access control	14
Security operational	7
All	6

Other particulars mentioned by respondents:

- Many are concerned about privileged access by people external to their organization.
- GDPR concerns
- Open communication, transparency

From Resource Providers

What are your operational challenges?

- Software/middleware updates/patching
- Software trends – knowing that some existing thing should be replaced with something newer/better
- Diversity – lots of different technologies to manage, no common way to manage them
- Keeping distributed instances in sync
- Dealing with old hardware
- User support
- User authentication
- Achieving/maintaining expertise in everything needed, especially when facing reductions in staffing levels
- Debugging issues with remote networks
- Unneeded heterogeneity of ATLAS sites
- Lack of transparency into operations – users know before we do that something's wrong
- Data flow management/storage capacity
- Not enough staff

Security benefits from Fed Ops?

Yes	36
No	10
Dunno/maybe	10

Can federated operations help?

Yes	33
No	9
Dunno/maybe	9

What security/policy requirements for a fed ops model?

- Site must specifically **delegate clearly delimited access** to fed ops
- Formal standing – perhaps somehow bestowed by WLCG
- Strong authentication for fed ops staff
- Fed ops only connect to non-production stuff, **cordoned off**
- Compliance with GDPR and **local policies**
- Known, trusted fed ops
- **Containers well vetted and secure**
- Well-designed operational and security model
  - Signed or attested in some formal fashion
- Transparency/open communication
- Exception to current local policy
- **Fed operator must demonstrate they can do a better job than site**
- Fed operator **must demonstrate reliability/sustainability**
- **Accountability/liability** accepted by Fed ops
- Depends on nature of federated service
- Some level of local control over fed ops
- Assurance that fed managed operation **won't negatively impact other stuff**
- Already partially addressed by EGI CSIRT agreement
- Others try it first – then maybe we'll follow

More ideas/comments from respondents

- Make trusted, vetted, containers available for sites to choose to download and install
  - This enables a focus of expertise/skills without adding operational integration to the picture
- Federated operations makes things even more complicated – hurts rather than helps
- Fed ops would contribute to uniformity, harmonization, across HEP HPC facilities
- Fed ops reduces risk of specialized skills leaving the site when one person moves on
- Fed ops provides a benefit similar to automation: less manual time, greater standardization, likelier to be well tested hence more reliable
- One respondent is already part of a centrally operated federated service

Other comments

- Fed ops blur lines of responsibility
- Possible learnings from federated cloud infrastructure policies
- Concern with net effect of shifting operational responsibility to people with less professional experience
- Maintain local control over fed operation
- Hard to see how some services, like file caching, can work in a federated model (one size doesn't fit all?)
- Possible reduction of overall staffing needs – good
- Adding k8s capacity across WLCG sites doesn't benefit WLCG – no need for dynamic scaling at WLCG sites
- It's harder to address security and trust when more than one organization is involved
- Another ill-conceived US-driven project, like "FAX". End it now.
- Sites have a variety of different operational models, hard to see how fed ops can simplify.
- Need to understand specifics of the federated model
- Easily deployable reference containers is valuable, less so the operational aspect

Summary Thoughts from Tom (and Chris)

- We may not have clearly articulated type and amount of local access is proposed in the federated operations model. This is hard to define generally; it may differ between SLATE and other federated platforms.
- Perhaps it would be useful to distinguish a person external to a site having privileged access from an external process which does so at the direction of an internal person.
- Small sites seem to have more interest in a new model; the threat of staff turnover leaving them short-handed seems highly relevant
- There seems to be stronger consensus for the usefulness of maintaining a curated set of containerized services. Giving sites a way to update these automatically, run purely internally, might be a useful step forward.

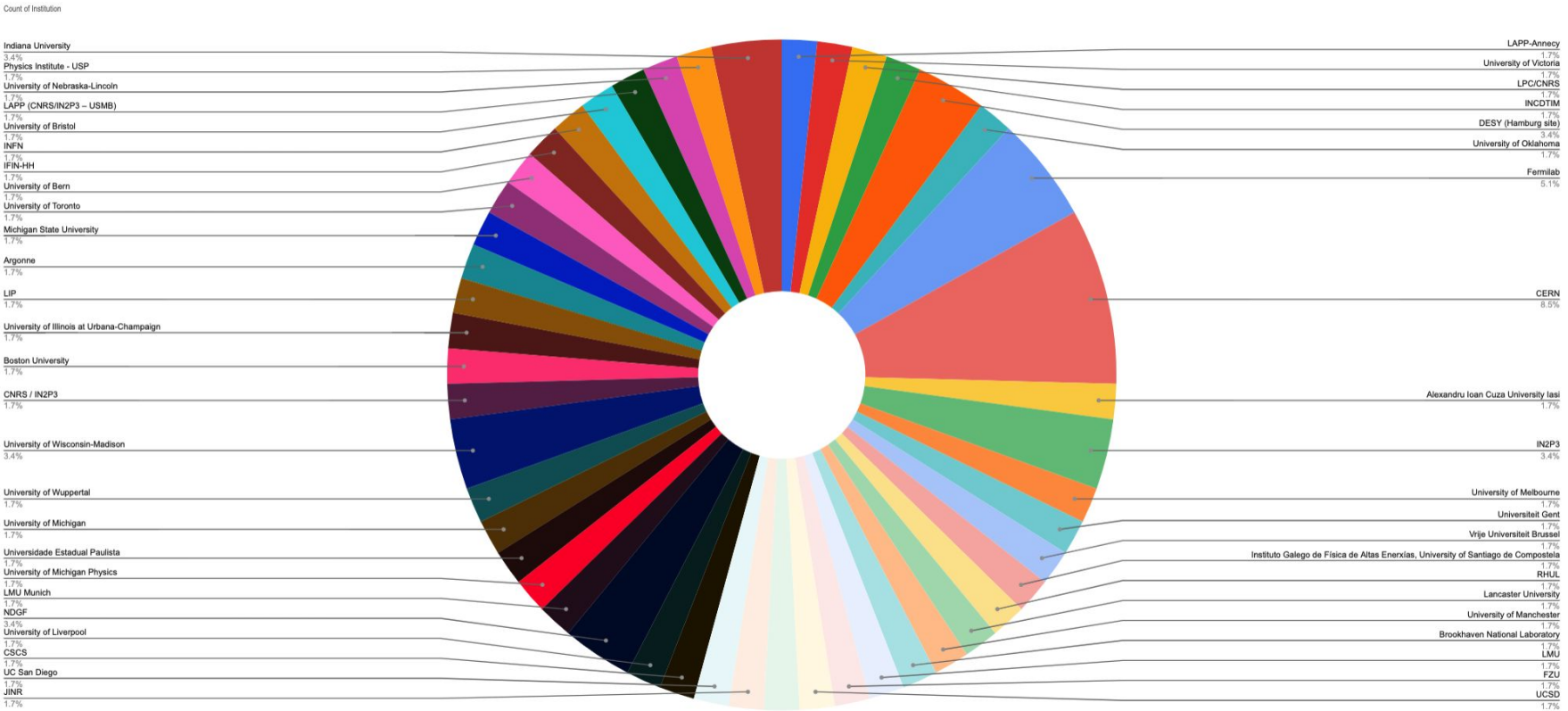
Full responses here. Summary report in preparation (n.b. WG twiki here)

Thanks to participants

& to Chris Weaver & Tom Barton for help with survey design and summary

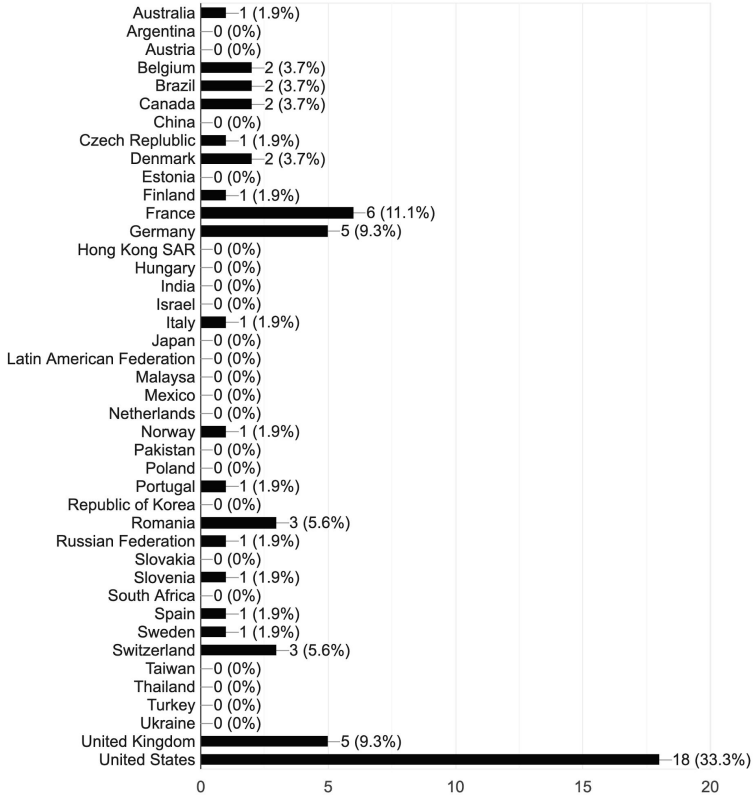
More Charts

institutions responding



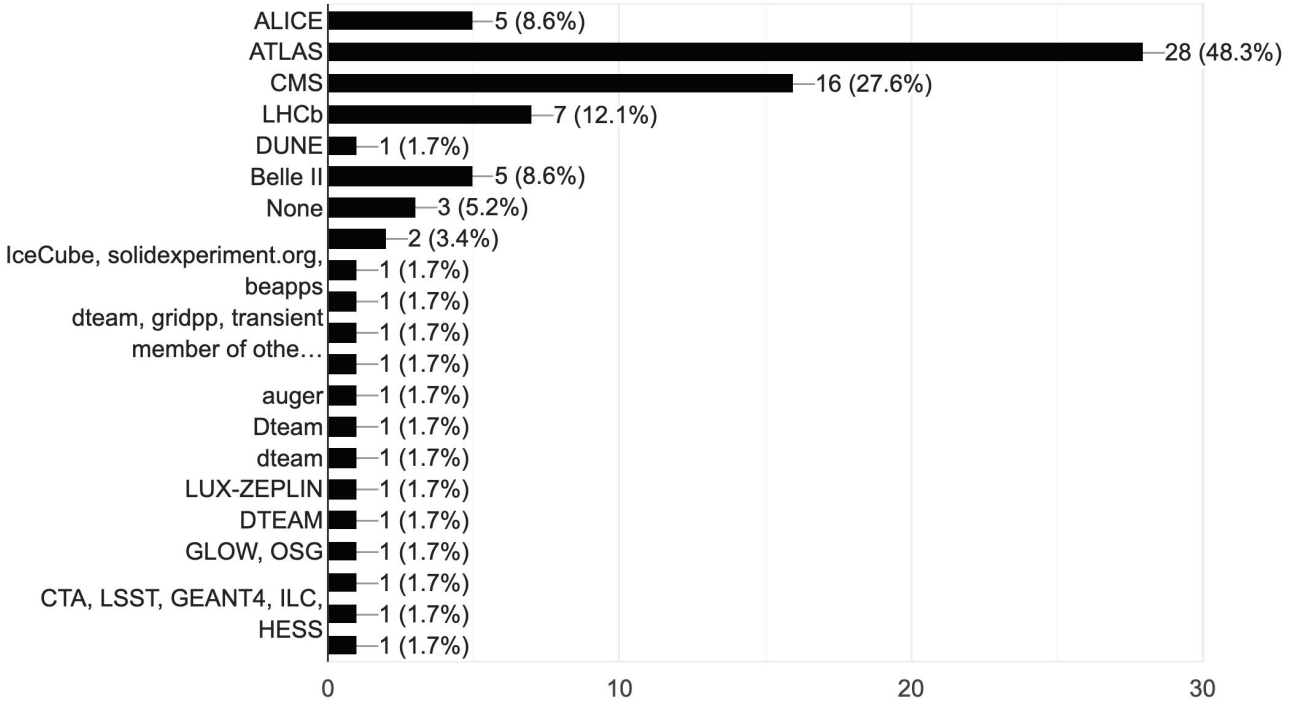
For Resource Providers: country

54 responses



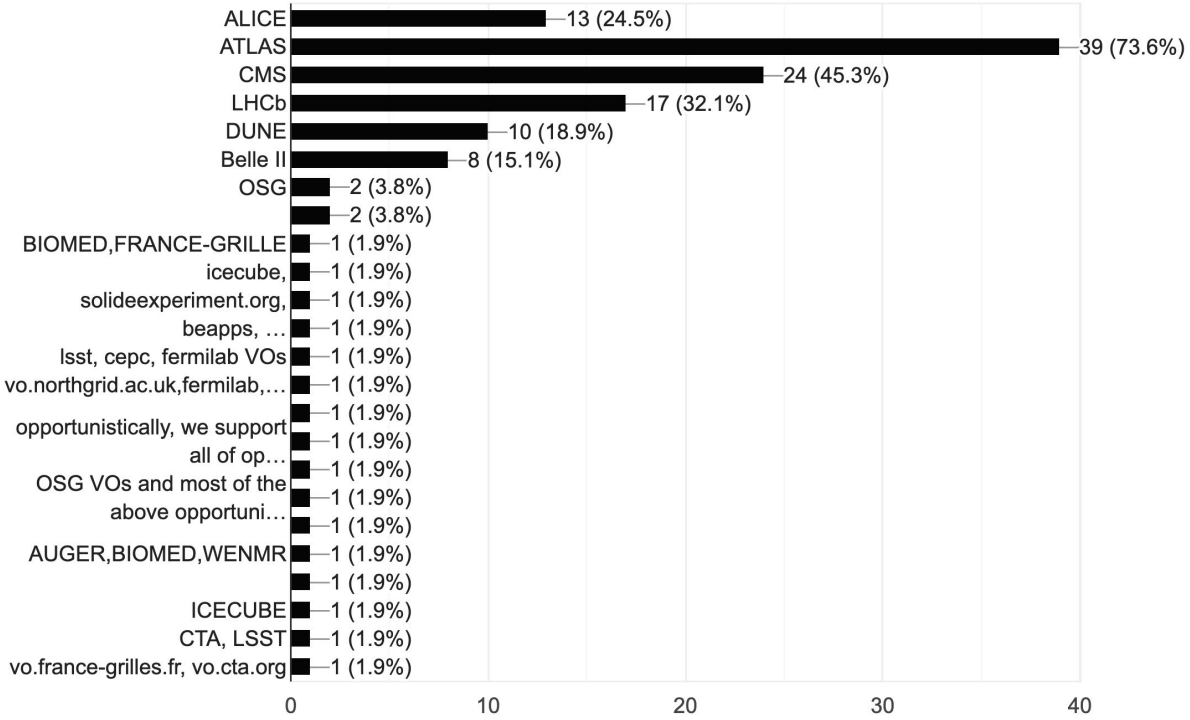
I am a member of the following Virtual Organization(s) (check all that apply, and add additional in "other" below)

58 responses



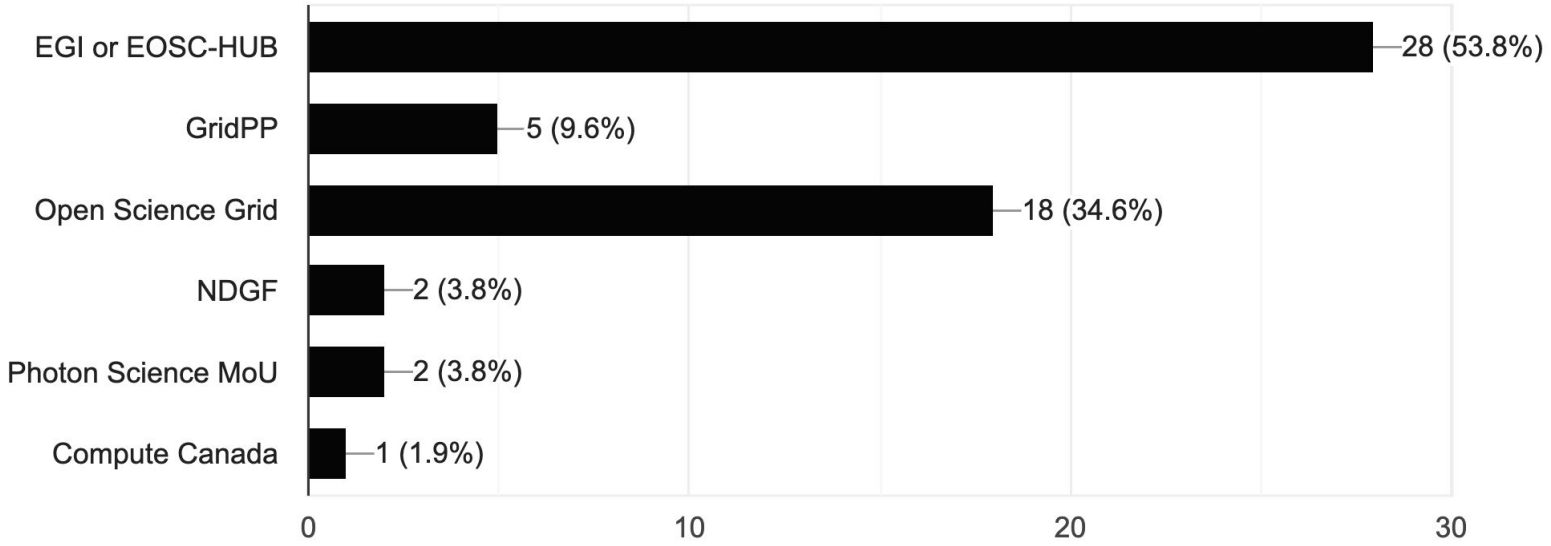
For Resource Providers (WLCG site manager or systems administrator, engineer, etc.): my WLCG site supports the following Virtual Organization(s...and add additional VOs or groups in "Other" below)

53 responses

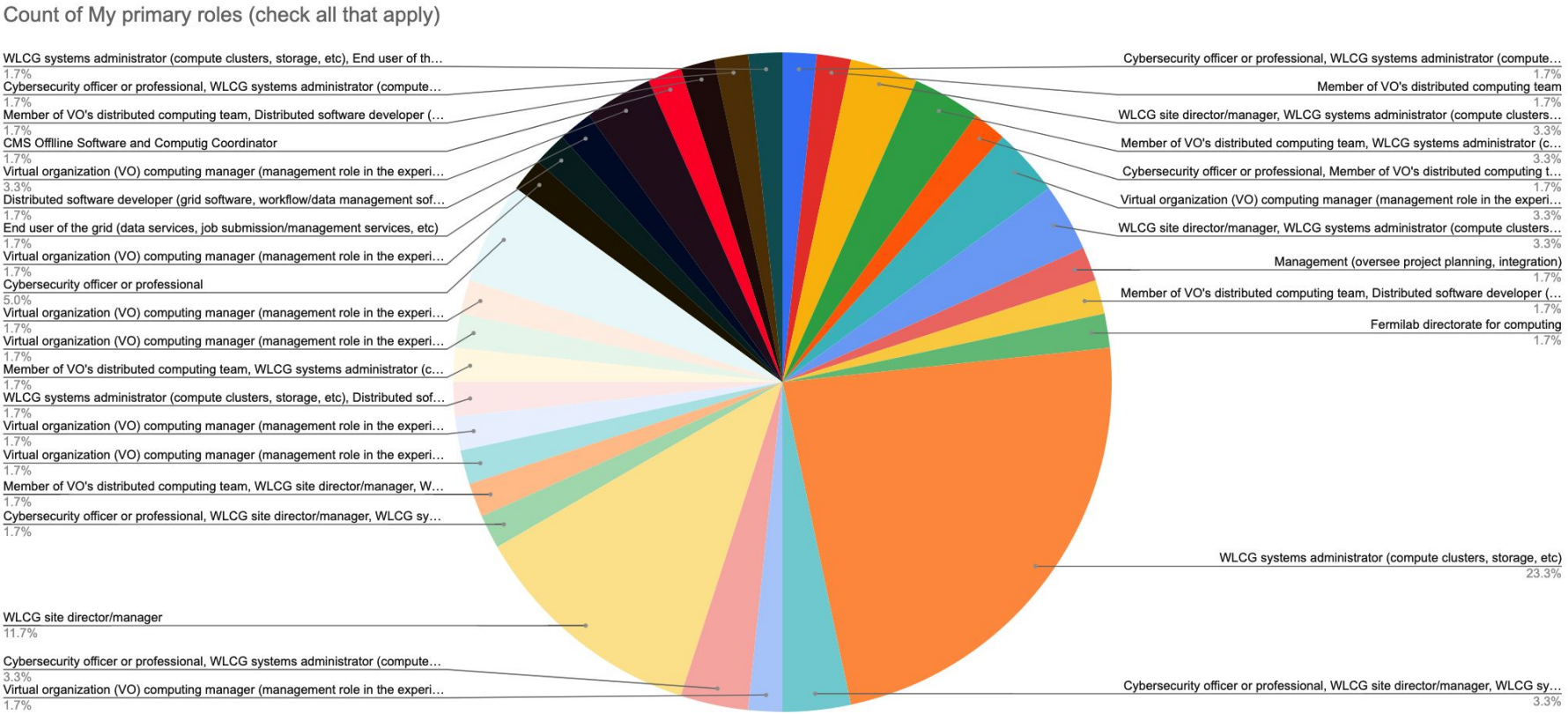


For Resource Providers: grid affiliation

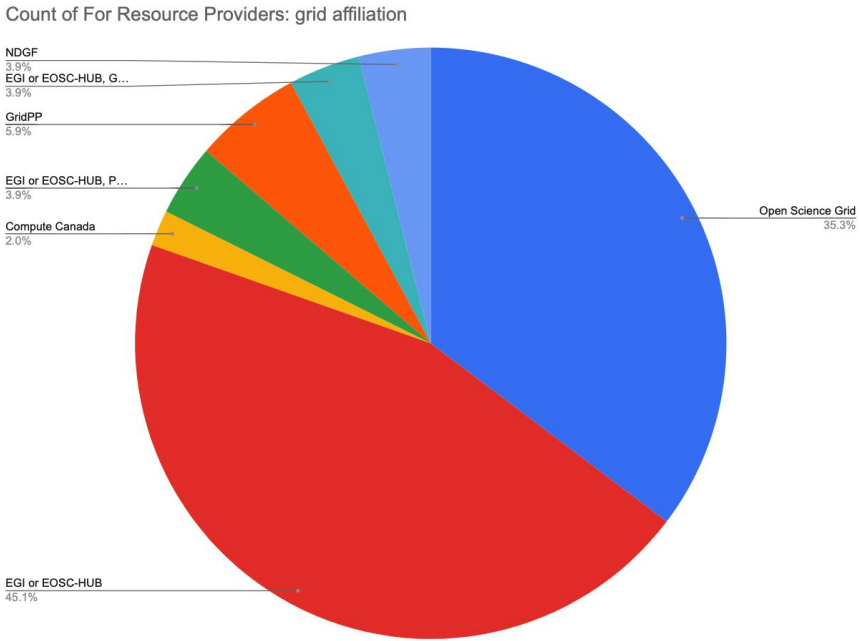
52 responses

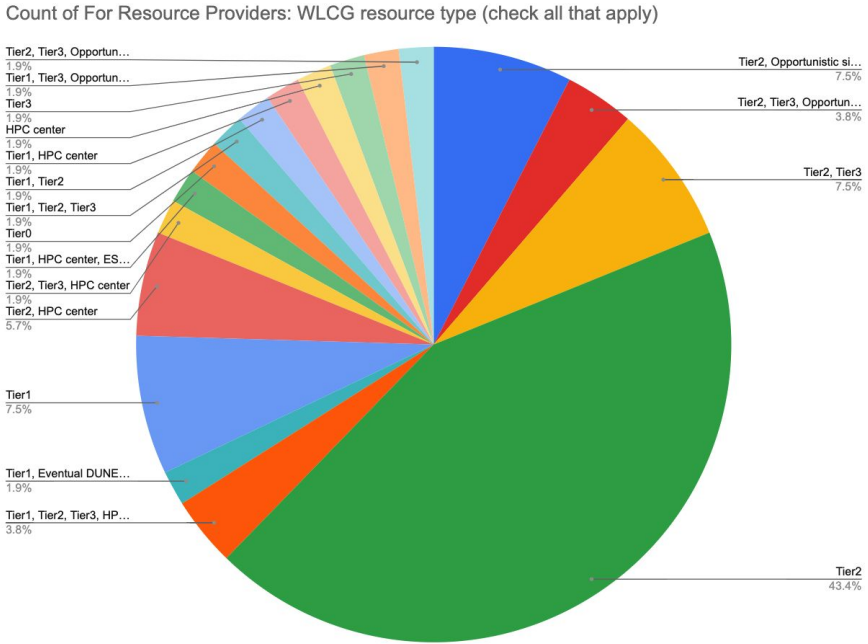


roles of respondents



by Grid & Provider Type





Sites responding