Gen3 CSOC WG Meeting

February 26, 2025

The Agenda

- Problem statement
- CSOC Vision
- Collaboration Opportunities
- IaC as a Plugin
- System Architecture
- Additional Roadmap items (if time permits)

Problem Statement

Need: Organizations require the ability to deploy multiple **enterprise-grade Gen3 environments** on their preferred cloud providers.

Challenge: Managing Gen3 infrastructure demands **specialized cloud-native expertise**, creating a barrier for teams without deep cloud knowledge. CTDS also doesn’t have deep expertise in all clouds.

Impact:

- Slower deployment timelines
- Increased operational complexity & costs
- Limited scalability across cloud providers
- Barrier to wide-scale use of Gen3

Solution Opportunity: A **streamlined, scalable approach** to Gen3 deployment, reducing technical friction and enabling seamless cloud management that leverages community contributions.

CSOC Vision: A Unified Gen3 Management Portal

One Portal for End-to-End Gen3 Lifecycle Management

- Seamlessly deploy, configure, and manage **multiple** Gen3 instances.
- Enable **zero to production** Gen3 deployments effortlessly.

Multi-Cloud Infrastructure Provisioning

- Support **Kubernetes** deployments across multiple cloud providers.
- Simplify cloud infrastructure setup and maintenance.

Community-Driven

- Incorporate **IaC contributions** from AU Biocommons, Krumware, OCC and other community partners.
- Collaborate on design and other features

Comprehensive Monitoring & Management

- Unified visibility into **Gen3, Kubernetes, and cloud resources** for proactive issue resolution.

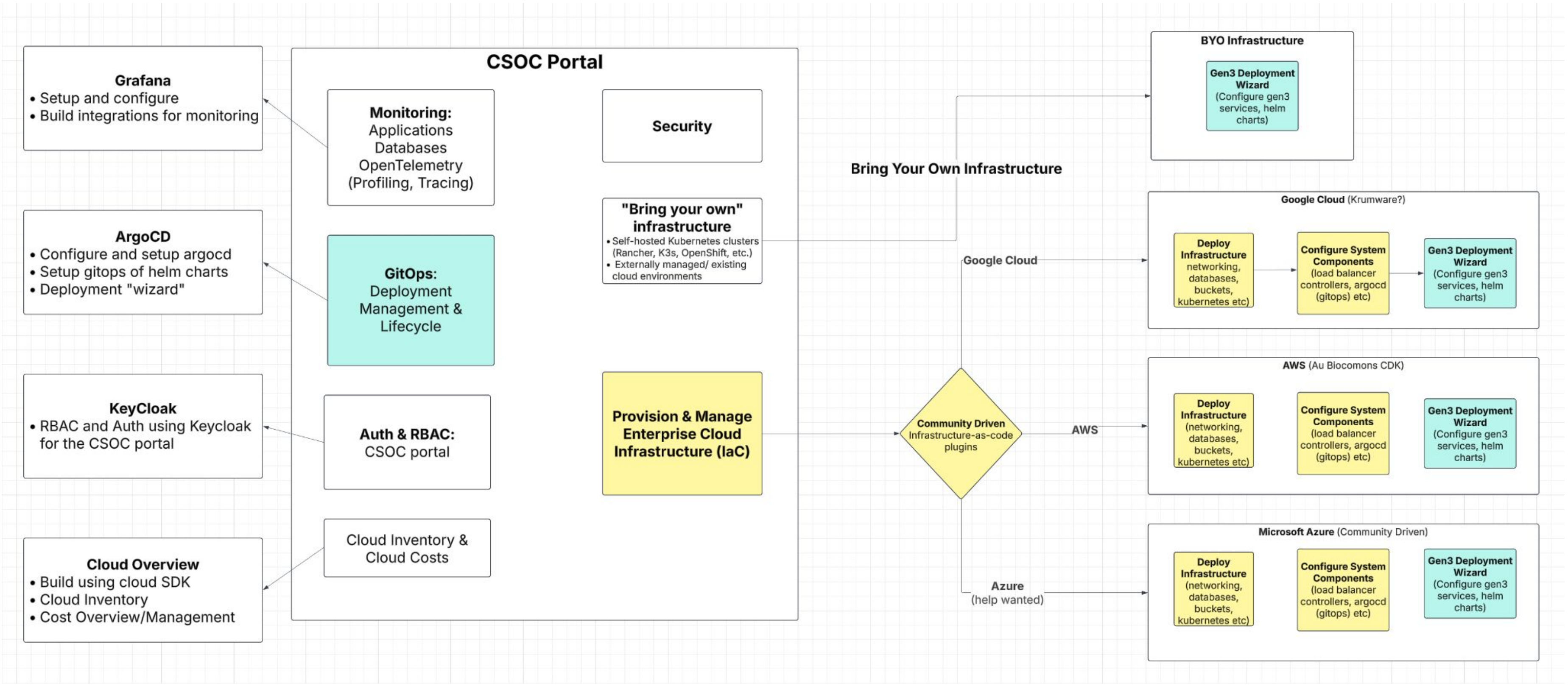
Collaboration & Third-Party Integration

- How to design the **CSOC** to facilitate cross-organization contributions?
- Ensuring flexibility so **different solutions** can be integrated effectively.
- Encouraging contributions that address various aspects of **Gen3 deployment, monitoring, and cloud management**.
- This may include a range of integration levels - from making containers available in Gen3 that are maintained by other organizations to full integration into Gen3 code base for other features.

Infrastructure as Code (IaC) for Enterprise-Grade Deployments

- Develop a **containerized plugin system** to manage infrastructure deployments.
- Benefits of a **containerized approach**:
  - Can be run independently without requiring CSOC.
  - Enables modular, reusable infrastructure components.
  - Getting a solution quickly to operators
  - Leverages expertise of others (which may be lacking at CTDS)
- Downsides includes support challenges (true for any community contributions) and maintenance, which may require future support from contributors
- **Integrate AU Biocommons CDK** to deploy Gen3 infrastructure across different cloud providers.
- Future expansion to support **Azure, Google Cloud, Digital Ocean**, and other cloud providers.

System Diagram



Grafana
- Setup and configure
- Build integrations for monitoring

ArgoCD
- Configure and setup argocd
- Setup gitops of helm charts
- Deployment "wizard"

KeyCloak
- RBAC and Auth using Keycloak for the CSOC portal

Cloud Overview
- Build using cloud SDK
- Cloud Inventory
- Cost Overview/Management

CSOC Portal

Monitoring: Applications Databases OpenTelemetry (Profiling, Tracing)

Security

GitOps: Deployment Management & Lifecycle

"Bring your own" infrastructure
- Self-hosted Kubernetes clusters (Rancher, K3s, OpenShift, etc.)
- Externally managed/ existing cloud environments

Auth & RBAC: CSOC portal

Provision & Manage Enterprise Cloud Infrastructure (IaC)

Cloud Inventory & Cloud Costs

Bring Your Own Infrastructure

Community Driven Infrastructure-as-code plugins

Google Cloud

AWS

Azure (help wanted)

BYO Infrastructure

Gen3 Deployment Wizard (Configure gen3 services, helm charts)

Google Cloud (Krumware?)

Deploy Infrastructure networking, databases, buckets, kubernetes etc)

Configure System Components (load balancer controllers, argocd (gitops) etc)

Gen3 Deployment Wizard (Configure gen3 services, helm charts)

AWS (Au Biocomons CDK)

Deploy Infrastructure (networking, databases, buckets, kubernetes etc)

Configure System Components (load balancer controllers, argocd (gitops) etc)

Gen3 Deployment Wizard (Configure gen3 services, helm charts)

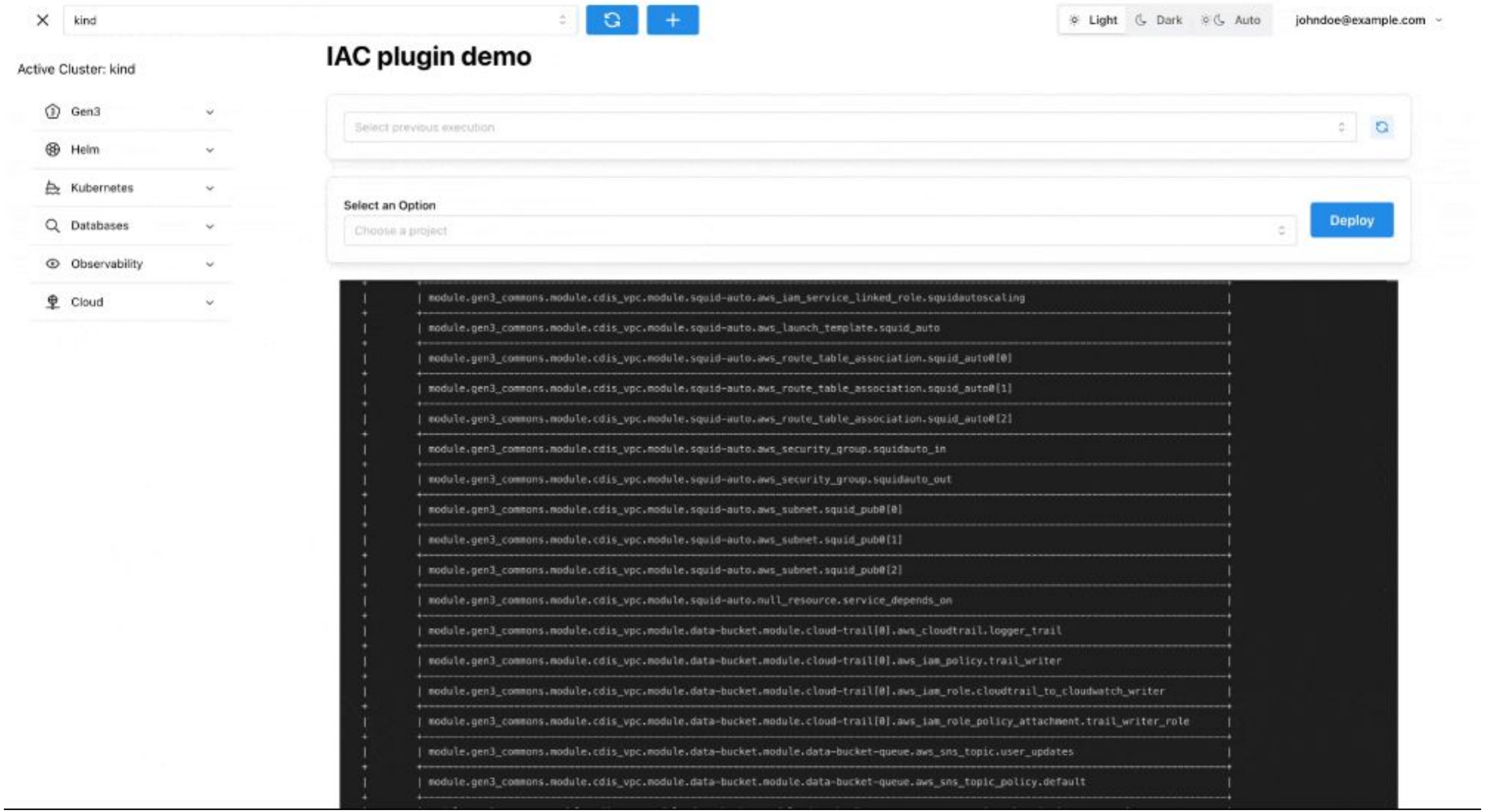
Microsoft Azure (Community Driven)

Deploy Infrastructure (networking, databases, buckets, kubernetes etc)

Configure System Components (load balancer controllers, argocd (gitops) etc)

Gen3 Deployment Wizard (Configure gen3 services, helm charts)

IAC plugin (proof of concept) demo



Active Cluster: kind

IAC plugin demo

Select an Option

```
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_iam_service_linked_role.squidautoscaling              |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_launch_template.squid_auto                            |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_route_table_association.squid_auto0[0]                |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_route_table_association.squid_auto0[1]                |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_route_table_association.squid_auto0[2]                |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_security_group.squidauto_in                           |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_security_group.squidauto_out                          |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_subnet.squid_pub0[0]                                  |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_subnet.squid_pub0[1]                                  |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.aws_subnet.squid_pub0[2]                                  |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.squid-auto.null_resource.service_depends_on                          |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.cloud-trail[0].aws_cloudtrail.logger_trail        |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.cloud-trail[0].aws_iam_policy.trail_writer        |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.cloud-trail[0].aws_iam_role.cloudtrail_to_cloudwatch_writer |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.cloud-trail[0].aws_iam_role_policy_attachment.trail_writer_role |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.data-bucket-queue.aws_sns_topic.user_updates      |
+          +--------------------------------------------------------------------------------------------------------------+
|          | module.gen3_commons.module.cdis_vpc.module.data-bucket.module.data-bucket-queue.aws_sns_topic_policy.default    |
+          +--------------------------------------------------------------------------------------------------------------+
```

Roadmap, 1 of 2

Infrastructure as Code (IaC) for Enterprise-Grade Deployments

- Develop a **containerized plugin system** to manage infrastructure deployments.
- **Integrate AU Biocommons CDK** to deploy Gen3 infrastructure across different cloud providers.
- Future expansion to support **Azure, Google Cloud, Digital Ocean**, and other cloud providers.

Cloud Integrations & Cost Management

- Build out a **cloud inventory** system for managing VMs (EC2 instances, Droplets, etc.).
- Provide a **cost overview dashboard** for resource tracking.
- Introduce **FinOps capabilities** to optimize cloud expenditures.

“Quick Start” for Gen3

- Develop an **easy-to-use Quick Start** feature to deploy Gen3 rapidly.
- Pre-configure Gen3 with **demo data** for testing and onboarding.

Roadmap, 2 of 2

RBAC for the CSOC + Integration with Keycloak

- Centralized authentication and authorization management.
- Support for **OIDC, SAML, and fine-grained role-based access control (RBAC)**.
- Add auditing functionality

Automated Security & Compliance Checks

- Continuous monitoring for security misconfigurations.

Advanced Monitoring & Observability

- **"At-a-glance" Overview**
  - Know exactly what’s happening inside your **Gen3 environment** in real-time.
- **Integration with OpenTelemetry**
  - Enable **distributed tracing** and deep observability for all services.
- **Service Health Metrics**