



# Interview at Diamond Light Source

For the position of Senior DevOps Engineer

---

Dr Matthew Heath

13<sup>th</sup> February 2024

# Table of Contents

Career Highlights

CERN and the University of Edinburgh

Science and Technology Facilities Council

EscherCloud

Interests and Hobbies

## Career Highlights

---

# Overview

- Doctoral Student  
**University of Edinburgh**  
(Sept 2016 – Feb 2022)
- Storage System Administrator  
**STFC**  
(Jan 2021 – May 2022)
- Cloud Engineer  
**EscherCloud**  
(Jun 2022 – Jan 2024)



Science and  
Technology  
Facilities Council

# CERN and the University of Edinburgh

---

# Doctoral Student

- Conducted research as a member of the ATLAS Experiment.<sup>a</sup>
- Emulated complex detector geometry as part of FASTCALOSIM upgrade.<sup>b</sup>
- ML derived multivariate reweightings of simulation samples.<sup>c</sup>

---

<sup>a</sup>Heath, “Modelling Uncertainties for Measurements of the  $H \rightarrow \gamma\gamma$  Channel with the ATLAS Detector at the LHC”.

<sup>b</sup>The ATLAS Collaboration, “AtlFast3: the next generation of fast simulation in ATLAS”.

<sup>c</sup>The ATLAS Collaboration, *Measurement of the properties of Higgs boson production at  $\sqrt{s} = 13$  TeV in the  $H \rightarrow \gamma\gamma$  channel using 139  $\text{fb}^{-1}$  of  $pp$  collision data with the ATLAS experiment*.

Modelling Uncertainties for  
Measurements of the  $H \rightarrow \gamma\gamma$  Channel  
with the ATLAS Detector at the LHC  
Matthew Peter Heath



Doctor of Philosophy  
The University of Edinburgh  
January 2023



# Science and Technology Facilities Council

---

# Storage System Administrator

- Maintained and developed 24/7 availability storage services for the Data Services group in the Scientific Computing Department.
- Managed key storage services:
  - **Echo:** ~70PiB Ceph object store.
  - **Deneb:** ~4PiB Ceph file system.
  - **Sirius:** ~700TiB Ceph block store backend for the Cinder service of SCD's OpenStack cloud platform.
- Provided line management and mentoring:
  - Mentored members of the internship program.
  - Guided junior members of the storage team.
- Conducted Research and Development:
  - Explored prospective new services and developments in the storage domain.
- On-call Support:
  - Part of the on-call rota for addressing service issues outside of office hours.

# VOMS AuthN/AuthZ for Echo

- **Objective:** Strengthen security and access control for Echo object store service via the XRootD protocol.
- **Previous AuthN/AuthZ Process:**
  - AuthN: VOMS certificate.
  - AuthZ: Scheduled lookup file update based on virtual organisation databases.
- **Challenges:**
  - Delayed permissions updates posed security risks.
  - Potential access for recently rescinded users during updates.
- **Implemented Solution:**
  - Configured XRootD authZ/N to directly integrate with virtual organisation VOMS servers.
  - Real-time access to the latest object, role, and member permissions.
  - Provided SCD admins with utility for custom banlist curation.
- **Outcome:**
  - Enhanced security and access control for Echo object store service.
  - Mitigated risks of delayed updates and unauthorised access.

EscherCloud

---

# Cloud Engineer

- **EscherCloud:** Startup providing GPU-enabled private cloud services, emphasising sustainability, European data sovereignty, and democratising AI/ML.
- **Role and Achievements:**
  - Deployed and managed Ceph storage backend for OpenStack, forming the foundation for the inaugural PaaS offering.
  - Expanded responsibilities to encompass all aspects of cloud infrastructure, from server provisioning to monitoring, visualisation, and central logging.
  - Managed OpenStack services, VLANs, DNS, private network access, and more.
- **Contributions to Company Growth:**
  - Enabled onboarding of engineering interns, providing ongoing line management and mentoring as they transitioned to full employees.

# Configuration Management Automation

- **Overview:** Developed a comprehensive configuration automation service, unifying server inventory with a CIDB.
- **Ansible Implementation:**
  - Utilised CIDB API for real-time physical and virtual server inventory.
  - Implemented Ansible plugin for up-to-date playbooks based on server inventory groupings.
- **Rundeck Deployment:** Implemented Rundeck for a streamlined UI, codifying and simplifying automation job execution.
- **Benefits:**
  - Achieved efficient and centralised infrastructure configuration management.
  - Simplified automation job execution through Rundeck.

# VM System Backup Service

- **Overview:** Developed a backup tool for libvirt KVMs across a data centre.
- **Key Features:**
  - Utilised restic, a modern backup program written in Go, for secure backups to Ceph S3 object storage.
  - Deployed Ansible for automation and developed custom Python modules for Virsh libvirt interaction.
- **Custom Ansible Modules:**
  - Developed custom Python modules to interface with the Virsh libvirt command line tool.
  - Extracted full KVM specifications and managed virtual disk images for seamless data export without downtime.
- **Benefits:**
  - Established a robust backup solution, ensuring data integrity and efficient recovery.
  - Utilised restic and Ceph S3 for streamlined backup processes.

# Zero Trust Access Control Plane

- **Overview:** Implemented zero-trust access for EscherCloud admins and engineers.
- **Zero-Trust Definition:** A security model demanding strict identity verification for resource access, irrespective of network location. No default trust in users or systems.
- **Tool Assessment:** Explored Pomerium, TailScale, and Warpgate as possible access solutions, selecting Teleport.
- **Teleport Features:** Provided secure and configurable MFA, RBAC, and IDAC for server access, extending benefits to a secure reverse proxy for private network web applications. Also provided implementation of machine users to provide access for service accounts like an Ansible user.
- **Benefits:** Implemented a robust zero-trust approach for heightened security, leveraging Teleport for enhanced access control and web service security.

## Interests and Hobbies

---

# À la Cuisine



# Out and About



# Admiring my Handiwork



Thank you for listening!

---

# Acknowledgements

- $\text{\LaTeX}$ Beamer theme.<sup>1</sup>

---

<sup>1</sup>Vogelgesang, *Metropolis*.

# References

---

-  Heath, Matthew Peter. “Modelling Uncertainties for Measurements of the  $H \rightarrow \gamma\gamma$  Channel with the ATLAS Detector at the LHC”. Presented 08 Nov 2021. The University of Edinburgh, 2022. URL: <https://cds.cern.ch/record/2801233>.
-  The ATLAS Collaboration. “**AtlFast3: the next generation of fast simulation in ATLAS**”. In: *Comput. Softw. Big Sci.* 6 (2022), p. 7. DOI: [10.1007/s41781-021-00079-7](https://doi.org/10.1007/s41781-021-00079-7). arXiv: [2109.02551](https://arxiv.org/abs/2109.02551). URL: <https://cds.cern.ch/record/2780174>.
-  — . *Measurement of the properties of Higgs boson production at  $\sqrt{s} = 13 \text{ TeV}$  in the  $H \rightarrow \gamma\gamma$  channel using  $139 \text{ fb}^{-1}$  of  $pp$  collision data with the ATLAS experiment*. Tech. rep. Geneva: CERN, 2022. arXiv: [2207.00348](https://arxiv.org/abs/2207.00348). URL: <https://cds.cern.ch/record/2814435>.
-  Vogelgesang, Matthias. **Metropolis**. Version 1.2. Jan. 2017. URL: <https://github.com/matze/mtheme>.