Hardening Kubeflow Security for Enterprise Environments

[Julius von Kohout](#) - DPDHL, Freelancer

Deutsche Post DHL Group

[Diana Dimitrova Atanasova](#) - VMware

Agenda

Introduction

- What is Kubeflow?
- Who uses it and why?

Security working group

- CVE image scanning
- SBOMs

Network

- Architecture
- Authentication

Example security issues and solutions

- Rootless containers
- Profile controller permissions
- Namespace sharing
- Multi-user artifact storage
- Multi-user ml-metadata
- KFP UI namespace verification
- Appendix: KFP denial of service

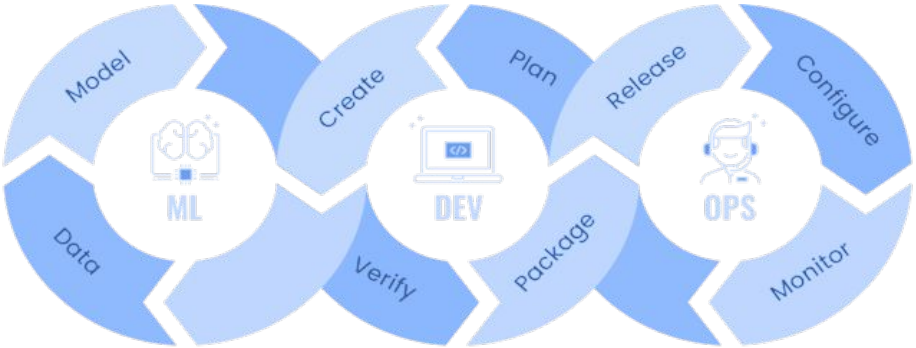
Conclusion

What is Kubeflow?

- Open-source MLOps platform on K8s
- Building, scaling, orchestrating ML workflows
- Standardize and automate the iterative ML Workflow
- Reusable modular pipelines, hyperparameter tuning, online IDEs, lineage tracking, multi-tenancy, model serving
- Developed by Google, IBM, AWS, Arrikto, DHL, VMware, …
- CNCF incubating project donated by Google

Kubeflow

1.7 Released



How to implement the **iterative** ML Workflow on Kubernetes?

Who uses it and why?

- Various industries including Telecommunication, finance, medical, insurance
  - Especially the regulated sectors
- IBM, Google, AWS, Bloomberg, DHL, Deutsche Telekom, VMware, Arrikto, Capital One, Walmart, Uber, Spotify, Shopify, PayPal, Hospitals, …
- Google even uses Kubeflow (Vertex AI) as default ML platform on GCP
- No similar open-source ML orchestration alternative available
- Vendor agnostic, scalable, sovereign, standardized and fairly secure
  - So similar reasons as for on-premises Kubernetes

Security working group

Define policies and procedures

Enforce security best practices

✓ Authenticate API calls

✓ Least privilege RBAC

✓ CVE scanning

SBOM

Slack,

bi-weekly meetings,

meeting notes

Some issues are covered on the following slides

CVE image scanning

KubeCon CloudNativeCon Europe 2023

Working Group	Images	Critical CVE	High CVE	Medium CVE	Low CVE
AutoML	13	12	83	58	6
Pipelines	28	44	300	239	12
Workbenches (Notebooks)	3	9	32	39	6
Kserve	12	53	406	277	33
Common	29	22	175	117	8

Canonical pledged to fix all critical and high CVEs

Secure Software Supply Chain

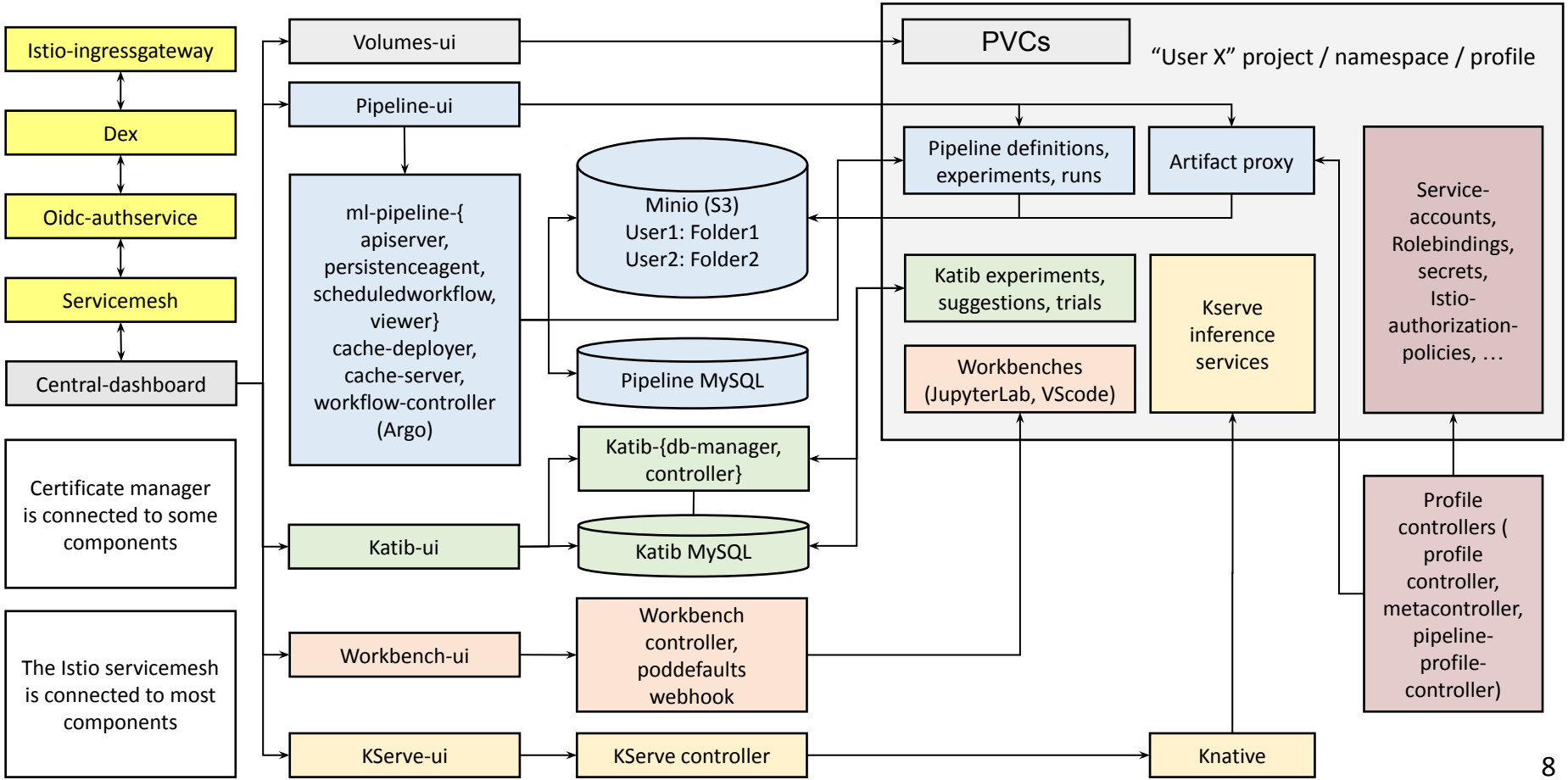
Integrate Software Bill Of Materials (SBOM)

Software component inventory list in standardized format

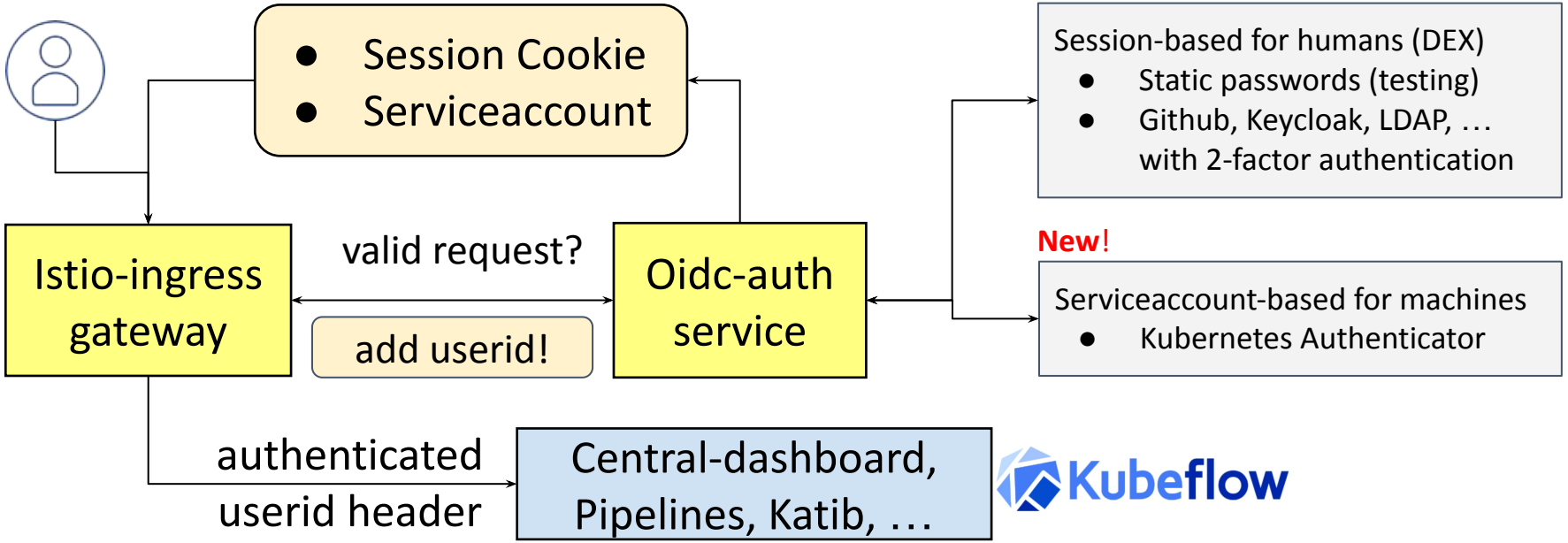
Ensure the project is license compliant

[Proposal]

Architecture



Authentication via session or token



- Oidc-authservice supports only interactive sessions for humans in KF 1.6
- We had to simulate web browsers and disable 2FA for machines
- 1.7 has programmatic authentication with Kubernetes serviceaccounts ✓

Istio and Networkpolicies

- We had a lot of problems over the last years
  - Services were misconfigured and allowed to fake the userid header
  - E.g. Workbenches, Volumes, etc. allowed to impersonate other users
  - Even the user-management was unprotected a year ago

✓ We fixed these issues upstream

✓ Hardened Istio with security best-practices

✓ Added Networkpolices as a second layer of defense

Rootless containers

- Root is in general an unnecessary security risk
  - Despite efforts such as usernamespaces in Kubernetes
- Forbidden by company policies in enterprise environments
- By default containers still run as root, also in user-controlled namespaces

✓ Over the last two years we made it possible to run 99 % rootless
✓ Istio-CNI for rootless Istio initcontainers (rootful CNI deamonset)
✓ Enforce PodSecurityPolicies (example) or PodSecurityStandards

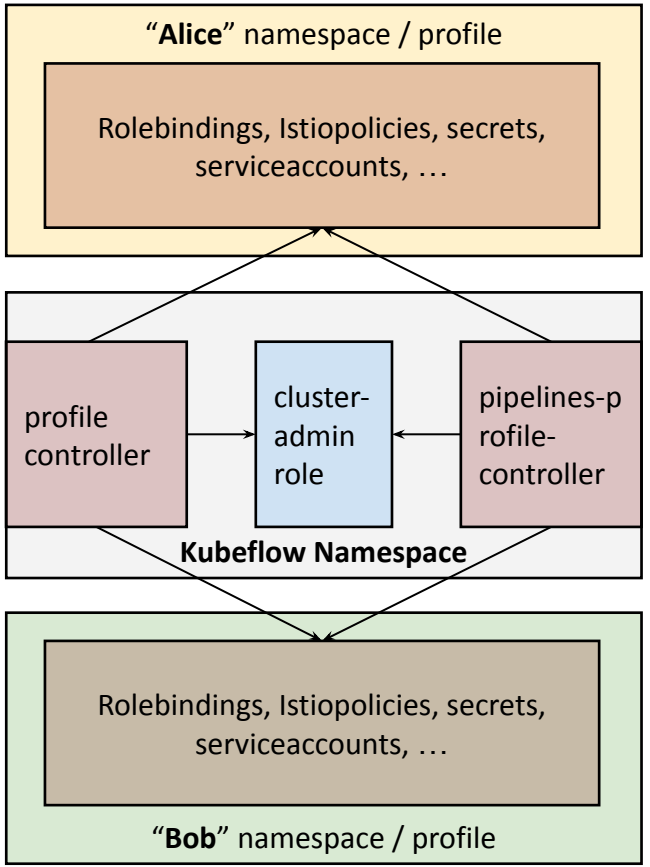
- Limitation: Podman and Kaniko do not support rootless builds yet

Profile controller permissions

- Profile-controller (PC) creates user namespaces and adds rolebindings and serviceaccounts in that namespace
- Pipelines-profile-controller (PPC) adds secrets and deployments to user namespaces

- Problem: Both use the cluster-admin role
- One exploit in the Kubeflow namespace and you can become cluster-admin

- There should be a reduced clusterrole
- Merge PC and PPC to reduce complexity



Namespace sharing

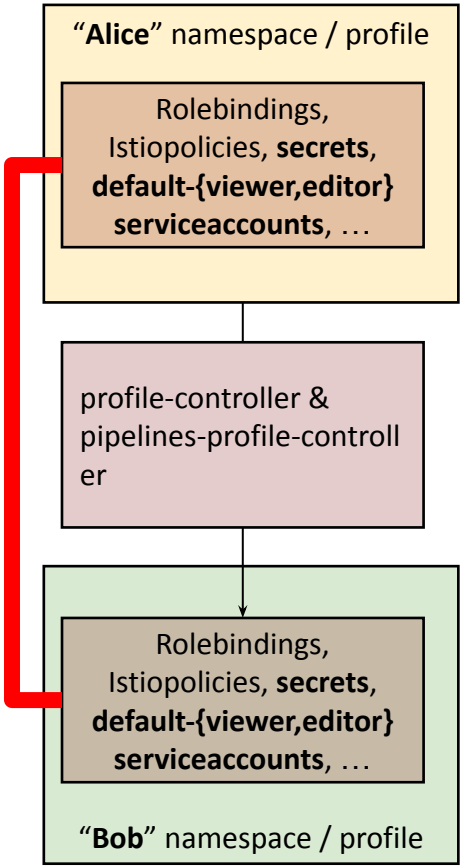
- You can share your namespace with collaborators
- Sharing is broken from a K8s security perspective

- Escalation from default-viewer to default-editor
- Alice steals the serviceaccount token, leaves the company and impersonates Bob with the bearer token

- Solution 1: “Disable Sharing”
- Solution 2: “Regenerate all generated secrets, serviceaccounts and pods when removing a collaborator”

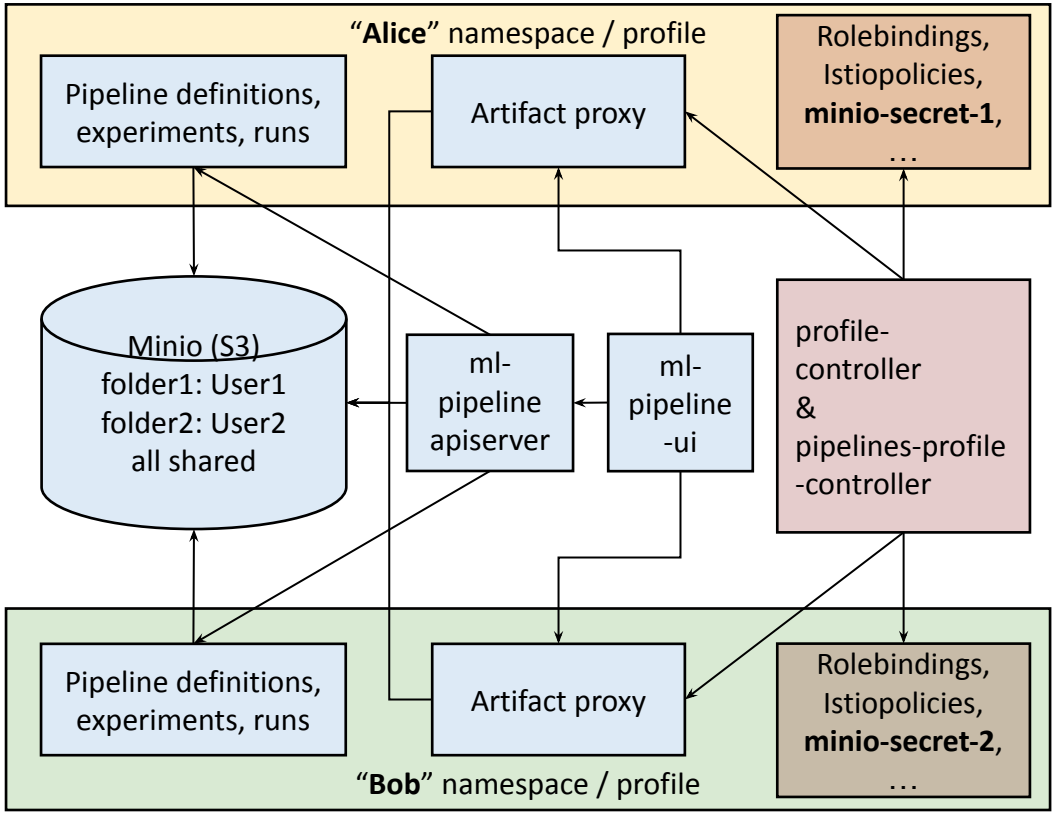
Sharing is Daring

Share with Collaborator



Multi-user artifact storage MinIO / S3

- KFP uses Minio as S3 storage
- Issue: Users share the minio admin secret and all artifacts
- PoC: isolate artifacts per user
- TODO: Get rid of passwords and use Istio namespace origin for authorization
- TODO: find replacement for Old minio image with CVEs (Apache 2 -> AGPL)



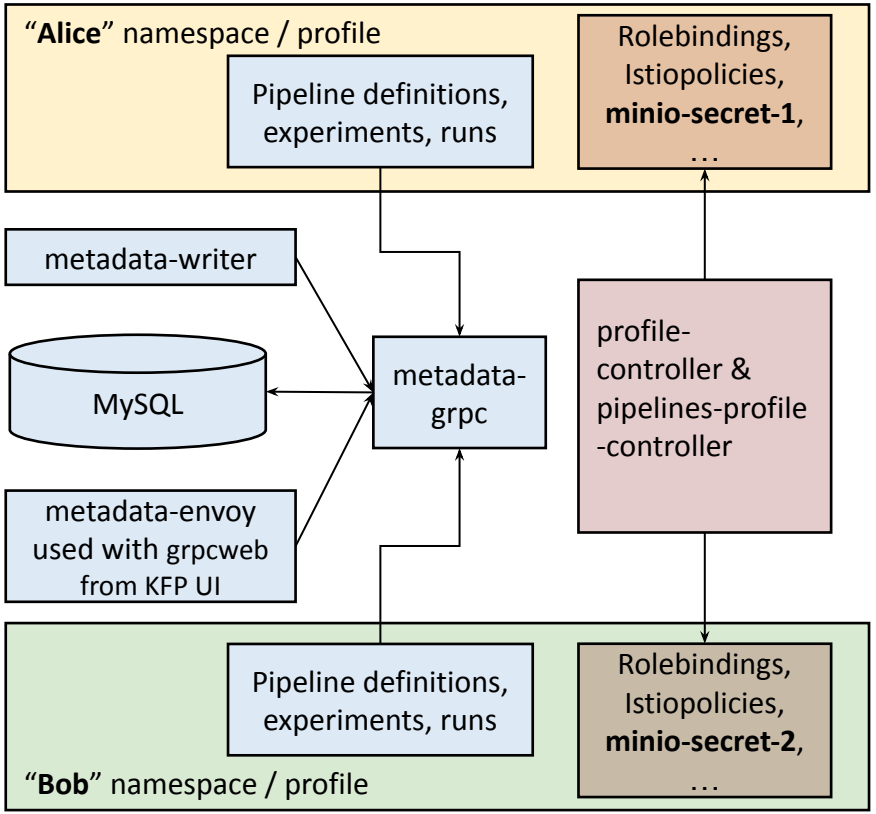
Multi-user ML-MetaData

- Metadata for pipeline run artifacts
- Also used heavily by TensorFlow

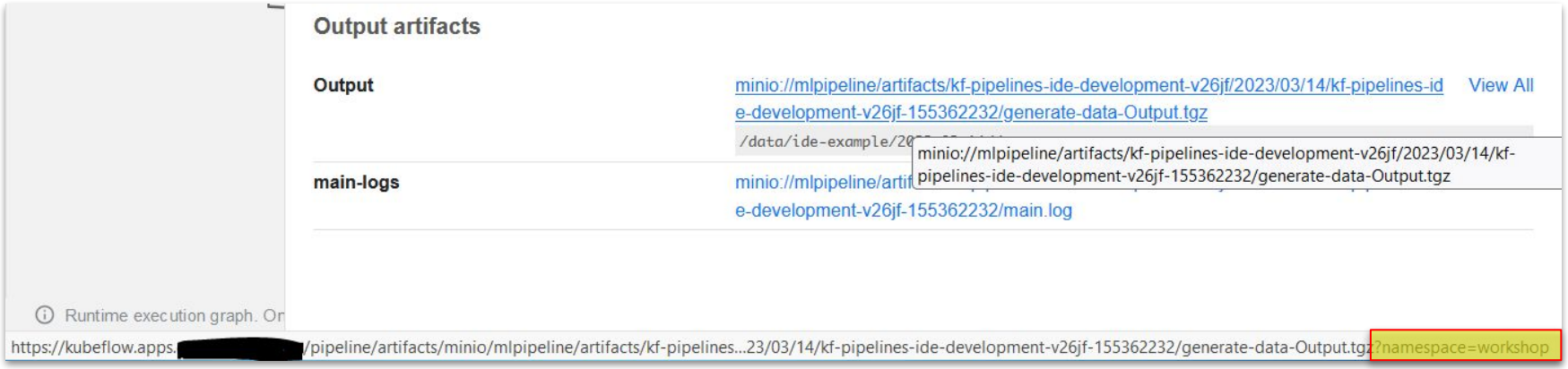
- No multi-tenancy support
- MLMD is just shared for all users

- Solution for KFP 1: Just disable it
- KFP 2 requires MLMD

- TODO: Isolate it per user for KFP 2
- Looking for volunteers



KFP UI namespace verification



- If Alice spies Bobs S3 artifact filepath, then KFP UI allows Alice to read the content
- Just remove the ?namespace=xxx parameter and the UI will not check permissions
- Technical debt:
  - UI server skips the protected KFP-API server and accesses MinIO directly
  - Artifact proxy in the user namespace is rather obsolete

Appendix: KFP denial of service

- Due to inefficient database queries
  - The database remains locked for a long time
  - All subsequent user requests against KFP API fails
  - Sabotaging other users and projects
  - Issue: https://github.com/kubeflow/pipelines/issues/6845

- Proposed solution:
  - *Replace nested subqueries* with *joins wherever possible*
  - *Joins* have better performance
  - *Joins* are more readable for experienced developers
  - It looks like update with join is not supported by squirrel/mysqlite
  - Pure MySQL works, we might have to update the library
  - Looking for volunteers

Conclusion

- ✓ Authenticate most API calls
- ✓ Lower privilege RBAC
- ✓ Security working group
- ✓ CVE image scanning
- ✓ SBOMs
- ✓ Authentication via serviceaccount
- ✓ Istio improvements
- ✓ Networkpolicies
- ✓ Rootless containers

- Profile controllers permissions
- Namespace sharing
- Multi-user artifact storage
- Multi-user ml-metadata
- KFP UI namespace verification
- KFP Denial of service

Join us!

Kubeflow welcomes new contributors!

Kubeflow

join the community

slack

#kubeflow/security

security WG
meeting minutes

Thank you


juliusvonkohout@gmail.com


https://www.linkedin.com/in/juliusvonkohout/


dianaa@vmware.com


https://www.linkedin.com/in/atanasova-diana/

Please scan the QR Code above
to leave feedback on this session

Selected contributions overview

Kubeflow member (promoted by Google) for around 2 years https://github.com/kubeflow/internal-acls/pull/509

KubeCon CloudNativeCon Europe 2023

- **Argo:**
- https://github.com/argoproj/argo-workflows/pull/3785
- **kubeflow/pipelines:**
- https://github.com/kubeflow/pipelines/pull/4479
- https://github.com/kubeflow/pipelines/pull/4645
- was dropped in favor of the argo emmissary executor
- https://github.com/kubeflow/pipelines/pull/5278
- https://github.com/kubeflow/pipelines/pull/5294
- https://github.com/kubeflow/pipelines/pull/5695
- https://github.com/kubeflow/pipelines/pull/5742
- https://github.com/kubeflow/pipelines/pull/5743
- https://github.com/kubeflow/pipelines/pull/6537 also affecting Kubeflow/manifests/contrib/metacontroller
- https://github.com/kubeflow/pipelines/pull/6622
- https://github.com/kubeflow/pipelines/pull/6691
- https://github.com/kubeflow/pipelines/pull/6882
- https://github.com/kubeflow/pipelines/pull/6892
- https://github.com/kubeflow/pipelines/pull/7031
- https://github.com/kubeflow/pipelines/pull/7155
- https://github.com/kubeflow/pipelines/pull/7311
- https://github.com/kubeflow/pipelines/pull/8270
- **Ray integration:**
- **https://github.com/kubeflow/manifests/pull/2383**
- https://github.com/ray-project/kuberay/pull/750
- https://github.com/ray-project/kuberay/pull/752
- https://github.com/ray-project/ray/pull/31563

- **BentoML integration:**
- https://github.com/kubeflow/manifests/pull/2350
- **kubeflow/kubeflow:**
- https://github.com/kubeflow/kubeflow/pull/5668
- https://github.com/kubeflow/kubeflow/pull/5891
- https://github.com/kubeflow/kubeflow/pull/6148
- https://github.com/kubeflow/kubeflow/pull/6216
- https://github.com/kubeflow/kubeflow/pull/6216
- https://github.com/kubeflow/kubeflow/pull/6241
- https://github.com/kubeflow/kubeflow/pull/6656
- https://github.com/kubeflow/kubeflow/pull/6673
- **kubeflow/manifests:**
- https://github.com/kubeflow/manifests/pull/1759
- https://github.com/kubeflow/manifests/pull/2013
- https://github.com/kubeflow/manifests/pull/2121
- https://github.com/kubeflow/manifests/pull/2189
- https://github.com/kubeflow/manifests/pull/2205
- https://github.com/kubeflow/manifests/pull/2254
- https://github.com/kubeflow/manifests/pull/2298
- https://github.com/kubeflow/manifests/pull/2304
- https://github.com/kubeflow/manifests/pull/2348
- https://github.com/kubeflow/manifests/pull/2357
- **Kserve:**
- https://github.com/kserve/kserve/pull/1996
- **Seldon:**
- https://github.com/SeldonIO/seldon-core/pull/3141
- **Jupyterlab:**
- https://github.com/jupyter-server/kernel_gateway/pull/321
- https://github.com/jupyter-incubator/sparkmagic/pull/541
- https://github.com/jupyter-incubator/sparkmagic/pull/549

- **Open PRs:**
- https://github.com/kubeflow/manifests/pull/2329
- https://github.com/kubeflow/website/pull/3403
- https://github.com/kubeflow/pipelines/pull/7729
- https://github.com/kubeflow/pipelines/pull/7725
- https://github.com/kubeflow/katib/pull/1768
- https://github.com/kubeflow/kubeflow/pull/6160
- https://github.com/kubeflow/pipelines/pull/6629
- **Mentoring, implementation help and reviewing:**
- https://github.com/kubeflow/kubeflow/issues/6702 Tobias Goerke first Kubeflow contribution
- https://github.com/kubeflow/pipelines/pull/7819 Major overhaul of KFP security with Diana Atanasova
- https://github.com/kubeflow/manifests/pull/2286 Contribution Guidelines
- https://github.com/kubeflow/kubeflow/issues/6228
- https://github.com/kubeflow/manifests/issues/2014
- https://github.com/kubeflow/pipelines/issues/5718 Emissary excutor and rootless pipelines
- https://github.com/kubeflow/kubeflow/issues/6662 Security Agenda
- Telekom Data Science Platform Kubeflow distribution
- https://github.com/kubeflow/manifests/issues/2312
- https://github.com/kubeflow/website/pull/3403