

Managing multiple IAM deployments on Kubernetes @ INFN-CNAF


Andrea Ceccanti & Cristina Duma
INFN CNAF

IAM User's Workshop
27/01/2021



IAM @ CNAF

INDIGO IAM for cta-1st @ INFN



Welcome to cta-1st @ INFN-CNAF

Sign in with

Your X.509 certificate


CTA-LST SSO

Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

INDIGO IAM for iotwins-Log in



Welcome to iotwins

Sign in with your iotwins credentials

Username

Password

Sign in

Forgot your password?


Or sign in with

INFN AAI

Not a member?

Apply for an account

INDIGO IAM for wlcg-Log in



Welcome to wlcg

Sign in with your wlcg credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your X.509 certificate


CERN SSO

Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

INDIGO IAM for virgo-Log in



Welcome to virgo


Sign in with

LIGO

Not a member?

Apply for an account

INDIGO IAM for t1-computing-Log in



Welcome to t1-computing

Sign in with your t1-computing credentials

Username

Password

Sign in

Forgot your password?

Or sign in with


INFN AAI

Not a member?

Apply for an account

https://iam-t1-computing.cloud.cnf.infn.it

INDIGO IAM for super-Log in



Welcome to super

Sign in with your super credentials

Username

Password

Sign in

Forgot your password?


Or sign in with

eduGAIN

Not a member?

Apply for an account

INDIGO IAM for herd-Log in



Welcome to herd

Sign in with your herd credentials

Username

Password

Sign in

Forgot your password?

Or sign in with


Google

INFN AAI

Not a member?

Apply for an account

INDIGO IAM for eosc-hub-Log in



Welcome to eosc-hub

Sign in with your eosc-hub credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google

B2ACCESS


eduGAIN

ESI

Not a member?

Apply for an account

INDIGO IAM for indigo-dc-Log in



Welcome to indigo-dc

Sign in with your indigo-dc credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Google


ESI

eduGAIN

Not a member?

Apply for an account

INDIGO IAM for escape-Log in



Welcome to escape

Sign in with your escape credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your X.509 certificate

Google

eduGAIN

Not a member?

Apply for an account

You have been successfully authenticated as
CN=Andrea Ceccanti,CN=657221,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch

IAM deployment @ CNAF

~20 IAM instances in support of various projects

- WLCG, ESCAPE, DODAS, Deep Hybrid DataCloud, EOSC-Hub, HERD, IOTwins, EOSC-Pillar, EGO-VIRGO, T1-Computing, PLANET, MVM, CTA-LST, ...

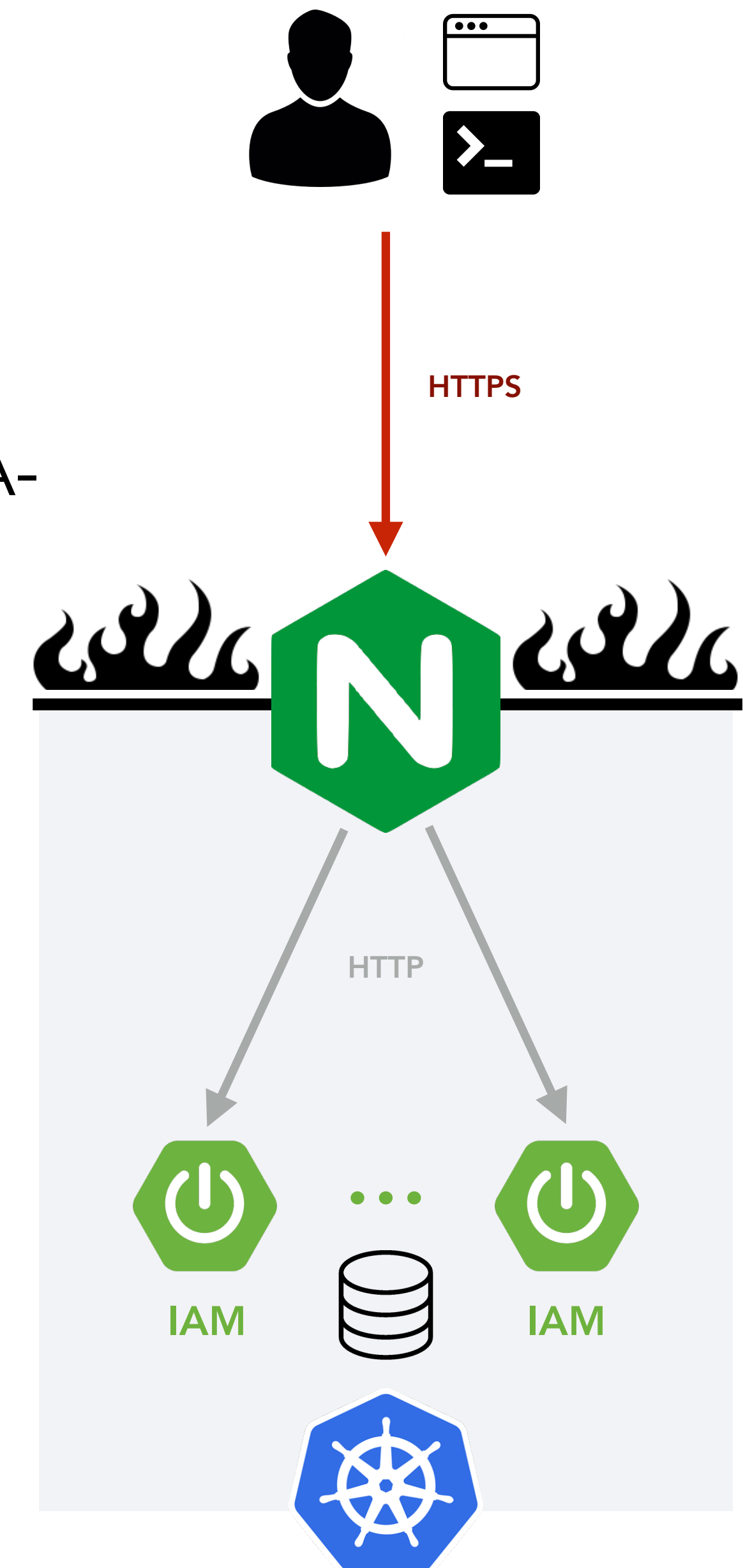
Deployed on a Kubernetes cluster

- Each projects gets a dedicated K8S namespace

Data stored on HA Percona MySQL cluster

Kubernetes advantages

- rolling updates
- consistent management



Kustomize for easy configuration management

Config for running instances stored on INFN Gitlab server

- baltig.infn.it

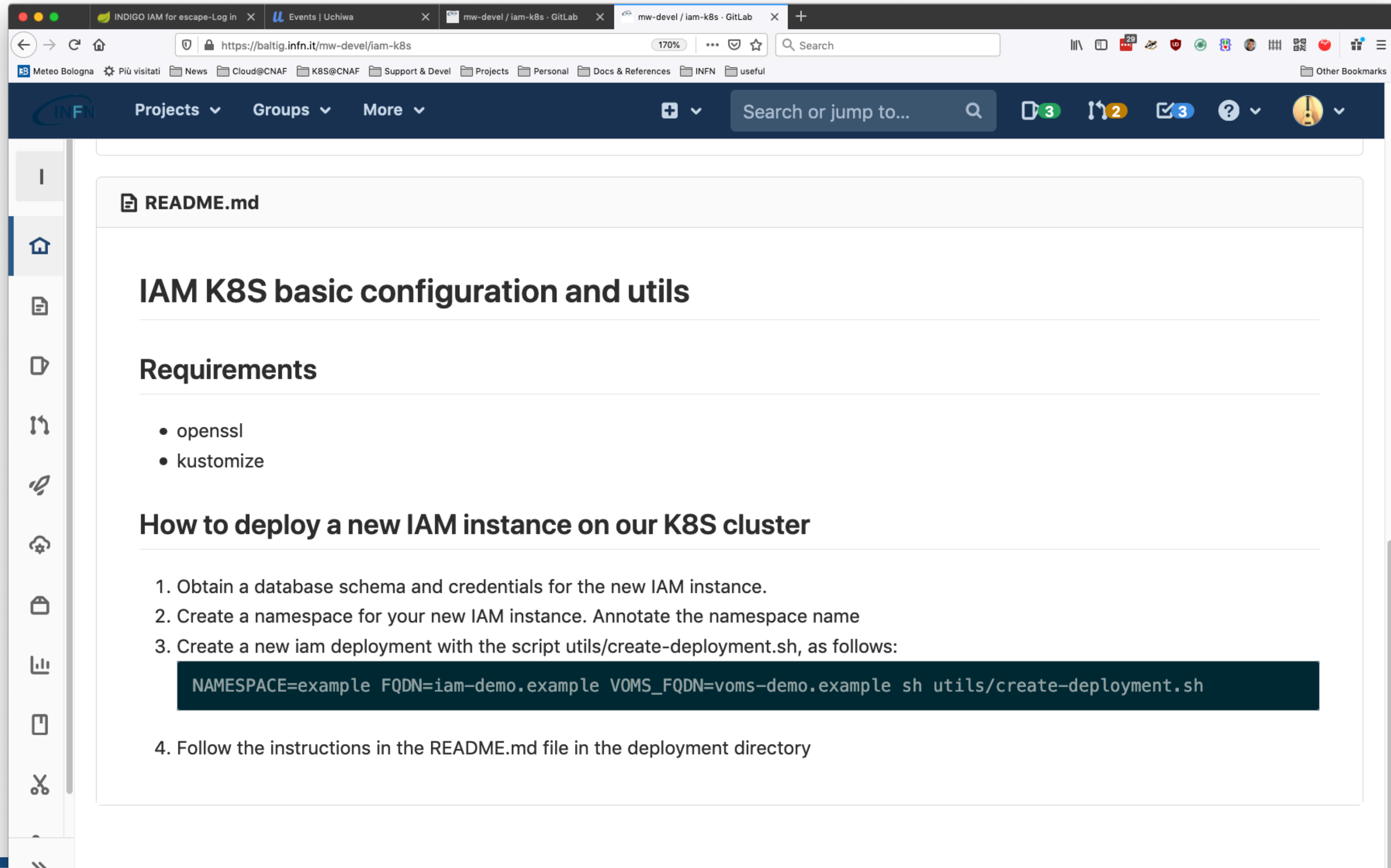
Kustomize used to implement configuration management

- K8S-blessed config management solution, built-in in kube
- Allows to implement hierarchical configuration structures
- Base configuration common to all IAM instances with reasonable defaults
- Each deployment then customizes the configuration according to the specific needs



image source: <https://kustomize.io/>

Deploying new instances is easy



The screenshot shows a web browser window with the URL `https://baltig.infn.it/mw-devel/iam-k8s`. The browser's address bar shows the URL and a search bar. The page content is a README.md file with the following sections:

- README.md**
- IAM K8S basic configuration and utils**
- Requirements**
 - openssl
 - kustomize
- How to deploy a new IAM instance on our K8S cluster**
 1. Obtain a database schema and credentials for the new IAM instance.
 2. Create a namespace for your new IAM instance. Annotate the namespace name
 3. Create a new iam deployment with the script `utils/create-deployment.sh`, as follows:

```
NAMESPACE=example FQDN=iam-demo.example VOMS_FQDN=voms-demo.example sh utils/create-deployment.sh
```
 4. Follow the instructions in the README.md file in the deployment directory

The create-deployment.sh script

Creates a folder with the configuration for the new deployment and implements basic IAM instantiation chores:

- create JSON Web Keys keystore
- create SAML keystore

Right after the command, the configuration can be applied and will result in a working IAM instance

- running against a volatile, in-memory database

Towards an HA deployment

The current deployment is not HA

- if the infrastructure hosting the k8s cluster goes down, all the IAM instances will be affected

We are currently exploring two strategies for an HA IAM deployment

- local HA deployment, leveraging multiple availability zones within INFN-CNAF
 - doesn't protect from a full INFN-CNAF data center down
- multi-center HA deployment, with IAM deployed on one(or more) K8S clusters deployed in different INFN data centers

**Thanks for your attention.
Questions?**

References

IAM @ GitHub: <https://github.com/indigo-iam/iam>

IAM documentation: <https://indigo-iam.github.io/docs>

Kustomize: <https://kustomize.io/>

Contacts:

- andrea.ceccanti@cnaa.infn.it
- indigo-iam.slack.com