AI Cluster

System Description

Abstract
This is the template for System Description (SysD document) according to the Eclipse Arrowehad documentation structure.

Contents

1 Overview

This document describes the aiCluster system, which provides a in house tool for creating specialized ai models for other systems to consume.

1.1 How This System Is Meant to Be Used

The intended usage of this system is to consume data from other producer services get the necessary data to train and produce Ai models which can be used by other systems to increase efficiency and/or streamline a process.

1.2 System functionalities and properties

1.2.1 Functional properties of the system

Produces Ai model for optimization in later parts of the operational process. This is achieved by Consuming data and forming datasets for training, evaluation and testing.

1.2.2 Data stored by the system

- Data stored: The system will store all data connected to the models. This will be hyperparameters, safetensors of model(for further future applications), metadata of training data and so forth.
- Data dumped: Data consumed for developing a Ai model will be kept until the deployment of the model. Afterwards the data will be removed from the cluster. But a timestamp description will be kept so future training updates of models don't contain already seen data. The deployed models data will be kept for use of other systems as deemed fit.

1.2.3 Non functional properties

- security, AA security based on x.509 certificate is supported.
- safety, ...
- energy consumption, ...
- latency, ...
- Power saving properties, ...

1.2.4 Stateful or stateless

- states preserved, functional and non-functional

1.3 Important Delimitations

This is a system for producing ai models of a specific end use case. The end use case can be anything from production optimization to reviling new approaches to current operation processes. Models might not generalize well between processes, but this is something that has to be evaluated on a case by case basis.

2 Services

2.1 Produced service

- aiCluster service

2.2 Consumed services

- ServiceRegistry
- ServiceOrchestration
- AuthorizationManagement
- Producer Services (For Data)

3 Security

Overview of security level chosen for the system
The following bullets are covered

- The system can be started in un-secure and/or Arrowhead secure mode.
- The system can only handle Arrowhead compliant X.509 certificates.

3.1 Security model

The following is supported by the system:

- Protocols: HTTP.
- Data protection: TLS.
- System authentication capability: Arrowhead X.509 certificate.
- Produced service authorization checking: Via token from Orchestration system directly via the Authorization system.

For Arrowhead certificate profile see github.com/eclipse-arrowhead/documentation

4 References

5 Revision History

5.1 Amendments

Revision history and Quality assurance as per examples below

No.	Date	Version	Subject of Amendments	Author
1	2020-12-05	X.Y.Z		Tanyi Szvetlin
2	2021-07-14	X.Y.Z	Minor updates	Jerker Delsing
3	2022-01-12	X.Y.Z	Minor updates	Jerker Delsing

5.2 Quality Assurance

No.	Date	Version	Approved by
1	2022-01-10	X.Y.Z	