Mentat system

Introduction and latest news

Jan Mach

v1.0, 2018-10-03

Agenda

1. Quick overview
2. Latest news
3. Current state
4. Resources

cesnet

Agenda

cesnet

Motivation

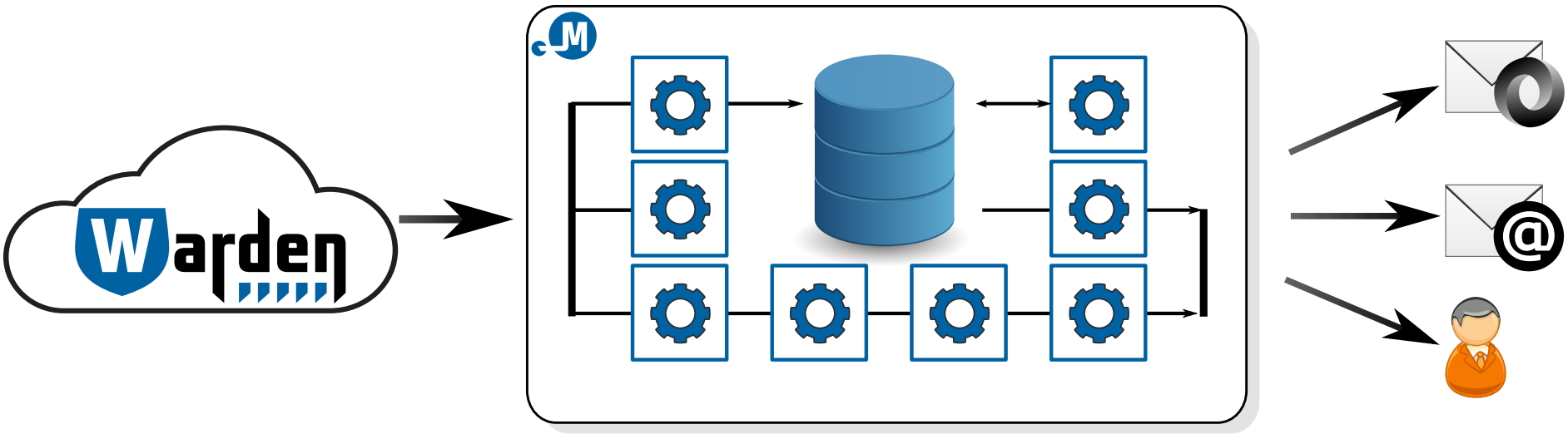
Key ideas

- Resource consolidation
- Aid for CESNET-CERTS security team
- Aid for network administrators

Main features

- Gathering/receiving information from various sources
- Long term searchable persistent information storage
- Real-time and back information processing with various methods
- Fully automatic processing, enable performing of automatic actions on specific conditions

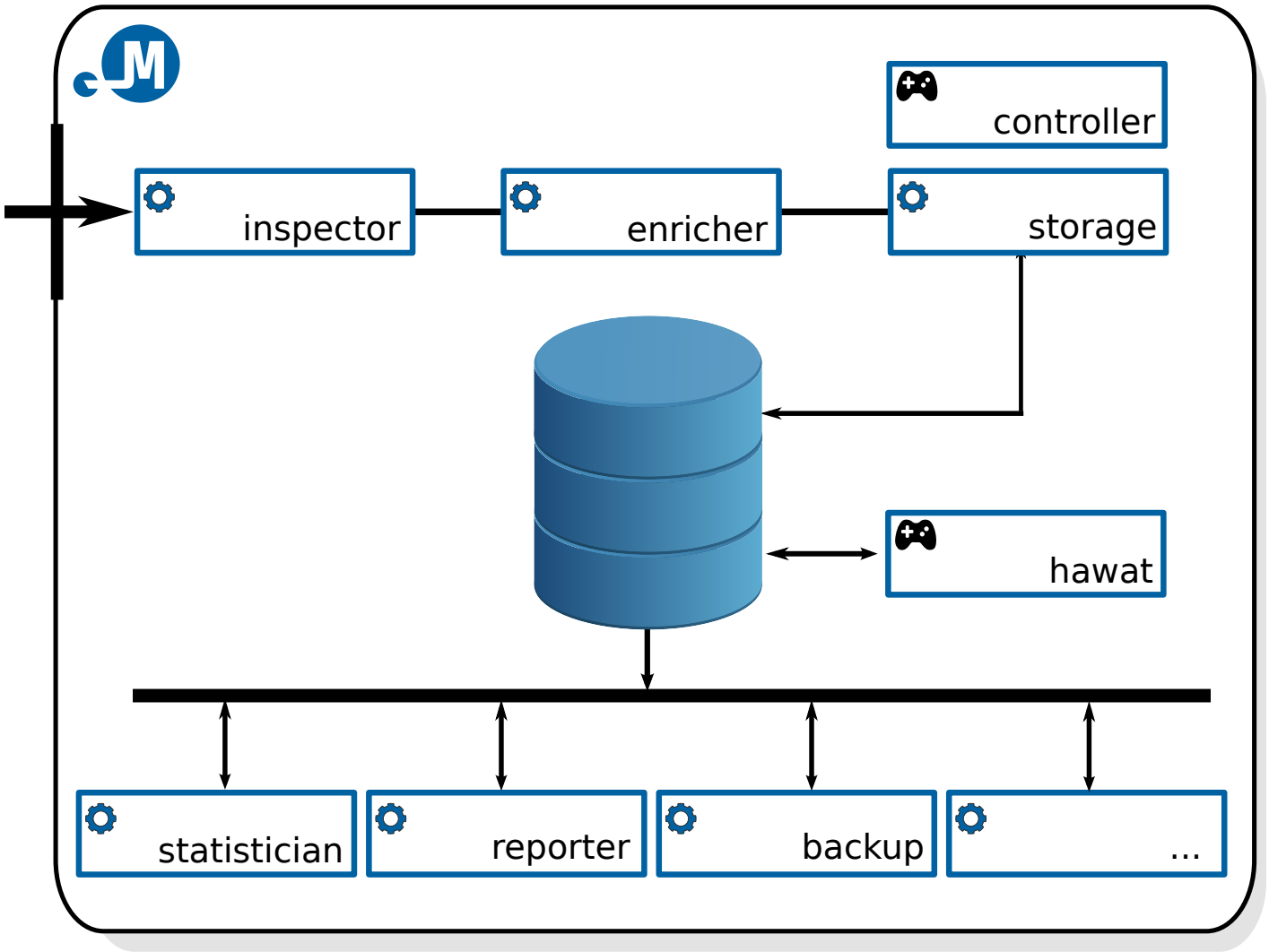
Architecture [1]



- Implementation language: Python3
- Data model: IDEA
- Data storage: PostgreSQL
- Network communication protocol: Warden

cesnet

Architecture [2]



Agenda

cesnet

Latest news

- Released version 2.1.x (Thu Sep 27 2018)
- Migrated completely to Python3
- Migrated database to PostgreSQL
- Automated build system Alchemist
- Autogenerated documentation
  - migration from 0.4.20
  - upgrading from 2.0.x
- Public Git code repository and issue tracker

cesnet

Alchemist build system

`https://alchemist.cesnet.cz/`

- Automated build system for Mentat and related libraries
- Contents:
  - General information
  - Build environment settings
  - Testing, linting, benchmarking
  - Autogenerated documentation
  - Git repositories
  - Debian packages
  - Python wheels
- Possible improvements:
  - Installation tests, functional tests
  - Documentation history
  - Automated changelogs, repository stats

cesnet

Agenda

cesnet

Libraries

- Utils: `geoip2`, `ply`, `rrdtool`, `psycopg2`
- Web: `Flask`, `Jinja2`, `Babel`, `WTForms`, `SQLAlchemy`
- idea-format: Library for working with IDEA messages
- pynspect: Data filtering library
- pyzenkit: Application development framework

cesnet

System modules

- Real-time event processing modules
  - mentat-inspector (classification and validation)
  - mentat-enricher (whois, geoip)
  - mentat-storage
- Event post processing modules (via database)
  - mentat-reporter
  - mentat-statistician
  - mentat-informant
  - (management scripts)
- Control modules and user interfaces
  - mentat-controller
  - Hawat

cesnet

Hawat: Web interface

- Implemented using Flask, Jinja2, Babel, SQLAlchemy and Mentat frameworks
- Modularization using Flask blueprints
- Customized Flask classes for deeper integration
  - View classes for common tasks (item management, searching, ...)
  - Application menu, item context menus, ...
- Read Flask‘s documentation!

cesnet

Agenda

cesnet

Essential resources

- Homeproj: Project issue tracker
- Primary code repository
- Official documentation
- Alchemist: automated build system

cesnet

Additional resources

- Project Mentat: official website
- Project Warden: official website
- IDEA: official website
- PostgreSQL: official website
- Sphinx: official website

cesnet

Thank you for your attention

Jan Mach
Jan.Mach@cesnet.cz