

# Deltares

# Deltares



# Deltares

## **Delft-FEWS**

### **Break-out Security & Cloud**

Rudie Ekkelenkamp  
Gert-Jan Schotmeijer

9 november 2022

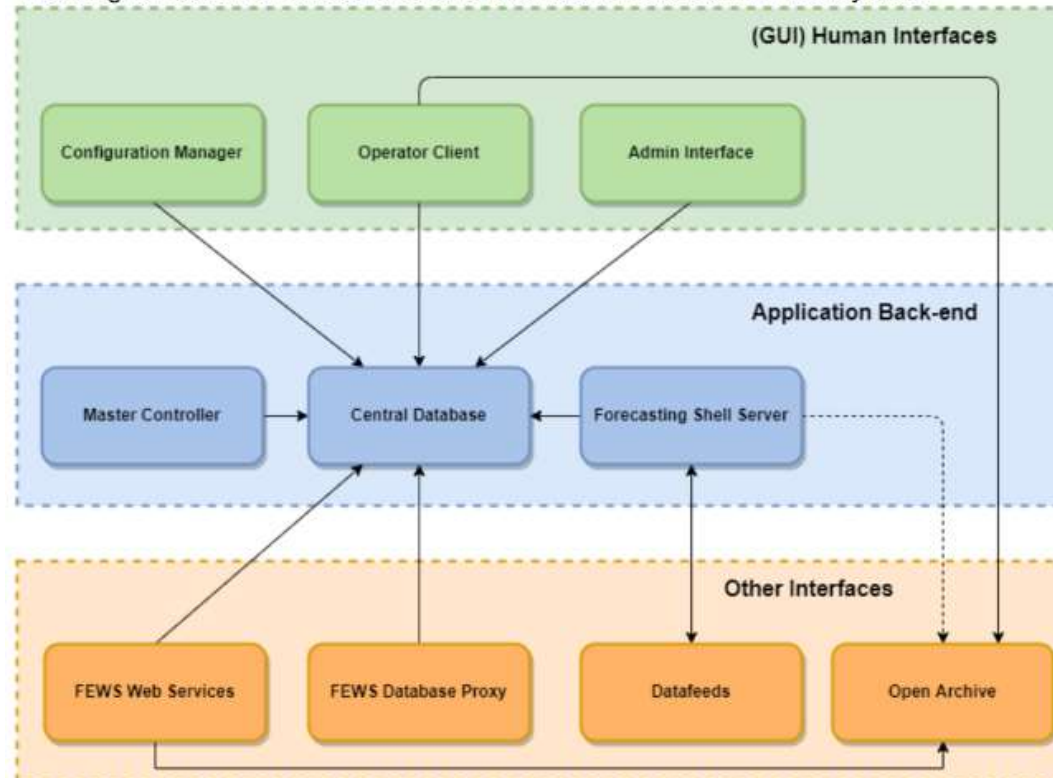
# Outline break-out

## Security

- Intro
- Current status
- Desired & planned developments
- Recent developments & demo (Cloud & Security)
- Q&A /possible demo

# General set-up and components Delft-FEWS

The diagram below shows a functional overview of the Delft-FEWS system.



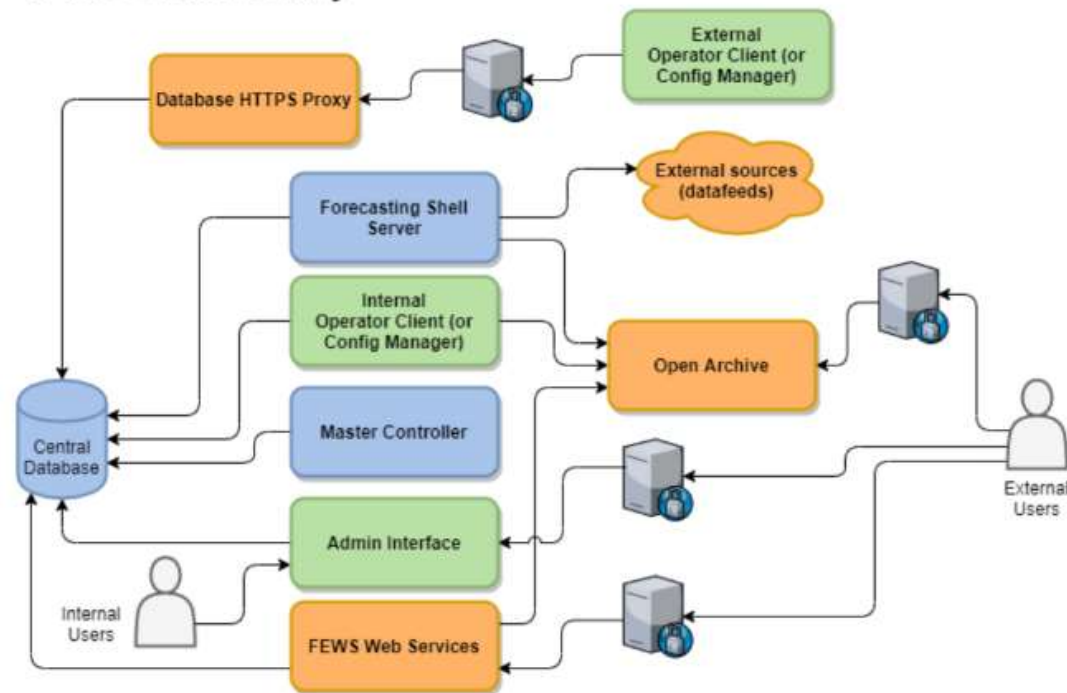
Note that in this diagram the *FEWS Database Proxy*, *FEWS Web Services* and the *Open Archive* are optional components.

Credits: André Speelmans

# General set-up and components Delft-FEWS

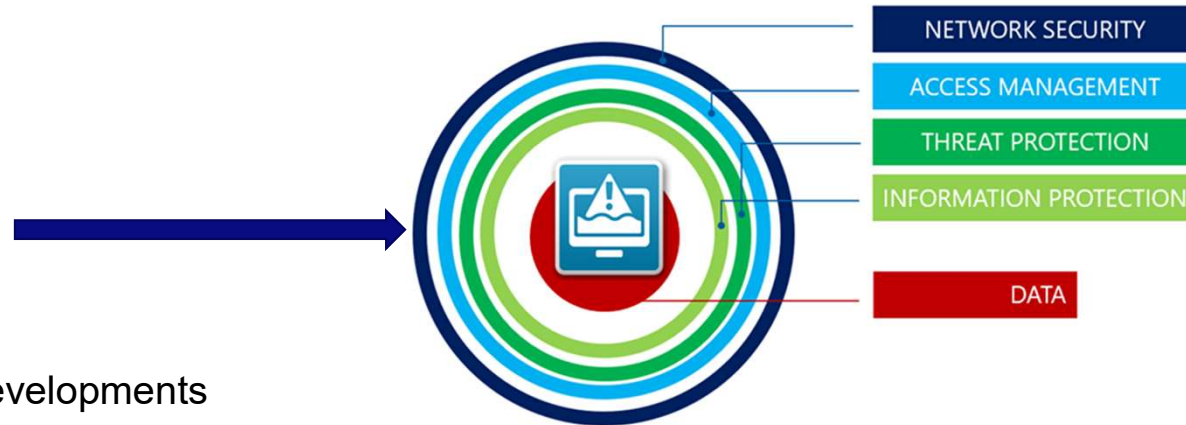
The diagram below shows the different connections between the components.

## FEWS Connectivity



# The approach

- ASSESSEMENT
  - Process
  - Security categories
- ROADMAP
  - Desired/required developments



# Security Roadmap

DRAFT

Delft-FEWS security guide  
Edition Q2

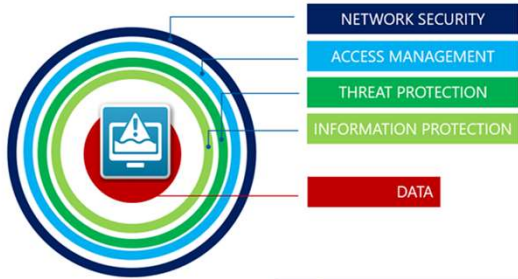


Deltares

Deltares

Delft-FEWS Security Documentation per Delft-FEWS component

1. Forecasting Shell Server  
The forecasting shell server has two outgoing connections (database and archive) and one incoming connection. Both the incoming and outgoing connections can be encrypted with TLS version 1.3. With the remark that the external data feed needs to support encrypted network traffic.
- A. Encrypted network traffic  
Network traffic to be encrypted using parties offer an
- B. Port security  
Outgoing connections  
-Central Database:  
-Open Archive(BDB)  
-Open Archive(BDB)  
-External sources
- C. Access 1. For  
There are no incoming port based addresses (of the 1
- D. MFA  
The Forecasting shell applicable. MFA is
- E. Role Based Access  
Role based access
- F. Access User  
The Forecasting shell
- G. OpenID Connect  
OpenID Connect is
- Delft-FEWS Security Documentation per Delft-FEWS component
- H. Access Audit Trail  
The Forecasting shell server has no log-in option, so there is no access audit trail on the Delft-FEWS component level of the user. On operation system level access audit trail can be configured.
- I. Change Audit Trail  
A change audit trail can be configured on operation system level. Uploads to the forecasting shell are logged to Admin Interface or Configuration Manager in the database of Delft-FEWS. The retention period of the logs is configurable.
- J. Session Time Out  
Session time out is not applicable.
- K. Encrypted storage  
Encryption of the data can be configured on operating system level.
- L. Recommended configuration  
We recommend running the Forecasting Shell Servers (with other FEWS components) in a separate network zone, allowing server access only to administrators and staff that needs to maintain model software on these servers. A firewall should prevent all unwanted incoming and outgoing network connections. The Forecasting Shell server should be running under a separate account.



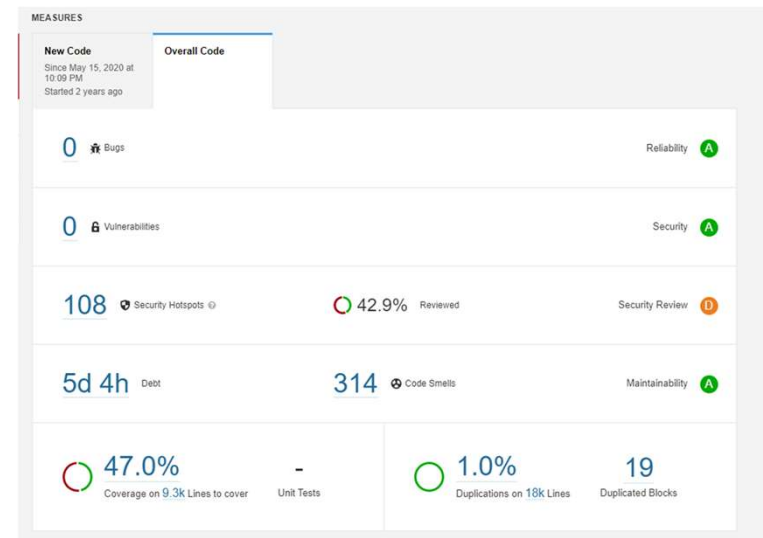
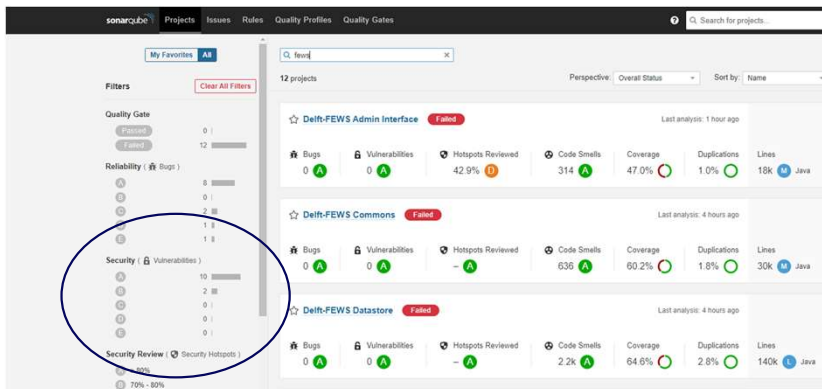
		Delft-FEWS security options per component										
		A. Encrypted network traffic	B. Port security	C. Access Delft-FEWS Component	D. MFA	E. Role Based Access (OS)	F. Access User	G. OpenID Connect (i.e. Azure Active Directory)	H. Access Audit Trail	I. Change Audit Trail	J. Session Time Out	K. Encrypted storage
BE	1. Forecasting Shell Server	✓	✓	IP-address Port-level	N/A	✓	N/A	✓	N/A	✓	N/A	✓
BE	2. Database	✓	✓	IP-address Port-level	N/A	✓	Role based	✓	✓	✓	N/A	✓
	3. Master Controller	✓	✓	IP-address Port-level	N/A	✓	N/A	✓	N/A	✓	N/A	✓
	4. Admin Interface	✓	✓	IP-address Port-level	✓	✓	Role based	✓	✓	✓	✓	✓
	5. Operator Client	✓	✓	IP-address Port-level	✓	✓	Role based	✓	✓	✓	✓	✓
	Configuration Manager	✓	✓	IP-address Port-level	✓	✓	Role based	✓	✓	✓	✓	✓
	Archive server	✓	✓	IP-address Port-level	N/A	✓	✓ *	✓	✓ *	✓ *	✓	✓
	Database proxy	✓	✓	IP-address Port-level	N/A	✓	✓ **	✓ *	✓ *	N/A	✓	✓
	Web services	✓	✓	IP-address Port-level	N/A	✓	Role based	✓ *	✓ *	✓	N/A	✓
	Datafeeds	✓	✓	IP-address Port-level	N/A	✓ ***	N/A	✓ ***	N/A	N/A	N/A	N/A
	Work End	✓	✓	OS level and Delft-FEWS level	✓	✓	N/A	✓	✓	✓	✓	✓
	Graphical User Interface	✓	✓	Available in Delft-FEWS	✓	✓	✓ **	✓	✓	✓	✓	✓
	Application Programming Interface	✓	✓	Needs special configuration	✓	✓	✓ ***	✓	✓	✓	✓	✓



# Security Control

Keep Delft-FEWS safe tooling & processes

- SonarQube
- OWASP dependency checker
  - ZAP



# Security Roadmap

Still work to do; security never stops

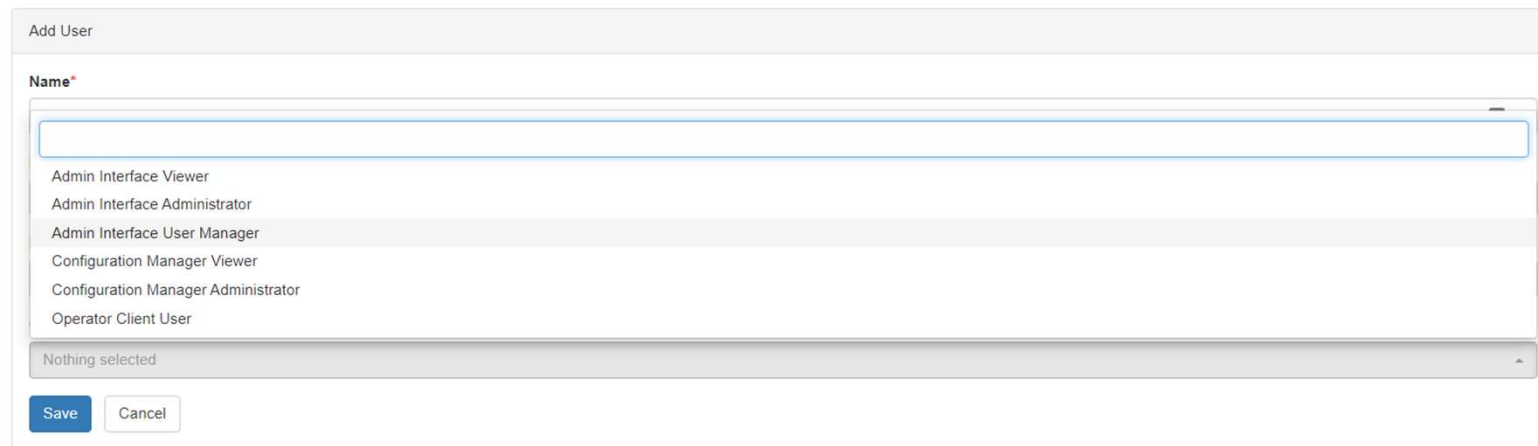
Main topics:

1. Gain insight on performance of the strict security measures
2. Audit trails
3. Improve insight vulnerabilities 3rd party libraries

# Some recent developments & demo & QA Rudie



# Admin Interface User Manager Role

- Admin Interface has a new group: AI\_USER\_MANAGER.
- Allow only user management actions in the Admin Interface



The screenshot shows a web-based 'Add User' dialog. At the top, it says 'Add User'. Below that is a label 'Name\*' followed by a text input field. A dropdown menu is open below the input field, displaying a list of roles: 'Admin Interface Viewer', 'Admin Interface Administrator', 'Admin Interface User Manager' (which is highlighted), 'Configuration Manager Viewer', 'Configuration Manager Administrator', and 'Operator Client User'. Below the list, it says 'Nothing selected'. At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

# Admin Interface User Manager Role

Delft-FEWS Admin Interface - Users

User Administration <

Users

Groups

Active Users

Active Services

Documentation <


Logout usermanager

Timezone: GMT

© Deltares

Build version: development\_2022.02 (116048)

Build date:02/11/2022 00:32



Filters

+ Add User

Show 10 entries

Search:

↻

User Name	User Display Name	User Email	Groups
admin	admin		Admin Interface Administrator
usermanager	usermanager		Admin Interface User Manager

Showing 1 to 2 of 2 entries

Previous 1 Next

# Open ID Support OC/CM and Database Proxy

Operator Client and Configuration Manager can login with Open Id when using the database proxy. No more database credentials required on the OC VM.

- New application role: OC\_USER required
- Admin Interface can map Open Id users to application roles or application roles can be mapped using OAuth2 claims (Azure AD).



# Delft-FEWS Web Services OpenID support

- Delft-FEWS Web Services can be protected using Open ID. Token claims can be mapped to Groups in the Delft-FEWS configuration. No more users in the UserGroups.xml. The Open ID app roles will be mapped to SystemGroups. See:
  - <https://publicwiki.deltares.nl/display/FEWSDOC/FEWS+Web+Services+Security+with+Open+ID+Connect>
- Will be possible to use with the Web OC.
  - <https://github.com/Deltares/fews-web-oc>
- Demo Web OC with openid login:
  - <https://delftfewsweboc.deltares.nl>

# Cloud info

- <https://publicwiki.deltares.nl/display/FEWSDOC/Delft-FEWS+and+the+cloud>



# Contact

 [www.deltares.nl](http://www.deltares.nl)

 [@deltares](https://twitter.com/deltares)

 [linkedin.com/company/deltares](https://linkedin.com/company/deltares)

 [info@deltares.nl](mailto:info@deltares.nl)

 [@deltares](https://www.instagram.com/deltares)

 [facebook.com/deltaresNL](https://facebook.com/deltaresNL)

