Current and future SDC security improvements

ONAP Joint Subcommittee Meeting · Antwerp, Belgium · September 26–27, 2019

Robert Bogacki <r.bogacki@samsung.com> · Samsung R&D Institute Poland

Agenda

- Pentest results and OJSI security issues
- HTTPS and certificates management
  - Development, testing and issues.
- Runtime generated certificates
- Cassandra issues
- Next steps
- Q&A

Why is it important?

- It is not only about security issues in SDC
- Problems faced during fixing security issues and learnings could be applied to any other ONAP components
  - E.g. runtime generated certificates
  - Cassandra issues
- El-Alto release is a right step into supporting platform maturity and stability but definitely not the last one

Pentest results and OJSI security issues

- Lack of HTTPS support (6)
- Exposed JDWP ports (5)
- Lack of proper user authentication (no password check, only user) (2)*
- Unsecured Swagger UI (1)
- No secured connection to Cassandra (1)*

* - still to be done

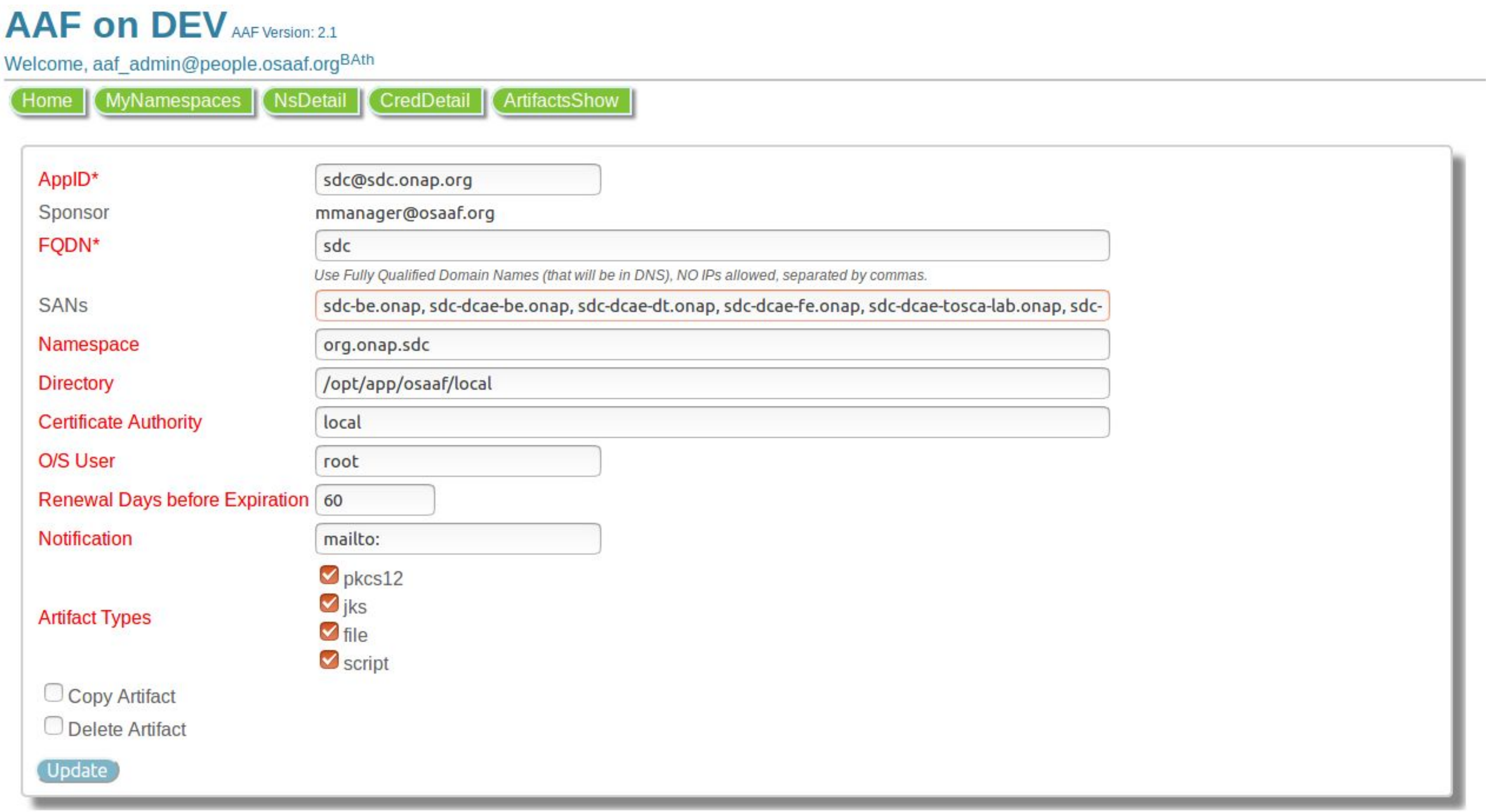
HTTPS and certificates management

Development

- Local development with SDC deployed as Docker containers
- AAF used for a certificates generation
  - Requires openvpn connection to the WindRiver Lab
  - Manual steps required to generate certificates signed by ONAP's Test CA: https://wiki.onap.org/display/DW/AAF+Certificate+Management+for+Dummies
  - Truststore and Keystore passwords decrypted locally (with AAF sample app)
- Portal changes
  - Development changes pushed as Docker images to the local Docker registry
- Changes to OOM. Local development and testing with Minikube.

HTTPS and certificates management

Certificates generation with AAF



AAF on DEV AAF Version: 2.1

Welcome, aaf_admin@people.osaaf.org BAth

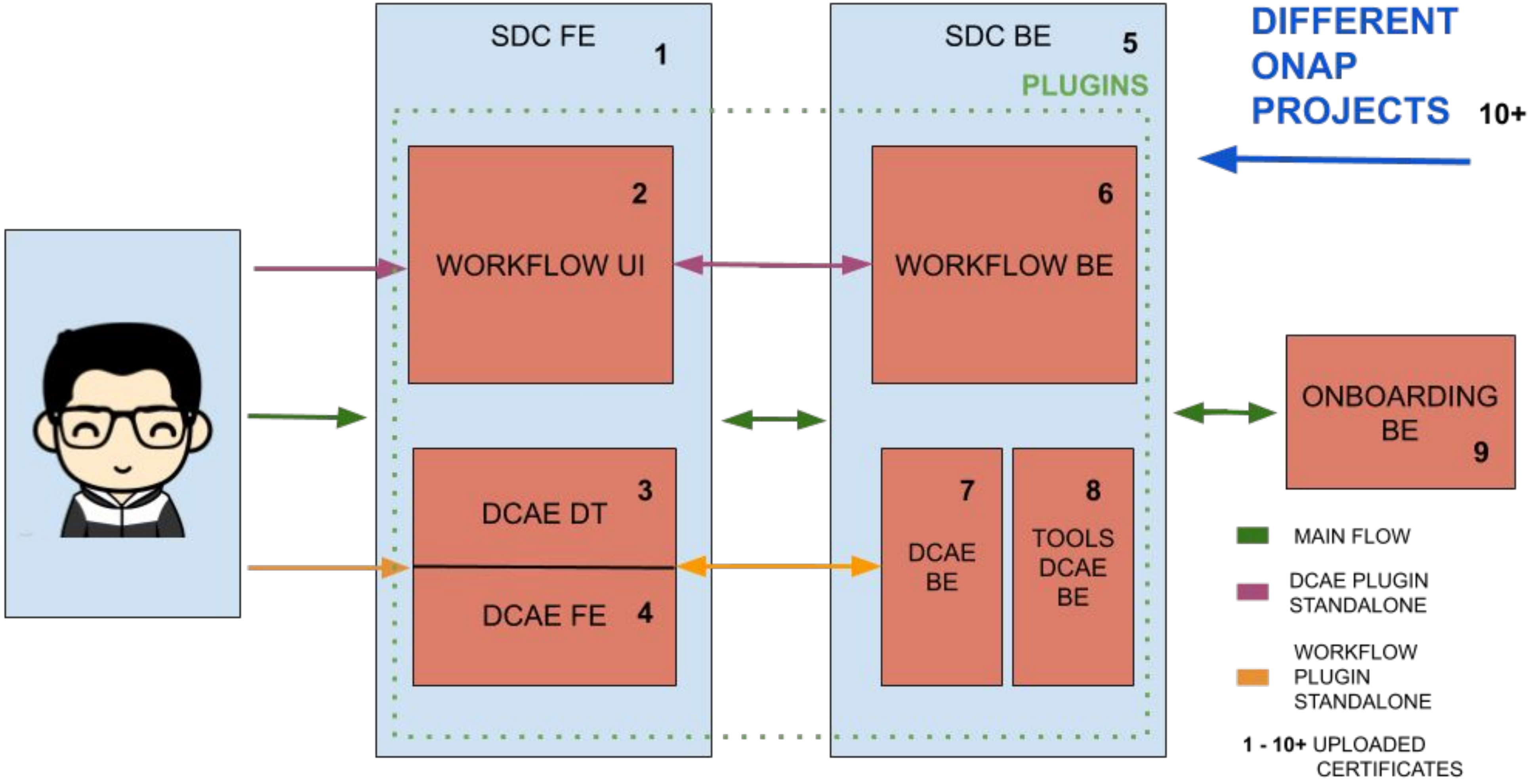
AppID*	sdc@sdc.onap.org
Sponsor	mmanager@osaaf.org
FQDN*	sdc *Use Fully Qualified Domain Names (that will be in DNS), NO IPs allowed, separated by commas.*
SANs	sdc-be.onap, sdc-dcae-be.onap, sdc-dcae-dt.onap, sdc-dcae-fe.onap, sdc-dcae-tosca-lab.onap, sdc-
Namespace	org.onap.sdc
Directory	/opt/app/osaaf/local
Certificate Authority	local
O/S User	root
Renewal Days before Expiration	60
Notification	mailto:
Artifact Types	☑ pkcs12 ☑ jks ☑ file ☑ script

□ Copy Artifact

□ Delete Artifact

HTTPS and certificates management

SDC structure



HTTPS and certificates management

Issues:

- Certificates spreaded all around. Not only in SDC repos.
  - Many commits for HTTPS support: SO, VID, AAI (~ 5) but in SDC (20+)
- Hardcoded Keystore and Trustore passwords available in repo

```
default['jetty'][:keystore_pwd] = "rTIS;B4kM]2GH"
default['jetty'][:truststore_pwd] = "Y,f975ZNJfVZh"
```

- Cadi filter not used for decryption of passwords
- Multi-domain AAF certificates (e.g. sdc-be.onap, sdc-dcae-be.onap, …) with Kubernetes ‘onap’ namespace
- Lack of enough description details in OJSI jira issues

Runtime generated certificates

- To get rid of manually generated certificates hassle it is recommended to use AAF Agent container
- AAF Agent is a container which uses HELM Charts to generate certificates before the application start
- On Volume accessible to the application:
  - Configure AAF property files
  - Use configuration to contact a running Certificate Manager
  - Generate Certificates signed by ONAP’s Test CA
  - Validate that the client works

More details:

https://wiki.onap.org/pages/viewpage.action?pageId=68540306

Cassandra issues

- Old common Cassandra version (2.2)
  - No support for encrypted and unencrypted connections at the same time.
    - Lack of “optional” flag in server_encryption_options
    - Update could affect other ONAP components
  - Related to Titan dependency in SDC which was already replaced with JanusGraph
- Old Cassandra Cqlsh clients not able to connect with SSL
  - Need for update to newer version

CSIT development

- SDC security hardening with CSIT
  - There is currently no good support in CSIT to setup privately built docker images for the testing
    - Existing scripts need to be privately hacked for local testing unless all the changes are already merged and available in upstream Nexus
- Sanity and UI sanity tests
- CSIT test case should test HTTPS
- Integration test case should be able to use HTTPS in ONAP CI

Future plans

- Use runtime generated certificates
  - Passwords decryption with Cadi filter
- Implement proper authentication
  - With Portal API or token based
- Upgrade Cassandra version and enable encrypted and unencrypted connection at the same time
- Development and improvements of CSIT tests
- Full support for http/https switch for development purpose (remove hardcoding from scripts)

Q&A

Questions?

Thank you!