DCAE Security Design & Assurance

DCAE Platform

Security Policy

Strive to improve the secure design principles across DCAE components.

DCAE components can be broadly classified between the DCAE platform and DCAE Services.

The DCAE Platform handles the control plane and manages the lifecycle of services. Inter-process communication within the platform components are TLS enabled by default. There is no sensitive data exposed by the platform component during processing. The communication between platform components are primarily through REST calls.

All external interfaces (exposed outside of clusters) are enabled as secure nodeport services. Both authentication/authorization are supported for such interfaces.

It's worth noting that as platform components handle application configuration and stores in Consul; the security of consul and data stored is not considered within application scope .

What You CAN Expect:

- We follow best programming practices. We test heavily, including unit-test, functional test, csit, gating. We follow ONAP standard process for building artifacts, e.g. when producing Docker images.
- We enforce a common shared database with access managed through secrets for individual application. OOM/Common modules are used wherever applicable to align with ONAP security requirements.
- We always use TLS by default for communication
- We use standard ONAP recommended base images for the majority of DCAE components
- All DCAE code is statically scanned by Nexus IQ and reports are published based on threat/vulnerability rating
- All DCAE component code is run through Sonar scans and reports are monitored periodically and addressed

What We DON'T Do (yet):

- We don't encrypt data stored in Consul.
- We don't allow specifying authorization for internal platform components

Supported Versions

https://wiki.onap.org/display/DW/Data+Collection+Analytics+and+Events

Reporting a Vulnerability

https://wiki.onap.org/pages/viewpage.action?pageId=84672487

DCAE Services

Security Policy

Strive to improve the secure design principles across DCAE components.

DCAE components can be broadly classified between DCAE platform and DCAE Services.

DCAE services are microservices that handle the collection, event-processing and analytics functions. These services are deployed largely based on end-user/operator usecases. The primary function of these services involves interfacing with Network functions, collecting fault/metrics event periodically and analyzing them to generate meaningful root cause actions for resolution.

The DCAE collector interface support multiple protocols (https/http/restconf/snmp/tcp/sftp/ftpes) depending on the type of VNF deployed. Different modes of authentication are supported: client certificate authentication, basic authentication, bearer token (e.g. JWT) authentication and no authentication.

All inter DCAE service communication is handled through ONAP/DMAAP services. As DMAAP is independent ONAP project, security of interface for DMAAP are outside scope of this project.

What You CAN Expect:

- We follow best programming practices. We test heavily, including unit-test, functional test, csit, gating. We follow ONAP standard process for building artifacts, e.g. when producing Docker images
- We enforce a common shared database with access managed through secrets for individual application. OOM/Common modules are used wherever applicable to align with ONAP security requirements.
- We always use TLS by default for external communication
- We use standard ONAP recommended base images for the majority of DCAE services
- All DCAE code is statically scanned by Nexus IQ and reports are published based on threat/vulnerability rating
- All DCAE component code are run through Sonar scans and reports are monitored periodically and addressed
- Component migration to use secure feed/topic feature

What We DON’T Do (yet):

- Only a handful of DCAE services currently use secure/dynamic DMAAP feed and topic, and most of the services currently use unauthenticated topics
- DCAE Components expect application configuration to be unencrypted, however certain configuration may require encryption/handling as K8s secret

Supported Versions

https://wiki.onap.org/display/DW/Data+Collection+Analytics+and+Events

Reporting a Vulnerability

https://wiki.onap.org/pages/viewpage.action?pageId=84672487