Proposed Container Logging Requirements

2021-02-22

Container logging requirements – event types
from VNF Security Requirements

[CON-LOG-REQ-1] The container and container application MUST log successful and unsuccessful authentication attempts, e.g., authentication associated with a transaction, authentication to create a session, authentication to assume elevated privilege. [Reference: R-54520]

[CON-LOG-REQ-2] The container and container application MUST log logoffs. [Reference: R-55478]

[CON-LOG-REQ-3] The container and container application MUST log starting and stopping of security logging. [Reference: R-13344]

[CON-LOG-REQ-4] The container and container application MUST log success and unsuccessful creation, removal, or change to the inherent privilege level of users. [Reference: R-07617]

[CON-LOG-REQ-5] The container and container application MUST log connections to the network listeners of the container. [Reference: R-94525]

[CON-LOG-REQ-6] The container and container application MUST log the addition and deletion of files in the container.

Container logging requirements – log data
from VNF Security Requirements

[CON-LOG-REQ-F6] the container application SHALL contextualizing the events (log enrichment)

e.g: Timestamp, IP address having generated the logs, user concerned, functionality concerned, error of application, detail of the error, all access to a resource, success of application, etc…

[CON-LOG-REQ-7] The container and container application MUST log the field “date/time” in the security audit logs. [Reference: R-97445]

[CON-LOG-REQ-8] The container and container application MUST log the field “protocol” in the security audit logs. [Reference: R-25547]

[CON-LOG-REQ-9] The container and container application MUST log the field “service or program used for access” in the security audit logs. [Reference: R-06413]

[CON-LOG-REQ-10] The container and container application MUST log the field “success/failure” in the security audit logs. [Reference: R-15325]

[CON-LOG-REQ-11] The container and container application MUST log the field “Login ID” in the security audit logs. [Reference: R-89474]

Container logging requirements – log management
from VNF Security Requirements

[CON-LOG-REQ-13] The container **MUST** have security logging for the container and container application active from initialization. [Reference: R-84160]

[CON-LOG-REQ-F1] Using systems and applications with native logging functionality is essential. This function MUST be taken into account during any design and development process.

[CON-LOG-REQ-14] The container **MUST** protect all security audit logs by standard operating system access control mechanisms, by sending to a remote system, or by encryption. [Reference: R-56920]

[CON-LOG-REQ-F4] Access to logs MUST be write restricted to a limited number of accounts with a need to know

[CON-LOG-REQ-F8] A disk partition MUST be dedicated to storing event logs on the equipment that generates them

[CON-LOG-REQ-F10] Access to logs MUST be write restricted to a limited number of accounts with a need to know

[CON-LOG-REQ-15] The container **MUST** detect when its security audit log storage medium is approaching capacity (configurable) and issue an alarm. [Reference: R-63330]

[CON-LOG-REQ-F9] An event log rotation policy MUST be formalized and implemented on all logging system equipment.

[CON-LOG-REQ-F2] It is recommended that no processing MUST be performed on the logs before they are transferred. (no classification, it is not the behavior of an application to define the categories of an event)

Note: this needs to be converted into a requirement

Container logging requirements – log management
from VNF Security Requirements

[CON-LOG-REQ-16] The container **MUST** support the capability of online storage of security audit logs. [Reference: R-41252]

[CON-LOG-REQ-F8] A disk partition MUST be dedicated to storing event logs on the equipment that generates them

[CON-LOG-REQ-17] The container **MUST** generate security audit logs that can be sent to Security Analytics Tools for analysis. [Reference: R-04492]

[CON-LOG-REQ-7] Logs MUST be automatically exported to a different physical machine than the one that generated them

Container logging requirements – log management
from VNF Security Requirements

[CON-LOG-REQ-18] The container **MUST** support the storage of security audit logs for a configurable period of time. [Reference: R-89474]

[CON-LOG-REQ-F9] An event log rotation policy MUST be formalized and implemented on all logging system equipment.

[CON-LOG-REQ-19] The container **MUST** be capable of automatically synchronizing the system clock daily with the Operator's trusted time source, to assure accurate time reporting in log files. It is recommended that Coordinated Universal Time (UTC) be used where possible to eliminate ambiguity owing to daylight savings time. [Reference: R-629534]

[CON-LOG-REQ-20] The container **MUST** have the capability to securely transmit the security logs and security events to a remote system before they are purged from the system. [Reference: R-703767]

[CON-LOG-REQ-F3] The container and container application **MUST** use the STDOUT for security logs collection [Reference: REQ-374]

[CON-LOG-REQ-21] The container **SHOULD** provide the capability of maintaining the integrity of its static files using a cryptographic method.

Propose to remove because this is a hardening requirement, not a logging requirement

Fabian Rouzaut Slides

Container logging requirements – log management

REQ for Developers:

- [CON-LOG-REQ-F1] Using systems and applications with native logging functionality is essential. This function MUST be taken into account during any design and development process.
- [CON-LOG-REQ-F2] It is recommended that no processing MUST be performed on the logs before they are transferred. (no classification, it is not the behavior of an application to define the categories of an event)
- [CON-LOG-REQ-F3] The container and container application MUST use the STDOUT for security logs collection [Reference: REQ-374]
- [CON-LOG-REQ-F4] Access to logs MUST be write restricted to a limited number of accounts with a need to know
  - See CON-LOG-REQ-14
- [CON-LOG-REQ-F5] It is recommended the container application SHOULD adopt a tree structure for the storage of event logs.
- [CON-LOG-REQ-F6] the container application SHALL contextualizing the events (log enrichment)
  - e.g: Timestamp, IP address having generated the logs, user concerned, functionality concerned, error of application, detail of the error, all access to a resource, success of application, etc…
  - See CON-LOG-REQ-7 – CON-LOG-REQ-11

Container logging requirements – log management

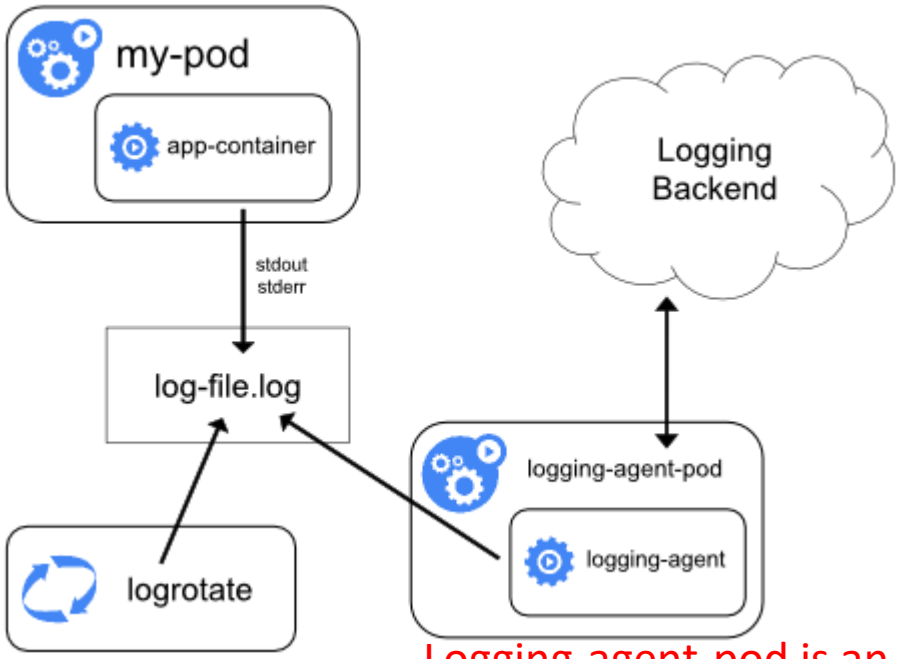
REQ for Developers:

- [CON-LOG-REQ-12] The container and container application MUST NOT include an authentication credential, e.g., password, in the logs, even if encrypted. [Reference: R-04982]
  - See CON-LOG-REQ-12
- [CON-LOG-REQ-XX] The container and container application MUST NOT include a sensitive information in the log
- [CON-LOG-REQ-6] The container and container application MUST log the modification of configuration files.
- [CON-LOG-REQ-1] The container application MUST log successful and unsuccessful authentication attempts, e.g., authentication associated with a transaction, authentication to create a session.

Container logging requirements – log management

REQ for infra:

- [CON-LOG-REQ-7] Logs MUST be automatically exported to a different physical machine than the one that generated them



Logging-agent-pod is an example

Container logging requirements – log management

REQ for infra:

- [CON-LOG-REQ-F8] A disk partition MUST be dedicated to storing event logs on the equipment that generates them
- [CON-LOG-REQ-F9] An event log rotation policy MUST be formalized and implemented on all logging system equipment.
  - See CON-LOG-REQ-15
- [CON-LOG-REQ-F10] Access to logs MUST be write restricted to a limited number of accounts with a need to know
  - See CON-LOG-REQ-14
  - Duplicates CON-LOG-REQ-F4