E-vote 2011
Auditing Architecture

V 1.6

Change history

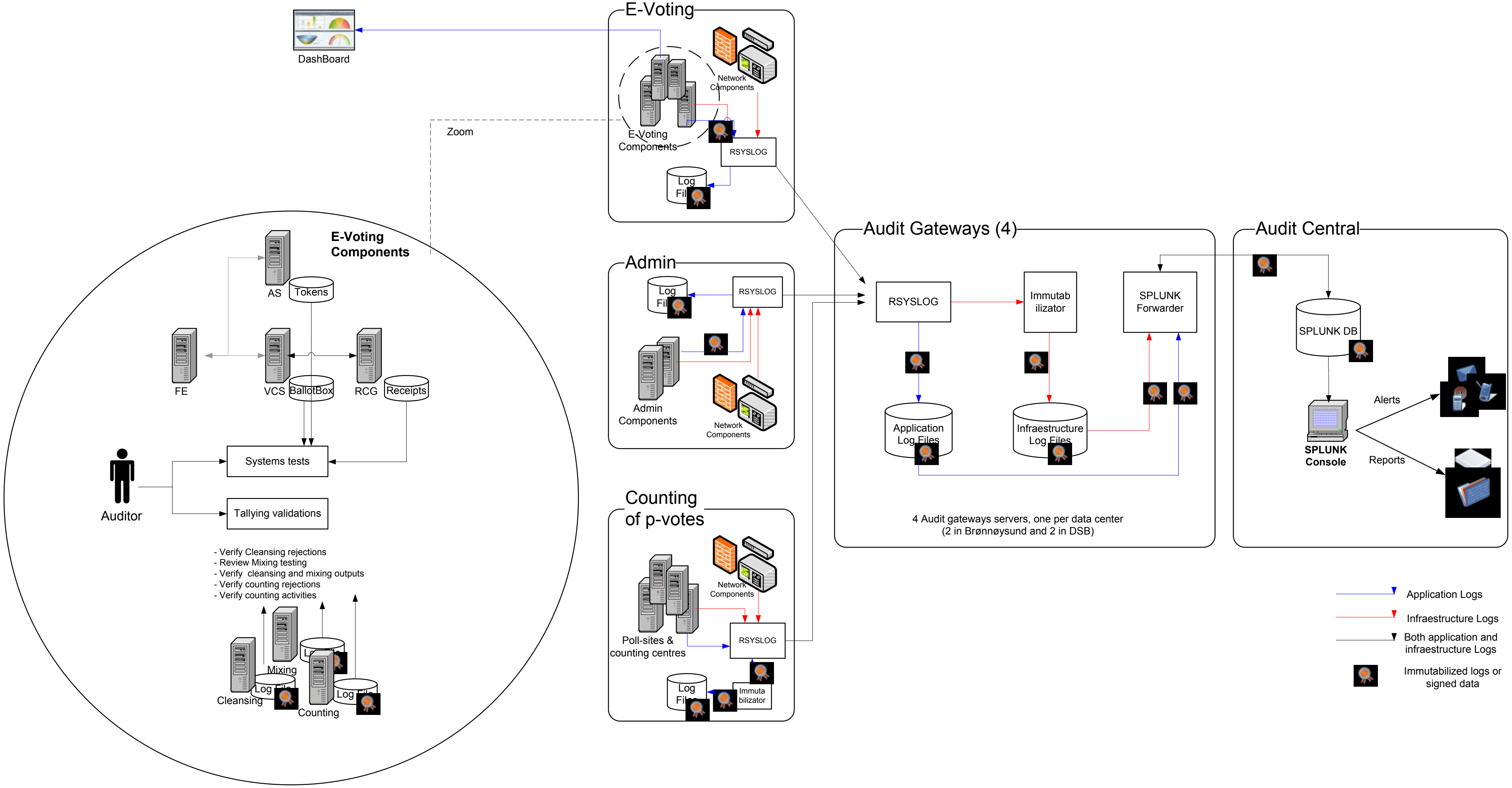
Date	Version	Description	Author
24.09.2010	1.0	Initial	SCYTL R&D
03.12.2010	1.5	New version considering SPLUNK installation	SCYTL R&D
03.06.2011	1.6	Reviewed version considering SPLUNK forwarder instead of RSYSLOG from gateways, and detailing log-alert categories.	SCYTL R&D

Approval

Approved by	Role	Sign	Date
Svein Endresen	Project Manager		22.03.2011
Svein Winje	Technical Architect		22.03.2011
Dan Sørensen	Customer		

Contents

1. Auditing Solution Diagram



2. Auditing Solution Rationale

For the Auditing Architecture, the following processes have been considered:

- **Logs Generation**.
  - Application Logs. The applications will be registering at the application logs, the critical and important events for application monitoring (having in mind security in front of attacks, data and election integrity, service availability, and election traceability requirements).
  - Infrastructure Logs. All components shall be configured to register logs for every security incidence (operating systems, databases, web servers, application servers, firewalls, IDS's, routers…).

  The log formats, and events to be registered at logs, have been defined in a separate document (excel file).

- **Logs Collection**. All log files are collected through the RSYSLOG protocol.
  For the logs collection, there are 4 log-gateways, one per datacenter (2 in Bronoysund and 2 in DSB). By this way, we are avoiding availability problems in the Central-Audit, and keeping a backup for the logs data. These four log-gateways are re-directing the logs to the Central-Audit Environment through the RSYSLOG protocol.

  The application logs are saved in the local machines where generated, and redirected to the log-gateway in its corresponding datacenter. From this log-gateway, the application logs will be re-directed to the Central Audit Environment through SPLUNK Forwarders.

  The infrastructure logs are generated by itself, and send to the local logs-gateways where are saved and redirected to the Central Audit Environment.

  * As exception, the logs from the firewalls and IDSs will be collected and analyzed directly by specific tools for network security monitoring.

- **Logs Protection**. All the logs have to be protected through the "Immutable Logs" mechanism, which is ensuring the integrity of the log information. To achieve this, there are three different scenarios:

  - Application logs are being generated in a secure way (immutabilized) directly by the application which is generating the logs.
  - Scanning Centre application logs. These log files are being generated by workstations instead servers, so the immutabilization process is not being performed by the application. The immutabilization is done by the "immutabilizator module" when the log files are processed by the RSYSLOG protocol.
  - Infrastructure. All components shall be configured to register logs for every security incidence (operating systems, databases, web servers, application servers, firewalls, IDS's, routers…). Logs coming from the infrastructure components are

- **Logs monitoring**.
  The central audit which is receiving all the logs will be running SPLUNK application, for logs monitoring and alert raising.

  We can consider 3 different types of alerts:
  - Direct alerts. This is a simple alert detection coming from a simple log entry. It involves having a very important log entry or a very critical error, which is raising an alert just when the message is received.
  - Threat Patterns security alerts. Advanced alerts generated by analyzing several logs entries which can be related, or a repetition of events which are not an alert on an individual treatment but yes on a group treatment.
  - Alerts from the audit functionalities. Alerts generated by analyzing the logs of the audit functionalities (both auditor manual requests as internal and automatic self-test process).

  There have been considered four alerts categories:
  - CRITICAL. This alert is related to an error which can be affecting to the related service or affecting the security. It would be necessary to evaluate each different message, but it would probably request some kind of intervention.
  - WARNING. This is a message indicating that something could be going wrong. There could be several minor errors, or a security attack could be starting. These alerts need to be investigated in order to decide if a corrective action is required.
  - MILESTONE MESSAGE. Initially, a milestone message is a relevant message which is normal to be received inside the usual flow of operations (e.g. the application is starting, or the ballot box is being exported at the end of the election). However, if this "normal" message is not being expected, then it can be considered like a critical message.
  - INFO. This alert is not related an error or an attack; it is an information message for administrators, operators, or auditors. The analysis of this information will decide more exhaustive verifications or any other action.

- **Monitoring Dashboard**. A web-dashboard will be implemented to monitor the status of the Ballot Box (number of votes mainly).

- **Logs Reporting**. SPLUNK monitoring console enables the possibility of performing advanced searchs and reports, in order to construct logs reports. These reports can be used as monitoring tool, as well as a input for the audit activity.
  Specific reports have been pre-generated with most interesting events.