SECOND EUROPEAN CONFERENCE ON EARTHQUAKE ENGINEERING
AND SEISMOLOGY, ISTANBUL AUG. 25-29, 2014

REDUNDANT DATA CENTER CONFIGURATION AND FAILOVER PROCEDURE FOR REAL-TIME SEISMIC NETWORKS

Mathias FRANKE[1], Stefan RADMAN[2], Toufik ALLILI[3]

We will discuss the experience gathered with deploying and configuring redundant data centers with automatic failover for real-time data acquisition, processing and storage of seismic networks. As solutions of intra-data center redundancy is rapidly progressing to virtual machines moving between two or more servers, such solution for inter-data center redundancy is currently hampered by bandwidth limitation of Wide Area Network (WAN) connections between the primary and secondary location. A successful implementation of a secondary data center with automatic failover capacity can be divided in six phases: i) normal operation; ii) failure detection of hardware or application; iii) failover procedure; iv) "fencing" operation at backup data center; v) failback procedure; and vi) Recovery. Moreover, we need to differentiate between real-time processes and database processes because at any given time only one authoritative database can exist. Also, the system should provide copious amounts of time-tagged log messages as well as notifications to the operators during the failover procedure for forensic analysis of the incidence in terms of error description (i.e., What was the root cause?) and improvements of the failover procedure itself.

The system disposition should consider as many multiple communication links as possible including redundant network equipment. Experience shows that the main requirement for a functional primary-secondary data center pair is a reliable and well-designed communication network.

Finally, we are recommending: i) prepare written procedures to which the operators can fallback in the stressful situation of a major data center failure; and ii) schedule drills as dry runs and once a year exercise an actual failover.

Fig. 1 shows an example of the data flow of the primary data center during normal operation. Fig. 2 shows an example of the data flow of the secondary data center during normal operation. The grayed out processes will be started as part of the failover procedure. Starting certain processes at the secondary center should be kept to a minimum and well tested.

We are probing two different design approaches. One authoritative database replicated to the backup data center (e.g., same event IDs in all databases), where data processes may run but do not write to the database. The other mirrors all process including writing to the database at the backup database with different event IDs. The advantage of the latter case is that during the failover only the database ID-service needs to be shifted to the secondary center. However, besides the fact that the two databases will evidently diverge because of analyst intervention, it is possible that databases may contain slightly different results even for the automatic events.

These and other issues need to be addressed for a successful design of redundant data centers and a robust failover procedure.

[1] Manager Open Systems & Services, Kinemetrics, Pasadena, CA 91107, USA, mf@kmi.com
[2] Sr. ICT Engineer OSS, Kinemetrics, Pasadena, CA 91107, USA, smr@kmi.com
[3] Sr. Network Operator OSS, Kinemetrics, Abu Dhabi, UAE, toufi.allili@gmail.com

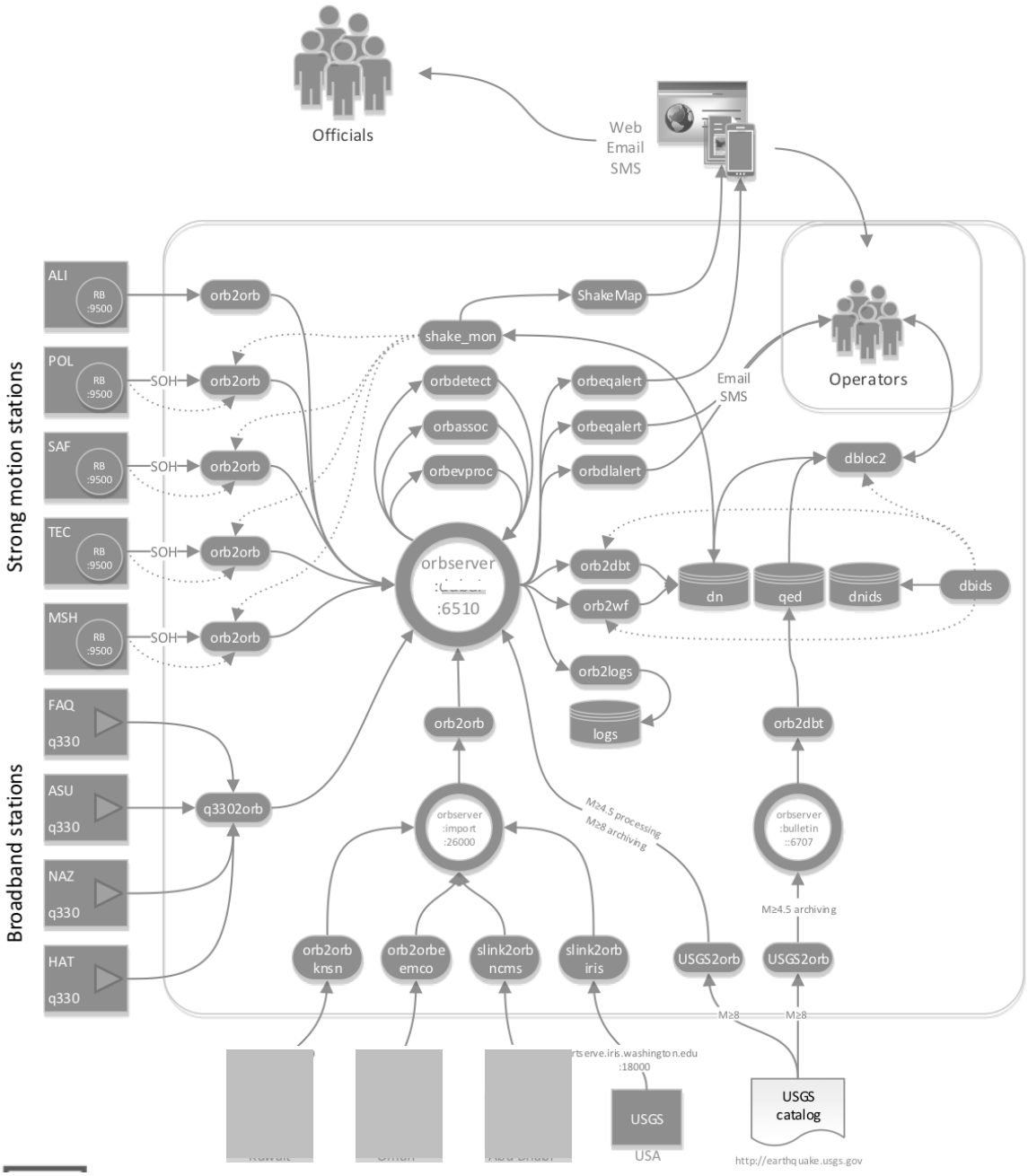

Figure 1. Antelope data flow at primary data center

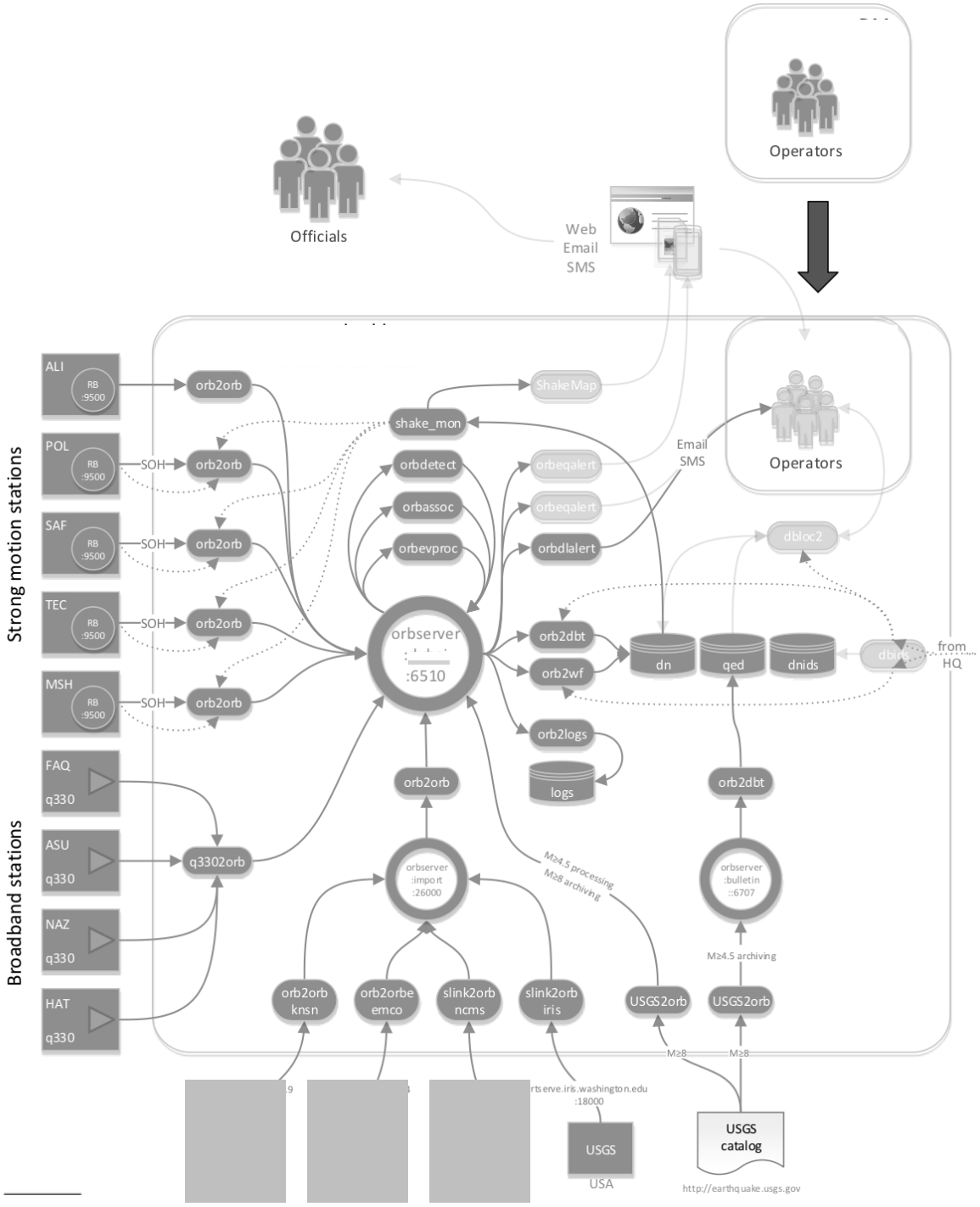

Figure 2. Antelope data flow at secondary data center