AMS - A Service for Turning Alerts into Messages

SEE-GRID-SCI eInfrastructure for regional eScience

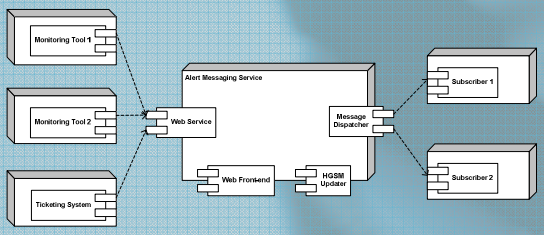
Highlights

- Service dedicated to notification of alerts from arbitrary monitoring tools
- Alert notification API accessible as web-service
- Web user interface for administrators and subscribers
- Message filtering and grouping
- To be used by SEEGRID infrastructure in the frame of SEE-GRID-SCI project, freely available for other applications

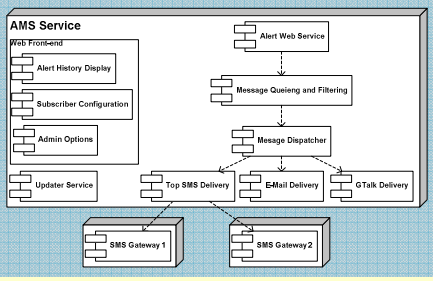
Overview

An infrastructural service designed to unify and simplify the process of sending and receiving different kinds of **alerts** in the **grid** (or some other) infrastructure. Alerts can be generated by various **monitoring** tools, **ticketing** systems etc. and dispatched to site administrators via **Jabber/GTalk** Instant Messaging, **e-mail** or some other transport mechanism. Subscriptions to alerts related to infrastructural elements define **filtering** and **aggregation** rules in order to avoid excess messages and false positives.

How it works



- Monitoring tools generate alerts
- AMS web service gets these alerts
- Senders are authenticated with their host certificates
- Subscribers, authenticated with their user certificates, define message creation rules
- Messages are created according to subscriptions
- Messages are filtered and aggregated
- Subscribers get resulting messages



Alerts

Generated by (monitoring, ticketing service, etc.) tools through the web service interface. Described by:

- sender – source of alert, typically a monitoring tool or ticketing system generating alerts
- target – affected administrative entity, e.g. grid site
- category –further specification target's element, service or event type (GOOD ticket, BBmSAM test, Nagios probe)
- subject – short description describing the alert (SMS content)
- body – detailed the alert text (e-mail or GTalk message body)
- isError – indication whether the alert is an error or positive status message

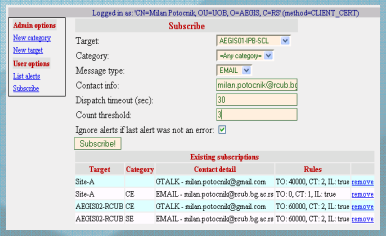
Web front end

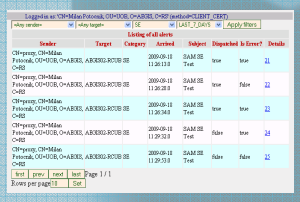
AMS administrator

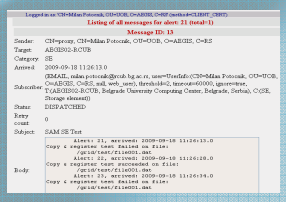
- Management of alert categories
- Management of targets

User (site administrator)

- Specification of rules for subscriptions
- History of alerts
- Messages produced by alerts







Messages

Users define rules transform alerts into messages. For each alert category and grid site, they define:

- Time limits and repetition counts used in alert filtering
- Message channels and addresses

Time-constrained filtering of repetitions and glitches:

- Customised by site administrators or individual subscribers
- Send only if a failure is repeatedly detected within a time window (without final recovery)
- Alert can be delayed until a specified number of errors is received during observation interval
- Repeated alerts received within the interval are aggregated into one message
- Message bursts (e.g. due to network or power problems) are avoided using sending delays and message aggregation

Message delivery: JavaMail API, Jabber GTalk API, SMS via GPRS/GSM modems or SMS gateways

Interaction with Grid infrastructure

Relation with other services

- The individual operational tools (Nagios, BBmSAM) act as web service clients
- Monitoring and control tools need to implement simple adaptors
- The already existing notification mechanisms, as OneOrZero e-mail generation, can be preserved as complementary tool-specific means of alerting
- Details of infrastructural changes are periodically obtained from HGSM (Hierarchical Grid Site Management)
- Delivering of SMS messages imposes additional technical and organisational requirements, may involve SMS gateways in several countries and should be postponed for after the usability evaluation

Effects on the infrastructure

- To be used by monitoring, ticketing and other operational tools to deliver alarms to site administrators
- "Push" instead of "pull" - reduces need for site administrators to constantly observe monitoring tools
- Should improve the response time for problems in infrastructure operation

SEE-GRID-SCI partners and communities

- Alerts from BBmSAM, Nagios, and helpdesk - collaboration with local developers of operational and monitoring tools
- SEEGRID infrastructure administrators
- Per-site configuration rules from HGSM

Other related usages

- Could also share message delivery with tools and services oriented towards users and jobs
- Additional user/job related use cases
- NRENs and NGIs could deliver network related alerts to their admins

Possible long-term developments

- Agents querying measurement archives using NM-WG schema
- Support for short lived entities (targets), like individual jobs, tickets, or issues
- Adaptation to additional messaging channels
- Enrichment of alert-to-message dispatching and filtering components

http://wiki.egee-see.org/index/Alert_Messaging_Service

Contact:
Dr. Branko MAROVIĆ branko.marovic@rcub.bg.ac.rs
Milan POTOČNIK milan.potocnik@rcub.bg.ac.rs

Belgrade University Computer Centre