An Alarms Service for Federated Networks

Charaka Palansuriya, Jeremy Nowell, Florian Scharinger, Kostas Kavoussanakis, Arthur S. Trew
EPCC, The University of Edinburgh, Mayfield Road, Edinburgh, EH9 3JZ, UK
Email: c.palansuriya@epcc.ed.ac.uk, j.nowell@epcc.ed.ac.uk, f.scharinger@epcc.ed.ac.uk, k.kavoussanakis@epcc.ed.ac.uk, a.trew@epcc.ed.ac.uk

Keywords:

Alarms, network monitoring, federated networks, Grid, Network Monitoring Working Group (NM-WG)

Introduction

Many Grid infrastructures, including the Large Hadron Collider Computing Grid (LCG), are composed of numerous federated networks distributed across the world. These networks can be heterogeneous and their managers may deploy different tools to monitor them and gather relevant data. Fundamentally, the monitoring data in federated networks belongs to multiple organisations. Access to the data is necessary to monitor the overall health of the networks. Our previous work [R1] has focused on providing access to federated network monitoring data, making use of standards developed by the OGF Network Monitoring Working Group (NM-WG) [R2]. During the course of this work it became clear that there was a requirement for alarms to be raised based on the network status. Grid and network operators need access to historical data to diagnose problems in the network, but more importantly they need alarms to notify them of such problems in a timely fashion. This paper describes an Alarms Service that is designed to monitor federated networks using standards-based access mechanisms. Such an alarms system will help network and Grid operators with timely trouble shooting of network problems.

The requirements for the Alarms Service described in this paper have been largely gathered from members of the Large Hadron Collider Optical Private Network (LHCOPN) [R3]. The architecture developed pays attention to sources of data such as those provided by perfSONAR [R4] and uses NM-WG to access the data. A prototype has been developed based on this architecture to obtain feedback from the network operators and other potential users.

Requirements

A list of prioritized alarm conditions were gathered from the operators of LHCOPN [R3]. The most important ones were determined to be:

1. **Routing Alarm**: If the path, as determined by traceroute [R5], changes and there are no light-paths down between the source and destination, then raise an alarm.
2. **Interface Congestion Alarm**: If a router interface drops packets at a rate above a threshold, whilst the link utilisation is below another threshold, then raise an alarm.

Further requirements for an Alarms Service were generated with the help of the LHCOPN [R3], Dante [R6] and WiN-Labor [R7]. In addition to the alarm conditions themselves, these include requirements [R8] that the status of the alarms MUST be accessible via a web-based dashboard, and that an alarm SHOULD display what action is to be pursued to solve the alarm. Users SHOULD be notified of alarms when they arise, for example via email. Another important requirement is that the alarm conditions as well as their threshold values MUST be configurable. Due to the distributed nature of the network monitoring data on which the alarms are raised, the alarm service MUST be able to access multiple data sources. The history of alarms SHOULD be available.

Architecture

The requirements led to the development of the architecture shown in Figure 1.

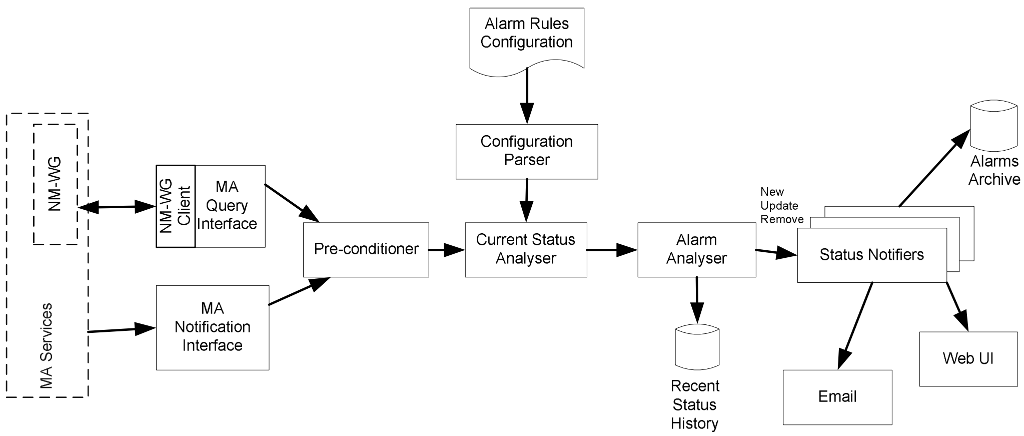

Figure 1: Alarms Service Architecture

The Alarms Service expects to utilise various external sources of network measurement data, known as Measurement Archives (MAs), shown in dotted lines in Figure 1. The data may be obtained from an MA on request via the MA Query Interface; or alternatively by allowing a data source to send status updates via the MA Notification interface. This latter case is especially interesting if the data source already does some processing of the underlying measurement data, and is able to determine if there is a problem. The data received by the MA Query Interface and the MA Notification Interface is fed into the Pre-Conditioner component for cleaning the data. The Pre-Conditioner performs various tasks such as removal of any *outliers* [R9] (i.e., a single measurement can be significantly off the norm and does not qualify for an alarm to be raised) and then presents data to the Current Status Analyser. The Current Status Analyser uses the cleaned up measurement data along with the configuration details (e.g., alarm conditions themselves and how often to analyse) to check whether an alarm condition has been reached. When an alarm condition is reached, the Current Status Analyser informs this to the Alarm Analyser. The Alarm Analyser checks the Recent Status History store to detect whether it is a new alarm, if it was recently detected or if an existing alarm is not valid anymore. The Alarm Analyser can also be used to detect conditions such as *flapping* (i.e., when an alarm rapidly changes state between on and off). The Alarm Analyser informs registered notifiers about status changes (new, update or remove alarm). Multiple notifiers, implementing the Status Notifier interface, fulfil different purposes. Examples include: the archival of the alarm history in a database, the email notification of appropriate people about new alarms, and the display of the current alarm status on a web page.

The architecture is both flexible and extensible. It allows the use of multiple data sources, new alarm conditions via an alarms configuration file, and different notification mechanisms (e.g., SNMP traps).

Prototype

In order to get early feedback from the LHCOPN and others, a prototype has been produced. Essential Alarms Service components have been developed, with limited functionality, in Java. The prototype is capable of monitoring the Routing Alarm condition as well as the Interface Congestion Alarm condition, these being the most urgent for the LHCOPN. It displays alarms on a web-based dashboard.

Conclusions and Future Work

An Alarms Service for monitoring federated networks has been introduced. The Alarms Service uses a flexible architecture to address the requirements gathered from the operators of such networks. The service uses an NM-WG standard interface to reduce the complexities of accessing monitoring data from heterogeneous sources. It is envisaged that with the adoption of the Alarms Service by underlying network infrastructures – such as the LHCOPN – large, federated, Grid projects such as LCG will benefit from smoother operations with timely troubleshooting.

At present, a number of enhancements are being made to the prototype to satisfy the essential requirements (e.g., addition of a configurable alarm definition framework). The plan is to use the service to monitor data and raise alarms in a number of sites in the LHCOPN when data become available, and then to improve the software based on experience and feedback.

Acknowledgements

We would like to thank: Dante [R6] for helping us with gathering requirements; LHCOPN [R3] for contributing requirements and providing useful feedback following the demonstration of the prototype; and WIN-Labor [R7] for help specifying the behaviour of the Alarms Service, providing prompt access to certain MAs and helping with related issues. This work is funded by the UK Joint Information Systems Committee (JISC).

References

[R1] Kavoussanakis, K.; Phipps, A.; Palansuriya, C.; Trew, A.; Simpson, A.; Baxter, R.; Federated network performance monitoring for the grid, Proceedings of 3rd International Conference on Broadband Communications, Networks, and Systems, 1-5 October 2006, San Jose, California, USA.

[R2] NM-WG 2008, https://forge.gridforum.org/projects/nm-wg)

[R3] LHC Optical Private Network TWiki, (https://twiki.cern.ch/twiki/bin/view/LHCOPN/WebHome)

[R4] Hanemann, A.; Boote, J.; Boyd, E.; Durand, J.; Kudarimoti, L., Lapacz, R.; Swanny, D.; Trocha, S.; Zurawski, PerfSONAR: A Service Oriented Architecture for Multi-domain Network Monitoring, Lecture Notes in

Computer Science, Volume 3826/2005,
(http://www.springerlink.com/content/f166672085772143/fulltext.pdf)

[R5] Gurun, S.; Szymanski, B.; Automatic Internet Routing Behaviour Analysis Using Public WWW Traceroute Service, (http://www.cs.ucsb.edu/~gurun/papers/brasil.00.pdf)

[R6] DANTE web site, (http://www.dante.net/server/show/nav.13)

[R7] WiN-Labor web site, (http://www.win-labor.dfn.de/)

[R8] RFC2119, (http://www.ietf.org/rfc/rfc2119.txt)

[R9] Holleczek, T.; Statistical Analysis of IP Performance Metrics in International Research and Educational Networks, Master's Thesis, Department of Computer Science, Friedrich-Alexander-University Erlangen-Nuremberg, 30 May 2008.

Author Biographies

Dr Charaka Palansuriya is an EPCC Applications Consultant. He has worked as a software developer or project leader on various Industrial and Open Source projects. These include the EGEE Network Services Development activity, BEinGRID and OGSA-DAI, as well as Digital Bridges and Altamira. He has a PhD in Mathematics and High Performance Computing (HPC) from the University of Greenwich.

Dr Jeremy Nowell is an Applications Consultant at EPCC, working primarily on large Grid infrastructure projects such as EGEE and DEISA. He has experience of a wide range of Grid technologies and middleware, and its application to High Performance Computing. His background is in Experimental High Energy Particle Physics, and he has a PhD from Imperial College London.

Mr Florian Scharinger is an EPCC Applications Consultant. He has worked on the EGEE Network Services Development activity, developing Web services for advanced bandwidth reservation and network performance monitoring tools. His main interests include High Performance Computing (HPC), Software Design and Architecture and also Test-Driven and Agile Development.

Mr Kostas Kavoussanakis is a Project Manager at EPCC. He manages technology transfer and research projects for academic and commercial clients of the Centre. He has experience of parallel software design and performance analysis of high-performance codes, and has managed various EC Framework V and VI projects, including the EUTIST-M cluster, BEinGRID and the EGEE Network Services Development activity.

Prof Arthur S. Trew is a Professor of Computational Science at the University of Edinburgh. He was a founder member of EPCC and has been its Director since 1995; in 2001 he helped establish the UK's National eScience Centre in Edinburgh and has been its Deputy Director since. He has lead roles in a number of UK national computational science projects, such as the HPCx and HECToR national HPC facilities.