EGEE-II

TROUBLE TICKETS EXCHANGE

THE ENOC EXPERIENCE

Document identifier:	EGEE-II-SA2-TEC-788081-TTexch-v0-3.doc
Date:	**29/01/2007**
Activity:	**SA2: Networking Support**
Document status:	**DRAFT**
Document link:	https://edms.cern.ch/document/78808/

Abstract: This document describes the experience of the ENOC in exchanging trouble tickets with various sources (mainly NREN and GÉANT2 NOCs). It will be used as a basis for starting the work to standardize Trouble Ticket exchange.

Document Log

Issue	Date	Comment	Author/Partner
0.4	2007-01-30	Adding "Informational" and "Supersedes" ticket type Details on link/equipment ID	Guillaume Cessieux (CNRS IN2P3)
0.3	2006-11-13	New version with minor modifications following Jean-Paul's comments	Jean-Paul Gautier, Mathieu Goutelle (CNRS UREC)
0.2	2006-11-10	Second Version following Toby's and GARR people's comments	Mathieu Goutelle (CNRS UREC), Toby Rodwell (Dante), Gloria Vuagnin, Giovanni Cesaroni, Claudia Battista (GARR)
0.1	2006-10-12	First version	Mathieu Goutelle (CNRS UREC), Toby Rodwell (Dante), Guillaume Cessieux (CNRS IN2P3)

Document Change Record

Issue	Item	Reason for Change

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

1.1. PURPOSE

The purpose of this document is to capitalize on the experience of running the ENOC inside EGEE in order to establish the requirements for a standardized format for exchanging Trouble Tickets between different organizations. Since the summer of 2005, the ENOC has been receiving tickets from a number of European NREN NOCs and the GÉANT2 NOC. From this most likely unique standpoint, we provide below the lessons learned to date.

1.2. DOCUMENT ORGANISATION

This document first introduces what the ENOC is and how its experience could help toward the development of a standardised Trouble Ticket exchange format. It then describes the different issues raised by the exchange of TT between various operational entities and finally provides some suggestions which may help this process to be performed more efficiently, accurately and easily.

1.3. APPLICATION AREA

This document applies to all the interested parties, mainly the SA2 activity, the TNLC members and all the NRENs involved in this action.

1.4. REFERENCES

Table 1: Table of references

R1: “Trouble Ticket Normalisation”, first TNLC meeting at EGEE’06, http://indico.cern.ch/getFile.py/access?contribId=54&sessionId=118&resId=0&materialId=slides&confId=1504
R2: “Common Trouble Ticket Schema”, first TNLC meeting at EGEE’06, http://indico.cern.ch/getFile.py/access?contribId=54&sessionId=118&resId=1&materialId=slides&confId=1504
R3: “NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist”, RFC 1297 http://www.ietf.org/rfc/rfc1297.txt
R4: “The Incident Object Description Exchange Format”, Internet Draft of the Extended Incident Handling Working Group, http://tools.ietf.org/wg/inch/draft-ietf-inch-iodef/draft-ietf-inch-iodef-10.txt
R5: “Requirements for the Format for Incident Information Exchange (FINE)”, Internet Draft of the Extended Incident Handling Working Group, http://tools.ietf.org/wg/inch/draft-ietf-inch-requirements/draft-ietf-inch-requirements-08.txt
R6: “Trouble management function for ITU-T applications”, Recommendation X.790, http://www.itu.int/rec/T-REC-X.790-199511-I/e
R7: TeleManagement Forum, http://www.tmforum.org/
R8: “JSR 91: Operations Support Systems Trouble Ticket API”, http://jcp.org/en/jsr/detail?id=091

1.5. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors.

1.6. TERMINOLOGY

This subsection provides the definitions of terms, acronyms, and abbreviations required to properly interpret this document. A complete project glossary is provided in the EGEE glossary http://egee-jra2.web.cern.ch/EGEE-JRA2/Glossary/Glossary.html.

Definitions

CC-IN2P3	Centre de Calcul de l'Institut National de Physique Nucléaire et de Physique des Particules – French Regional Operational Centre and French Tier 1.
GÉANT2	Pan-European Network interconnecting the European NRENs

Glossary

CSIRT	Computer Security Incident Response Team
E2E	End to End
ENOC	EGEE Network Operational Centre
FTE	Full-Time Equivalent
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ML	Mailing List
MIME	Multipurpose Internet Mail Extensions
NOC	Network Operational Centre
NREN	National Research and Educational Network
RFC	Request For Comments
TT	Trouble Ticket
XML	Extended Markup Language

2. INTRODUCTION

The EGEE Network Operational Centre (ENOC), as the network support entity of the EGEE infrastructure, has been set up to provide an operational interface with network providers. Besides the internal network support provided to the users and the support entities inside EGEE, the ENOC is also the entity relaying operational information from each single domain NOCs to the EGEE infrastructure. As such, the ENOC gathers a large amount of data, such as Trouble Tickets, which are received by emails.

A first ENOC prototype was launched in the summer 2005 and operated until the summer 2006. At that point, with the switch to the second phase of EGEE in April 2006, the ENOC became fully operational. The ENOC is now staffed with 2 FTE (split between 5 individuals located in Lyon in CC-IN2P3).

From an initial base of two network providers who participated in the prototype, The ENOC now has relationship with 10 NRENs plus GÉANT2 (the pan-European network interconnecting the NRENs). During this period, the ENOC has received more than 18 000 emails corresponding to about 5 500 separate tickets. From all of this, the ENOC has gained a unique insight into trouble tickets: their content; their lifecycle (which differs from NREN to NREN); what the obstacles to a successful TT exchange are; what could ease such a process.

This document describes the various difficulties that the ENOC encountered and describes what could be done to ease the process of exchanging trouble tickets between different organizations.

3. THE LESSONS FROM THE TROUBLE TICKET EXCHANGE

Managing the trouble tickets received from various NRENs is difficult. The major problem for the recipient is to understand completely, reliably and accurately the information enclosed in the ticket. Considering the amount and the heterogeneity of the information received by the ENOC, this task becomes harder mainly because of:

- The different languages used in the different tickets (currently the ENOC dataset contains TTs written in 8 different languages);
- The number of character sets (character encoding) of the information sent and the often non-conformant MIME formatted mails received;
- The often non-specified time zone of the dates;
- The variety of minor modifications in the “fixed” field (status e.g.): “open” vs. “opened”, upper/lower case, differences in date formats;
- The amount of free text that is unparsable (or at least very difficult to parse).
- The location field is quite inaccurate, for instance when many paths are crossing the same geographical location/trench/duct/hut it is hard to know which services could be impacted or not. When it is noticed it is often as free text.

We have identified a subset of information that is common to all ticketing systems. The list of common fields is:

- An **unique identifier** that is necessary to follow the evolution of the ticket during its lifetime;
- The **start date & time** and the **end date & time** of the problem if applicable;
- The **status** of the ticket (e.g. opened, pending or closed);
- The **summary** of the problem (often one line of text in the email subject)
- A longer **description** (usually as free text).

The following information data are often but not always present:

- The type of the trouble (planned maintenance or incident).
- The impact of the trouble. This is often a free text filled by the operator and therefore difficult to analyze automatically.

Finally we remarked that the evolution of the status of the ticket may also be different across the ticketing systems. For example, in the case of a scheduled intervention, one can have tickets that start "Open", goes through some "Updates" (at least one when the maintenance really starts) and then get "Closed". Other may start firsts as "Maintenance" and be "Opened" only when the maintenance starts.

4. POSSIBLE IMPROVEMENTS

A possible solution to improve the ability to manage automatically the TTs [R1] when it is necessary to exchange them could be that all the TT providers agree on:

- The minimum information, in an agreed format, that should be present in all tickets;
- The information schema (how the information are represented);
- The evolution of the status of the ticket (what the different states and possible transition of a ticket status are);

We would also like to stress that the TT providers do not have to change their existing ticketing system. The only requirement is that is put in place a translator that can transform a ticket from the local format into the agreed common format. The operation of "normalizing" a ticket is of course necessary only for the subset of tickets that have relevance for other communities interested to exchange such data with the TT provider..

4.1. NECESSARY INFORMATION

From the ENOC experience, we have identified a set of data that forms a comprehensive description in a TT. Besides the (relatively) small set of common information already present (see section 3), the following information should be present in tickets:

- **Type:** A ticket concerns essentially two types of problems, the scheduled maintenance and the incident. Some variations around these two types can be envisaged, for instance types "Informational" or "Supersede". Informational tickets are related to non-network tickets sent to the tickets ML (change of TT systems, phone number of the NOC updated, ML account information) to take advantage of their spreading without bothering about further contingent software processing. The "Supersede" type allows replacing easily a ticket, which ID is provided, by another without closing the replaced. Then we know that new ticket is related to another that will no longer be updated. It can be used when different groups create duplicated tickets by mistake.
- **Location:** this information should give the equipment name and/or site of the provider. The possible values for this information should be agreed between the provider and the customer for the recipient to be able to infer the impact of the trouble on their own infrastructure. A way could be to have a Circuit ID/Equipment ID identifying uniquely parts of their infrastructure. If a provider does not want to expose its internal topology, it could provide for instance fictive ID.
- **Impact:** The recipient of the ticket should be able to know what is the foreseen impact of maintenance or the current impact of the incident (e.g. no impact, light performance impact, severe performance impact, no connectivity). Again, the possible values should be an agreed fixed list.

- **Date & time when the ticket has been opened and closed (if applicable):** these dates are different from the problem start and end date and may be relevant for both the customer and the provider to assess the global reactivity and efficiency of the operational system.

The **Summary** may be a short description, written in English, to be selected from a small defined set of possibilities (menu list). The **Description** of the trouble is maybe the only "free text" field that should remains. It should only give extra details that are not possible to include in all the other fields of the ticket.

4.2. TICKET FORMAT FOR EXCHANGE

The basic requirements [R2] for the exchange format should be extensible and upgradeable, should make use of established and inclusive technologies and standards, and adopt standard conventions.

In terms of flexibility, a suggestion is to have a marked-up schema rather than plain text (with key-value pairs). "Hard-coded" field-names should be avoided so that changes can be easily made. Instead, a key should be used for the field name and an attribute giving its description. The description can then be in different languages to allow localization of the ticket. The schema should also define for example the date format, the terminology. These definitions should come from adopted standards (RFCs, ISO, etc.).

A good candidate choice could be the XML technology. If an appropriate, publicly available, already defined information schema exists, then this should be used (after minor needed modifications). However, initial research suggests there is no such suitable, existing schema.

4.3. EVOLUTION OF THE TICKET STATUS

The ticket status often follows a simple evolution. It is opened. It may then be updated zero or more times, and finally it is closed. This is the preferred behaviour. The updates are of course not mandatory: in the case of planned maintenance, there will probably be a ticket update when the maintenance actually starts (or is postponed). For an incident, it is possible that no update occurs.

In some NOCs, the status evolution can differ slightly: for example, an NREN can announce a planned maintenance by creating a ticket with status "Maintenance". The ticket is then "Opened" when the maintenance starts and then it is closed. This kind of behaviour should be dropped in favour of the first described evolution plus a "Ticket type" field clearly stating if it is a scheduled maintenance or an incident.

5. RELATED WORK

We can find some initial thoughts (a "wishlist") in [R3] but this work seems a little old (1992) and the IETF User Connectivity working-group defunct. Within IETF, there is also some work [R4, R5] carried out by the Extended Incident Handling (INCH) working group on standardisation of the exchange of Trouble Ticket concerning Security incident, between Computer Security Incident Response Teams (CSIRTs). This is focused on Security Incidents but lessons can be learned from this activity.

Work in the field of standardisation of TT and of TT exchange can be found from the TeleManagement Forum [R7]. They're referring to an ITU recommendation X.790 [R6] on a TT standard format and also to a comprehensive Java API for TT exchange [R8].

These first references can serve as starting point for a common action: it can be taken as input or as a whole if the previous work is found to fulfil the requirements.