Project Acronym	**Fed4FIRE**
Project Title	**Federation for FIRE**
Instrument	**Large scale integrating project (IP)**
Call identifier	**FP7-ICT-2011-8**
Project number	**318389**
Project website	**www.fed4fire.eu**

D8.11 – Second Report on First Level Support (FLS)

Work package	WP8
Task	T8.1
Due date	30/09/2015
Submission date	23/03/2016
Deliverable lead	Toby Rodwell (GÉANT)
Version	1.0
Authors	Toby Rodwell (GÉANT) Akil Radhakrishnan (GÉANT)
Reviewers	David Margery (INRIA), Brecht Vermeulen (iMinds)

Abstract	This document describes the experience gained in First Level Support operations in the 12 months between October 2014 and October 2015 It analyses the operational data gathered during this period and summarises the lessons learned.
Keywords	First Level Support, Trouble ticket, Operations, Maintenance

Nature of the deliverable	R	Report	X
	P	Prototype	
	D	Demonstrator	
	O	Other	
Dissemination level	PU	Public	X
	PP	Restricted to other programme participants (including the Commission)	
	RE	Restricted to a group specified by the consortium (including the Commission)	
	CO	Confidential, only for members of the consortium (including the Commission)	

Disclaimer

The Fed4FIRE project received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no FP7-ICT-318389.

Executive Summary

This report analyses the activity of the First level Support (FLS) function of Fed4FIRE during the 12 month period from October 2104 to October 2015. FLS was defined at the start of the project and its initial requirements were fed in to the Architectural work of Fed4FIRE. The requirements led to the development of a dashboard that displays a standardised set of operational alarms from each of the test-beds in the federation. Using this dashboard, complemented with email alerts for the relevant alarms, the FLS team, in co-operation with Subject Matter Experts (SMEs) in the individual test-beds, manage faults detected in the test-beds. Incidents are logged in a Trouble Ticket System (TTS) which acts as a central repository for Fed4FIRE. It was originally envisaged that the FLS team would also use the TTS to log and track experimenters queries and issues however in practice the activity of assisting experimenters has been done using a simple e-mail list monitored by the test-bed SMEs and the project developers.

FLS collects operational data from the email notifications generated for dashboard events, and from analysis of Trouble tickets, and summarises it in a monthly operations report which is distributed within the project.

Experience of using the dashboard has led to the enhancement of its capabilities, in particular the auto-creation of tickets in the TTS based on e-mails auto-generated by the dashboard. The FLS service only operates for 8 hours a day during working days, whereas the e-mail notification is constantly available, so tickets are now created for events on a 24/7 basis. This has led to the generation of significantly more operational data regarding incidents, as it became apparent that only about 40% of issues arise during working hours. When ticket automation was first introduced there was an excessive number of new tickets created, as an intermittent fault would generate multiple tickets – this has been addressed and now repeat e-mails are associated with just one incident ticket.

994 dashboard-triggered tickets were created during the period under review, 21% of which were related to a lack of free resources (a condition which it is important test bed administrators are aware of, but is not normally indicative of a fault). There is a wide variety in the number of tickets created per test-bed, and also in the activity of test-bed Subject Matter Experts (SMEs), with some SMEs conscientiously updating incident tickets with reasons for outage, and other tickets auto-closing (after the alarm has cleared) without any additional information being added. To help and encourage SMEs to provide this information as efficiently as possible the ‘fault fix’ codes in the TTS are being expanded to give options relevant to Fed4FIRE test bed SMEs, so in future it will be possible to quickly and easily analyse the root causes of incidents.

Acronyms and Abbreviations

CET	Central European Time
FLS	First Level Support
SME	Subject Matter Expert
TTS	Trouble Ticket System

Table of Contents

1 Introduction.

Fed4FIRE is a federation of independent test-beds who have all implemented a common set of standards for experiment definition, monitoring and control. This enables experimenters to utilise multiple test-beds, of differing technologies, to create more complex experiments closer to real-life situations. Historically, prior to the federation the test-beds had relatively close contact with the own experimenters. The creation of the federation means that experimenters will not generally have a close relationship with the test-beds that they use. It also introduces operational issues related to the interaction between test-beds as well as the operation of the additional functionality provided by the federation itself.

All of these factors require a new approach to operational support for experimenters. The First Level Support Function (FLS) acts as a single, common point for the detection and management of operational incidents occurring on test-beds within the federation. Using a standard Trouble Ticket System (TTS), it logs these incidents and analyses them on a monthly basis.

This deliverable reviews the experience of operating FLS since October 2014. It analyses the data gathered as an assessment of the operational performance of the federation. On the basis of the lessons learned it details further improvements that can be made to FLS.

2 First Level Support (FLS)

First Level Support (FLS) provides the fault logging tools and resolution processes that underpin the operational support model of the federation. Figure (i) illustrates the positioning of FLS and its interactions with other functions within the federation

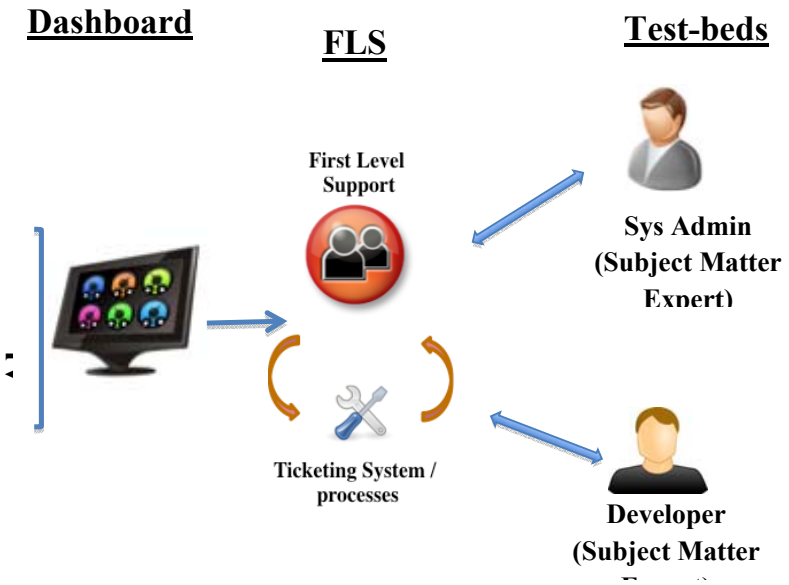


Figure (i) FLS and the Fed4FIRE federation

The key elements are as follows:-

1. **The Dashboard**. This provides a visual indication of the state of health of the test-beds within the federation. It is based on a polling function that regularly tests a number of key elements of each test-bed and displays the results in visual format for FLS operators. Figure (ii) shows a snapshot of the dashboard. The dashboard, which was based on the requirements set out in Deliverable D8.1, provides a Red/Amber/Green indication of alarms status. In August 2014 email notifications were introduced to complement the visual indication of the events.
2. **Trouble Ticket System (TTS).** The TTS is the database where all incidents are recorded. It represents the repository of incidents dealt with by FLS. Ticket automation was introduced in December 2015 using the email notifications from the dashboard. This has allowed logging faults on a 24/7 basis.
3. **Standard Operational Processes**. Issues must be handled in a consistent manner, and a given incident may be handled by a number of disparate people. For these reasons a strictly standardised approach to incident management is required. A guide for getting support and work flow of support are also available from http://doc.fed4fire.eu/support.html.
4. **Subject Matter Experts (SME's)**. FLS staff are generalists. Their main skill-set is in managing and resolving incidents. They do not have an in-depth knowledge of the

functioning of all the test-beds in the federation and in order to deal with test-bed specific issues an expert, familiar with the functioning of that particular test-bed, is needed. These 'Subject Matter Experts' liaise with FLS staff to manage the resolution of incidents. In order to ensure prompt and reliable access to this second line of expertise an escalation path is required. This is provided by iMinds (coordinating partner) and within the TTS a user ID ***default SME*** is used for this purpose**.** Issues that are not resolved in a timely manner by a test-bed SME are escalated to the default SME.

2.1 The Dashboard Function

The dashboard is a key tool for FLS to observe the behaviour of test-beds within the federation. For each test-bed it shows that status of a common set of key status indicators. Figure (ii) bellows shows the current version of the FLS dashboard. The indicators are

- **Ping Latency.** This tests the reachability of the test-bed from the Internet. It is expressed as a latency time. A test-bed, which is not reachable, is effectively disconnected from the federation.
- **Get Version Status.** This is the result of a Get version Status call to the Aggregate Manager Software of the test-bed.
- **Free Resources.** This is an indication of the availability of resources for experimentation. As such, it is not necessarily a critical indicator as far as incidents are concerned. There will be occasions when there are no free resources. It is nevertheless an aid in terms of diagnosing problems.
- **Internal Status.** This is an aggregate alarm based on the status of individual, test-bed specific, alarms.
- **Login Status.** This feature was introduced in June 2015 to indicate the node login status for the testbeds (done twice a day).
- **Monitor self test status:** This feature was again introduced in June 2015 to indicate the working status of the dashboard. This feature is discussed more in details in section 4.4.

Monitor Self Test Status: SUCCESS

Fed4Fire Testbeds

Testbed Name	Ping Latency (ms)	GetVersion Status	Free Resources	Internal Status	Aggregated Status	Login Status
BonFIRE	16.23	SUCCESS	0	SUCCESS	SUCCESS	SUCCESS
Bristol openflow	25.14	SUCCESS	6	SUCCESS	SUCCESS	SUCCESS
Bristol VTAM	31.34	SUCCESS	2	SUCCESS	SUCCESS	SUCCESS
C-Lab	52.04	SUCCESS	69	SUCCESS	SUCCESS	SUCCESS
ExoGENI NICTA	297.11	SUCCESS	20	SUCCESS	SUCCESS	SUCCESS
FUSECO	21.59	SUCCESS	34	SUCCESS	SUCCESS	SUCCESS

Figure (ii) Current version of FLS dashboard

FLS, which began full operational service in February 2014, provides service during central European working hours (9am-5pm CET) on working days, however since the introduction of ticket automation in December 2015, events are logged in tickets on a 24/7 basis.

With any IT system there is a need for scheduled maintenance, and for Fed4FIRE it is important that such maintenance is visible, in advance, both to experimenters and FLS,

otherwise experiments will fail and FLS will react to the consequences of scheduled maintenance as incidents rather than managing this incident as an expected outage. A maintenance calendar is therefore associated with the dashboard and is accessible from a link below the dashboard alarm status display. FLS receives e-mail notification of maintenance and this leads to the auto-creation of an appropriate maintenance ticket in the TTS. FLS also manage the entry of scheduled maintenance in the calendar.

2.2 Experimenters' List

A mail list is maintained by iMinds, to which Experimenters can post any problems they are experiencing. The list is monitored by SMEs from the participating test-beds who deal with the queries as and when they arise.

2.3 E-Mail Notification of Incident Reports

Until e-mail notifications were introduced the dashboard's visual indications were the primary source of incident reports for FLS. The FLS team did not (and does not) have a person dedicated to monitoring the display full time, rather the dashboard's visual indications were checked every 5 or 10 minutes, and this placed some limitations on the effectiveness of FLS - if alarms in adjacent fields changed colour (one from green to red, the other red to green) this could be difficult to spot, and short-lived incidents would leave no lasting record. Dashboard-generated e-mail notifications were first introduced in August 2014, meaning visual indications were supplemented by an e-mail generated when a new incident was detected. There was an immediate, significant increase in the number of reported incidents, partly because E-mails were triggered for all events, 24/7, not just non-transient events occurring during working hours, but also because of 2 other less desirable reasons.

i. Each separate change of state from normal to 'alarm state' generated an e-mail. A major failure of a test-bed will would typically generate multiple incident e-mails.
ii. When email notifications were first introduced, there was no matching e-mail created when an incident clears. This meant it was possible that intermittent faults would be registered as new event rather associating it with an existing event.

Because of these limitations, the e-mail notification was initially used only as an adjunct to visual monitoring, but in October 2014 FLS started using a new ticketing system, called OTRS, which has more advanced features than the previous JIRA ticketing system. In particular, OTRS was configurable to solve above limitations and furthermore it supported an Auto ticket creation (and close) feature. After extensive and thorough testing, the ticket automation process was introduced in December 2014, with following benefits:

i. Tickets are logged automatically on a 24/7 basis for the e-mail notifications related to the dashboard events.
ii. The ticketing system is configured so that each testbed part of the federation has a sub-queue and only the SME's related to that testbed have access to it. This provided an opportunity to auto assign the ticket to SMEs based on the keywords in the email

notification. The auto assigning feature provides almost real time notification of an event to the relevant SMEs.

iii. Where a testbed problem is characterised by a sequence of short-lived faults, the ticketing system is intelligent enough to associate all related email notifications to a single open ticket.

iv. The ticketing system is able to receive and act on 'Incident clear' mails sent by the dashboard. Once it receives such a mail, the TTS puts the affected ticket in a 'pending closure' state – SMEs then have 3 days to update the ticket with an appropriate reason for outage at which point, regardless of any more information having been added, the ticket will close. This process means that the only incident tickets which are open are those where an alarm is still active, making it easier for FLS to follow up, with SMEs, incidents which are genuinely ongoing.

3 Operational Experience to Date

The activities of FLS are recorded in a monthly summary report, which is distributed within Fed4FIRE. The report covers the following areas of First Level Support

1. An analysis of trouble tickets generated during the month by test-bed and by type of incident.
2. Trend analysis on the volume of tickets created monthly, over the last 6 months.
3. Trend analysis over the past 6 months of the number of tickets that are escalated to the default SME, on a monthly basis, because of a lack of responsiveness by a test-bed SME for an ongoing event.
4. An analysis of the automatically generated e-mail incident reports, including the distribution of events by weekday, working hours and incident type.
5. An analysis of the number of tickets closed automatically compared to manually(incident resolved itself and no resolution provided by SME) with count of tickets resolved with manual intervention

The first 4 points are self-explanatory, but the last point warrants further explanation. When a trouble ticket is raised in FLS ticketing system it is automatically referred to the SME of the relevant test-bed. In some instances, a fault will be rectified before there is a response from the test-bed SME. The trouble ticket will, however, only be closed when such a response is received indicating the diagnosis of the problem. In order to avoid having trouble tickets remaining open for faults that are no longer present, but where no fault diagnosis is received from the test-bed SME, these tickets are automatically closed three working days after they have been opened. The count referred to by Point 2 is a monthly count of these types of tickets and represents an indicator of the service responsiveness of the federation. As explained in Section 2 there is an escalation path from the test-bed SME to an SME function provided by the co-ordinating partner. The count in point 2 registers the number of times the escalation path is used where there has been no initial response from the test-bed SME. It also represents an indicator of the service responsiveness of the federation

A typical monthly report is shown in Appendix A. The sections below aggregate and summarise the monthly reports over the period October 2014 to September 2015 inclusive.

3.1 Analysis of Trouble Tickets

A Trouble Ticket is generated whenever an email is generated for an event detected by the dashboard. If the event is a recurrence of a recent, previous event for which ticket is already open, then the new event is associated with that already open ticket, on the basis the event is related to an ongoing intermittent fault. Figure (iii) below shows the count of trouble tickets opened, on a monthly basis.

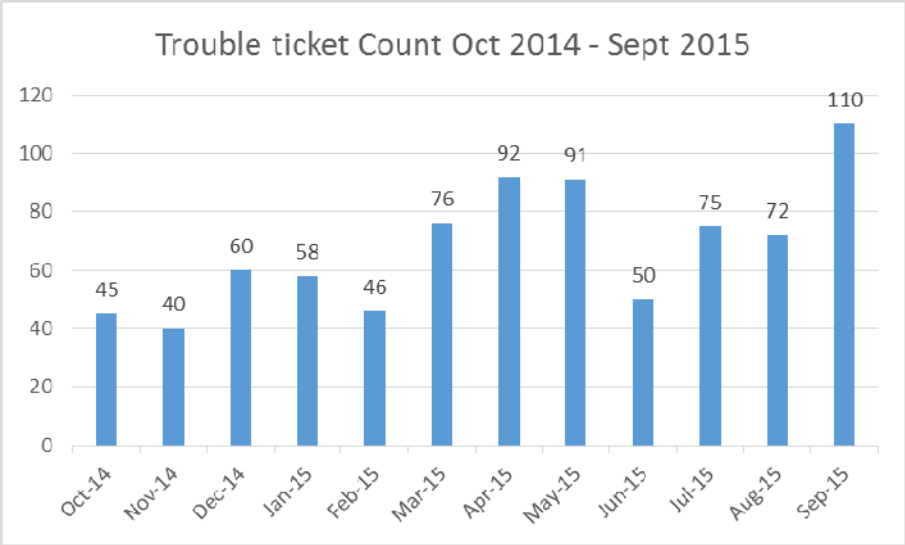


Figure (iii) FLS Trouble Ticket Count October 2014 – September 2015

Figure (iv) analyses these tickets further by category of incident

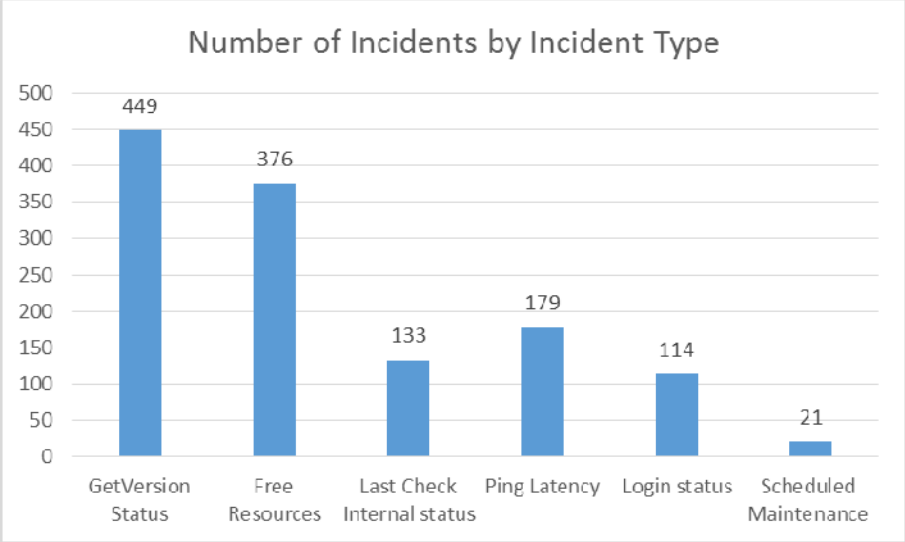


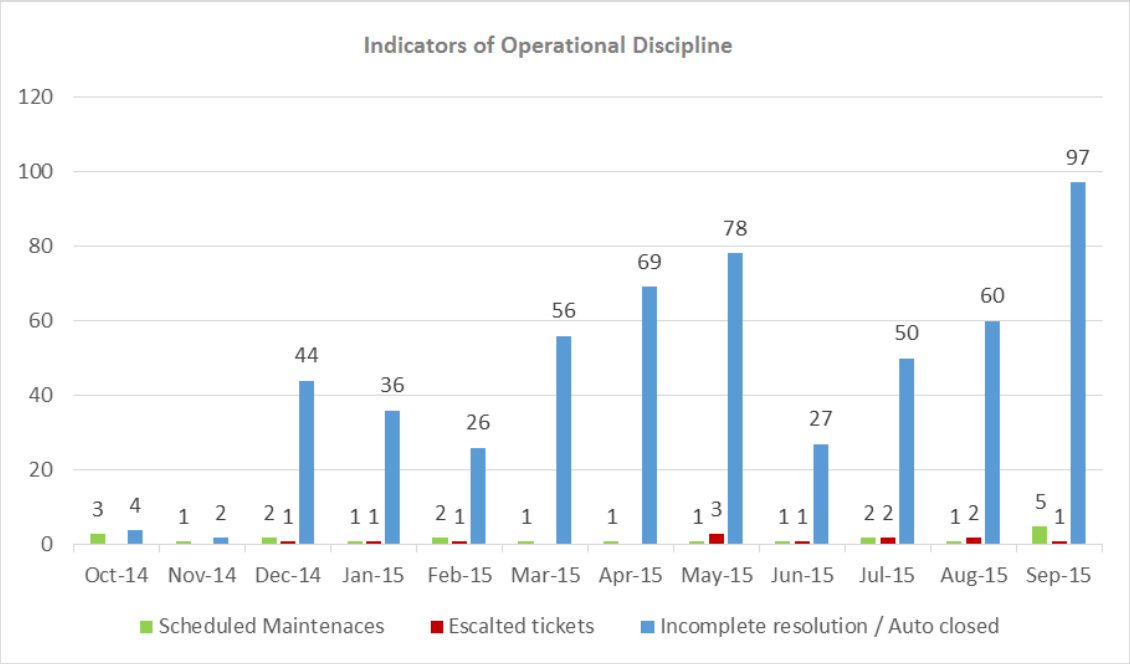
Figure (iv) Analysis of Trouble tickets by type of Incident

Two items are of note. 'Free resources' incident tickets are created whenever a testbed's free resources fall below a certain level and this i.e. it may not indicate a fault and it is more it alert administrators to capacity issues and warn experimenters. Scheduled maintenance is also not a fault but as noted in section 2 management of maintenance is an important element of operational management within the federation.

3.2 Operational Discipline

In any federation it is important that common attention to operations applies across the federation. Members of the federation are, typically, not directly accountable to experimenters in a way that a

single test-bed would be to its users. FLS measures three indicators which provide a view on operational discipline within the federation. The indicators are 'Scheduled maintenance', 'Escalated tickets' and 'tickets with resolution summary' (as described in Section 3 above). Scheduled maintenance is a good indicator of operational discipline as unscheduled maintenance can be difficult for FLS to diagnose. Figure (v) below plots the monthly development of these trouble ticket counts.



Figure(v) Indicators of Operational Discipline

In general most testbeds adhere to a good level of operational discipline when it comes to reporting scheduled maintenance and following up on ongoing incidents. There is a significant increase in the volume of tickets since FLS started logging tickets 24/7 and there is a quite a high percentage ticekts resolved without any proper resultion note by the SME. More analysis and possible improvements in this area are discussed in the lessons learned section (Section 4).

3.3 Analysis of e-Mail Notification of Incidents

E-mail notification of incidents has been operational since August 2014. As described in section 2.3 e-mails have been used to automate the process of Trouble Ticket management since December 2014. The data gathered from analysing the e-mail notifications is a useful addition to understanding the operational performance of the federation.

3.3.1 Distribution of Incidents Over Time

Between October 2014 and September 2015 there were 994 incidents (this includes 'Free resources' alerts, which are significant events but rarely a fault). Figure (vi) Shows trend on the volume tickets on each quarter since Feb 2014. There were two noticeable jumps in monthly ticket volumes, the first due to the introduction of email alerts in August 2014, the second due to ticket automation in December 2015.

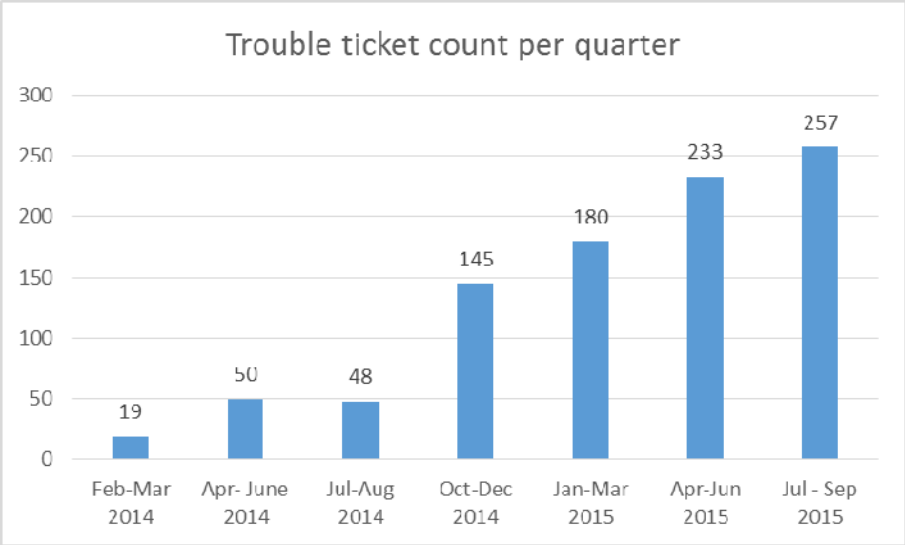


Figure (vi) Ticekt counts per quarter since October 2014.

FLS officially operates for a limited period of the week, Mondays to Fridays between 9am CET and 5pm CET but incidents occurring outside of these times will still be dealt with as the auto-generated tickets are queued to the appropriate SMEs for follow up. Figure (vii) shows a breakdown of when incidents occur.

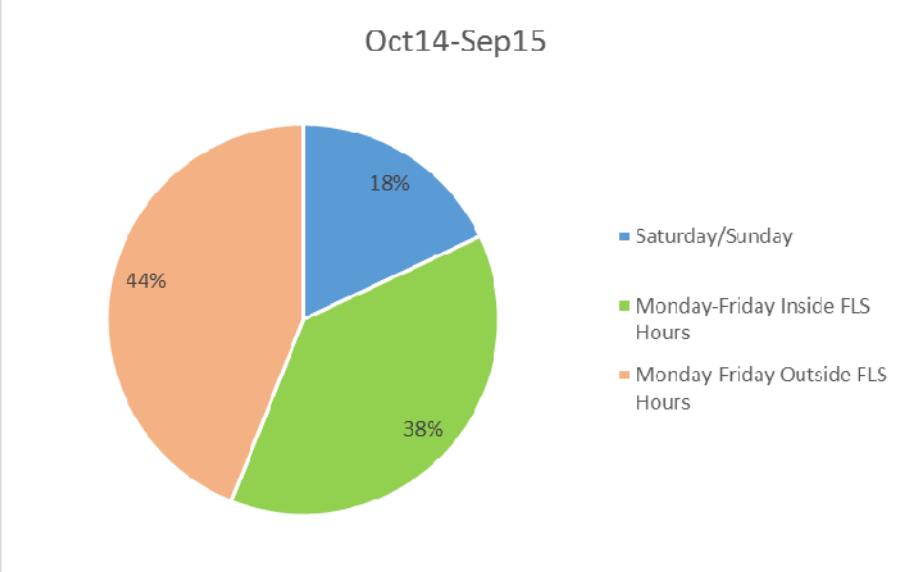


Figure (vii) Distibution of e-mail incidents over time.

3.3.2 Distribution of Incidents by Incident Type.

Table 1 below shows the number of incident tickets over the period broken down by test-bed and type of incident:

Test-bed	GetVersion Status	Free resources	Ping Latency	Last check internal status	Internal testbed monitoring status	Login Status	Total number of Incidents
Bonfire	3	7	3	6	6	4	29
C-Lab	17	57	12	3		32	121
ExoGENI NICTA	0	0	0	0		15	15
Fuseco	11	7	2	13	2	4	39
Koren	14	13	12	22		3	64
NETMODE	23	24	7	3		1	58
NITOS Broker	11	20	9	0		7	47
NITOS SFAWrap	3	4	0	0		0	7
Norbit	0	0	0	5	1	0	6
Ofelia (BristolOpenflow)	10	34	19	12		2	77
Ofelia (Bristol vtam)	11	23	17	12		7	70
Ofelia (i2CAT Openflow)	19	89	4	10		14	136
Ofelia (i2CAT vtam)	23	67	5	9		8	112
Planetlab Europe	18	18	4	2		10	52
SmartSantander	10	16	5	2		0	33
Stanford Optical	2	2	3	1		1	9
UC3M Optical	1	2	2	1		0	6
Virtual Wall 1	4	5	0	5		0	14
Virtual Wall 2	9	2	1	5	5	3	25
Virtual Wall 2 (openflow)	7	13	0	4	5	2	31
w-iLabt.t 2	9	9	4	12	4	2	40
Total	**205**	**415**	**109**	**127**	**23**	**115**	**994**

Table 1 Distribution of Incidents by incident type by test-bed

The most number of events were recorded for 'Free resources' alarm category (41%). Three testbeds (C-Lab, Ofelia i2CAT Openflow and vtam) contributed to 37% of the total events, nearly two thirds of which were related to 'Free resources' event. Apart from this, there is no discernible pattern in the distribution and types of incident recorded – this may be reflecting the different technologies in use in the different test-beds and/or also the differences in operational practice.

4 Experience and Lessons Learned

4.1 E-mail Notification of Incidents / Ticket automation

E-mail notification of incidents offered the possibility of automating the process of Trouble Ticket management. By using a standard format e-mail a trouble ticket is automatically created. When a related incident resolve email is generated this is automatically linked to the existing open ticket. As e-mail notifications are generated throughout the entire week, this has meant all incidents are now logged, not just those seen during the working day. Over the last 12 months operational period 62% of the incidents were logged outside FLS operational hours (08:00 – 16:00 Central European Time), without ticket automation it would have been impractical to log the volume of events we have observed out of hours.

4.2 Managing Experimenters' issues

It was originally planned that FLS would also manage any issues reported by the experimenters using the various testbeds of the federation. However, it was decided that whilst it may have been possible to train up FLS operators in the operational specifics of the individual testbeds, specific testbed-related issues found by experimenters were best dealt with, directly, by the experts from the test-beds concerned. As a consequence, operational issues resulting from experimentation are handled via an Experimenters' email list where experimenters post their issues. The list is monitored by SMEs from the participating test-beds who deal with the queries as and when they arise. This has functioned reasonably effectively, although the level of activity is not high. It has the advantage that experimenters get direct answers from experts. It does however mean that there is no central logging of issues.

4.3 Dashboard Functionality

Although incident logging is now automated, the dashboard display remains a key tool for FLS as it provides a comprehensive, instantaneous visual indication of the status of all test-beds within the federation. Since October 2014 there have been 7 failures or significant faults with the Dashboard. As e-mails are generated for all dashboard detected events, and now all new e-mails generate new tickets, it is very important that false positive alarms are minimised. On 2 of these 7 occasions the fault with the actual dashboard monitoring server did lead to a large number of false alarms being generated and to this a new 'Monitor self' status feature was added to the dashboard. When the dashboard is working normally, the 'Monitor self status' will show "Success" (see figure (ii) in section 2.1) - if any problems are detected the 'Monitor Self status' will show 'Failure' status and, importantly, no event failure emails will be sent out.

4.4 Variation in operational discipline

In a federation, a test-bed will generally not have any direct relationship with experimenters. As such there is a greater need for formality in the operational management of the federation and in the approach that individual test-beds take to operational management at least as far as the federation is concerned. There are two areas where this is particularly important:

i. Advance notice of Planned Maintenance.
ii. Availability of expertise to diagnose and resolve problems.

Although over the year there has been significant increase in the monthly number of tickets the volume of Scheduled maintenance notification is still low when compared with the previous period. Not all test-bed SME's are prompt in updating tickets and ~60% of the tickets closed in the last year were without any recorded resolution. This may be because SMEs are notifying maintenance and fault resolution information to the Experimenters mailing list but not recording the same info in the ticketing system. In order to encourage SME's to properly resolve tickets it is planned, before the end of March, to add additional fault code options in the Ticket System which are specific to test-beds (e.g. eg. Reboot of Aggregate Manager, Connectivity issue) and can be quickly and easily selected by the SMEs. The statistics of fault fix type will be of relevance and use to the project.

Appendix A: Specimen Monthly (FLS) – September 2015 Monthly Report

Executive summary

2015 is the second year of operation of Fed4FIRE First Level Support. September 2015 is the ninth month when the analysis, in this report, is based on the new incident reporting mechanism that was introduced during December 2014.

During September, 110 Trouble Tickets were opened. This is the most number of tickets recorded since we went live with the service. Ofelia i2CAT, C-Lab and ExoGENI NICTA in total contributed to 74% tickets in September. Most number of tickets were recorded for Ofelia i2CAT test bed (51) and 93% of their tickets were for 'Free Resources' alarm. All 15 tickets created for ExoGENI NICTA were for 'login status' failure alarms. Refer to Tables 1-3 below for full analysis on all events.

FLS Report September

During September 2015, 110 Trouble Tickets were opened. There was 5 scheduled maintenance notification.

Since the incident e-mails are generated on a 7*24 hour basis, auto-generation of Trouble Tickets means that they are generated around the clock and not just limited to the period where the FLS service is staffed. In September, only 39% of incidents occurred inside the FLS service window. See Figures 4 and 5 and section 6 incident distribution since January 2015 and for September. In September, only 17% of the tickets (Free resources events excluded) were resolved with an active engagement from SME. Tables 1, 1.1, 2 and 3 below summarize the position by test-bed and by type of alarm.

As before, three graphs are contained in the report to continue the trend analysis. Figures 1 and 3 continue to present a rolling six-month view.

Trouble Ticket Analysis.

The following tables summarize the FLS activity by Trouble Ticket count, Trouble Ticket per test-bed and ticket cause.

Table 1. Tickets statistics for the period 01/09/2015 to 31/09/2015

Total number of tickets	110
Total number of tickets resolved	109 Note 1
Number of tickets opened based on dashboard events	104
Number of Scheduled maintenance tickets	5
Duplicated/Merged/Other tickets	1
Number of tickets escalated to Default SME	1
Number of tickets on Hold	2

Note 1 Includes 1 ticket from previous month

Table 1.1 Auto Vs Manual tickets statistics

Number of Auto created tickets	110
Number of Auto closed tickets	97 Note 2
Number of manually closed tickets	12
Number of tickets closed by SME	4
Number of tickets closed by FLS team	8 Note 2
Number of tickets with active intervention by SME team**	11
Number of tickets with active intervention by FLS team**	23

Note 2 Includes 1 ticket created from previous months

** These tickets refers to cases where the FLS agent and/or SME have to login to the ticket to make an Update/add a note/close/ duplicate or link the ticket to another ticket

Table 2. Breakdown of tickets based on the Test-bed

Test-bed	Number of incidents based on Dashboard	Number of Service and Information request	Number of Scheduled Maintenance
Bonfire	1		5
C-Lab	15		
ExoGENI NICTA	15		
Fuseco	3		
Koren	4		
NETMODE	1		
NITOS Broker	3		
NITOS SFAWrap			
Norbit			
Ofelia (Bristol OpenFlow)	1		
Ofelia (Bristol vtam)	1		
Ofelia (i2CATOpenFlow)	28		
Ofelia (i2CAT vtam)	23		
Planetlab Europe	2		
SmartSantander			
Stanford Optical	1		
UC3M Optical	2		
Virtual Wall 1			
Virtual Wall 2	1		
Virtual Wall 2 (OpenFlow)	1		
w-iLabt.t 2	2		
Dashboard			
other	1		
Total	105		5

Table 3. Dashboard incident break down

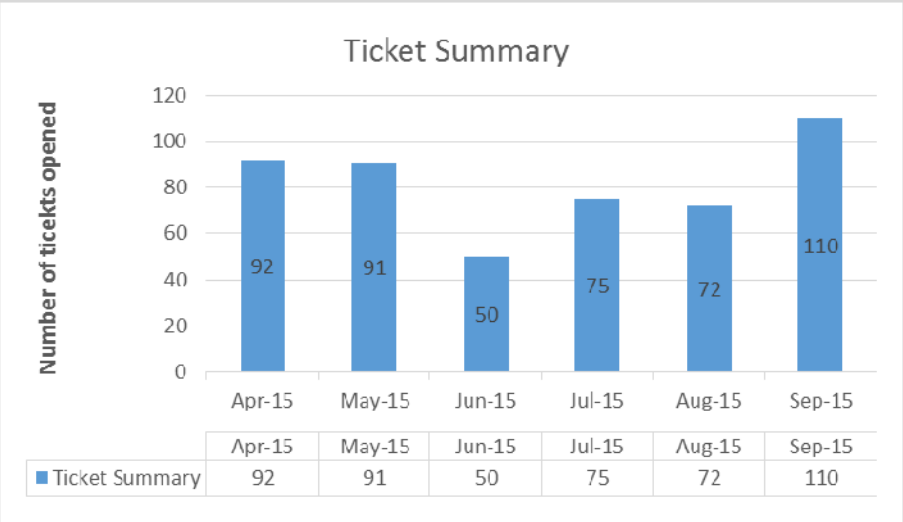
This table illustrates the type of alarms and the total number of dashboard events detected per test-bed. It is based on an analysis of e-mail incident reports. Note, the total number of dashboard incidents detected may not be in line with total number of dashboard tickets, as normally multiple alarms for a test-bed will be tracked from one ticket.

Test-bed	GetVersion Status	Free resources	Ping Latency	Last check internal status	Login status	Total number of Incidents
Bonfire					1	1
C-Lab	1	5			12	18
ExoGENI NICTA					14	14
Fuseco				3	3	6
Koren	1	2	2	2	2	9
NETMODE				1		1
NITOS Broker	1	1	1		2	5
NITOS SFAWrap						
Norbit						
Ofelia (BristolOpenflow)		1	1			2
Ofelia (Bristol vtam)		1	1		2	4
Ofelia (i2CAT Openflow)		28			2	30
Ofelia (i2CAT vtam)		23			2	25
Planetlab Europe		1	1		2	4
SmartSantander						
Stanford Optical	1	1			1	3
UC3M Optical	1	2	2			5
Virtual Wall 1						
Virtual Wall 2	1		1			3
Virtual Wall 2 (openflow)		1				1
w-iLabt.t 2	1	2	2	3	1	9
Total	7	68	11	9	44	138

Trend Analysis

Three graphs illustrate the trend analysis. The second graph illustrates the number of tickets closed automatically versus those closed manually.

Figure 1 Number of tickets opened by FLS on a monthly basis.



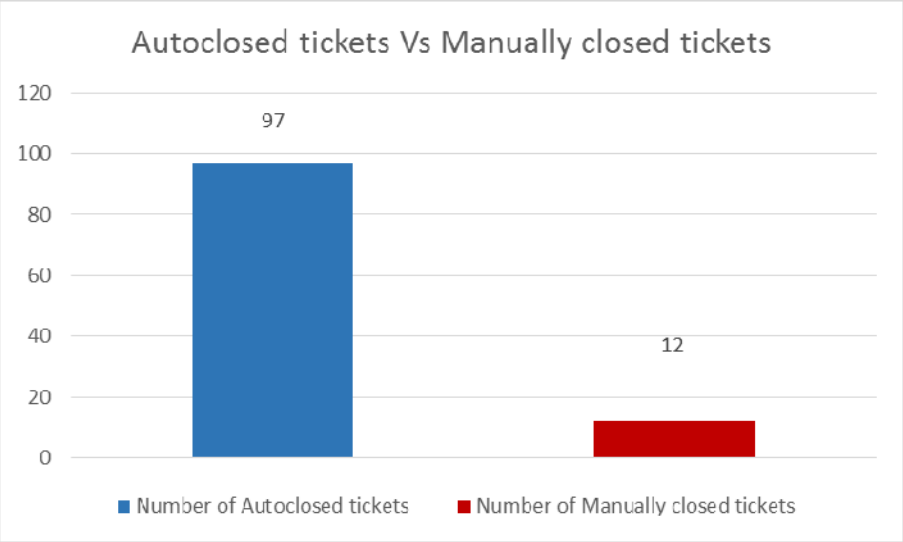


Figure 2 – Auto closed tickets Vs Manually closed ticket

All auto created dashboard tickets for a DOWN event are assigned to appropriate SMEs, when an UP event is received the ticket will go to pending status for three working days, SMEs can provide an explanation for the event and close the ticket within the three day window or the ticket will be auto closed. Figure 2 shows the comparison of number of auto-closed tickets (i.e no explanation provided by SME for the event) with manually closed tickets (i.e Reason for the event provided by SME).

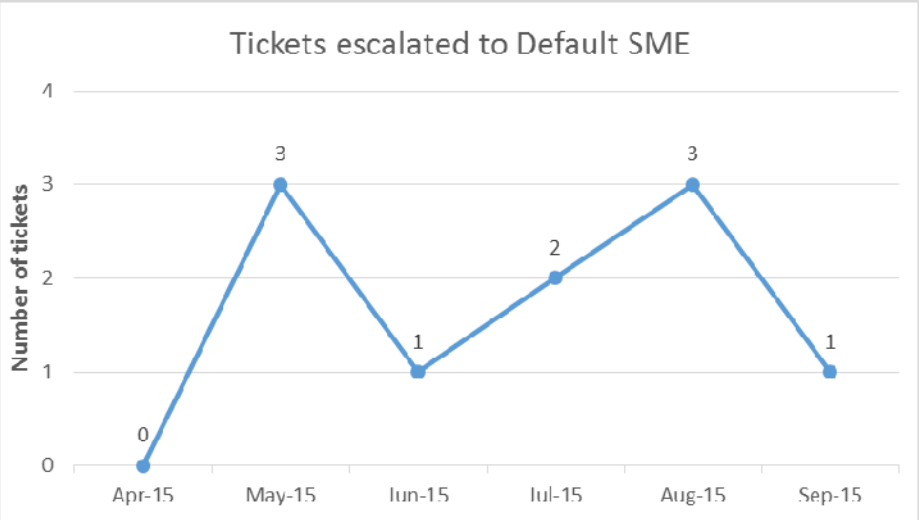


Figure 3 – Tickets Escalated to Default SME.

For an active dashboard alarm or an Incident, if a prompt response is not received from the corresponding test-bed SME, the ticket is escalated to "Default SME" (i.e. iMinds OPS). Figure 3 indicates the number of escalated tickets.

4.5 E-Mail Incident Reports

The analysis presented here continues some the analysis presented in previous reports in 2015, which looked at the time occurrence of incidents. Since the data is not directly comparable with 2014 reports new data-sets have been established which now show either cumulative or average data, as well as monthly data.

4.6 Figure 4 Distribution of Incidents by weekday September + Monthly Average 2015

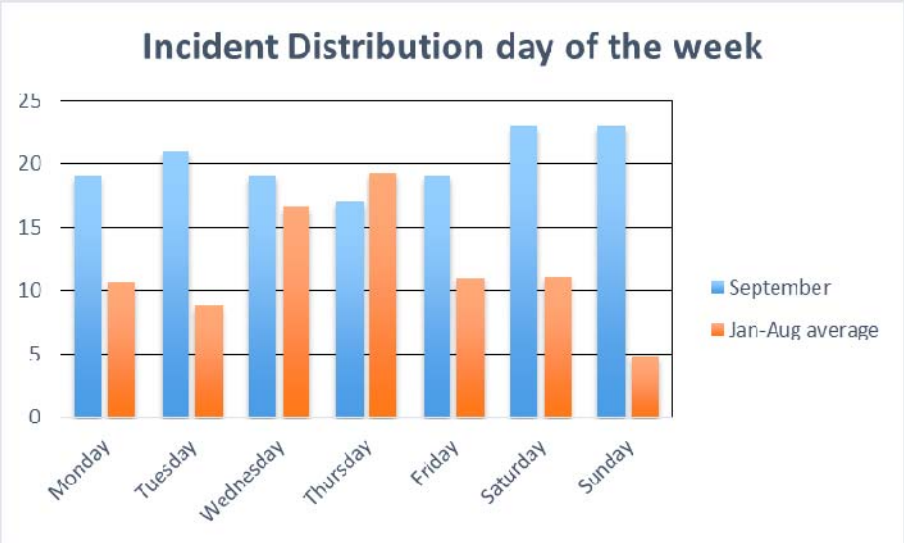


Figure 5 Cumulative Distribution of Incidents 2015 (Pi Chart)

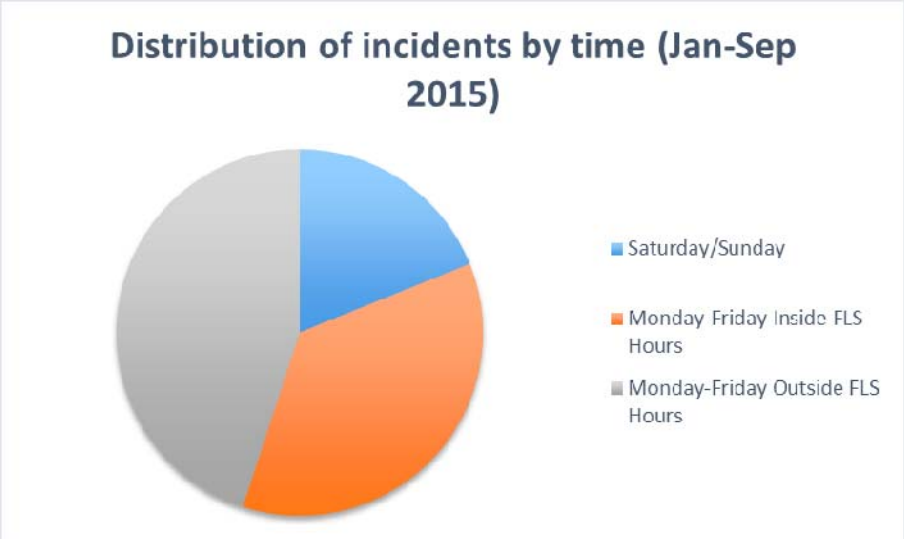


Table 6.1 Distribution of Incident types by time of day and day of week (September)

	Saturday/Sunday	Monday-Friday		
Alarm Type		**Inside FLS hours**	**Outside FLS hours**	**All Incidents**
GetVersion Status	3	2	2	7
Free Resources	21	6	41	68
Last Check Internal status	5	2	2	9
Ping Latency	5	3	3	11
Login status	9	19	15	43
Total	43	32	63	138

4.7 Table 6.2 Distribution of Incident types by time of day and day of week (Cumulative Jan-Aug 2015)

	Saturday/Sunday	Monday-Friday		
Alarm Type		**Inside FLS hours**	**Outside FLS hours**	**All Incidents**
GetVersion Status	29	59	62	150
Free Resources	68	84	170	322
Last Check Internal status	21	63	27	111
Ping Latency	12	34	40	86
Login status	18	43	53	114
Total	148	283	352	783

4.8 Figure 6 Cumulative Distribution of Incidents by Incident Type