

EGEE-III

OPERATIONAL PROCEDURES MANUAL FOR REGIONAL OPERATIONS

Document identifier: EGEE-III-SA1-840932-OperationalProceduresforROD-v2.0.odt

Date: **9.04.2010**

Activity: **SA1: Operations**

Document status: **Released 2.0**

Document link: <https://edms.cern.ch/document/840932/>

Copyright notice:

Copyright © Members of the EGEE-III Collaboration, 2008.

See www.eu-egee.org for details on the copyright holders.

EGEE-III ("Enabling Grids for E-science-III") is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 7th Framework Programme. EGEE-III began in May 2008 and will run for 2 years.

For more information on EGEE-III, its partners and contributors please see www.eu-egee.org

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: "Copyright © Members of the EGEE-III Collaboration 2008. See www.eu-egee.org for details".

Using this document in a way and/or for purposes not foreseen in the paragraph above, requires the prior written permission of the copyright holders.

The information contained in this document represents the views of the copyright holders as of the date such views are published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE EGEE-III COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trademarks: EGEE and gLite are registered trademarks held by CERN on behalf of the EGEE collaboration. All rights reserved"

Table of Contents

1 Operational Procedures Manual for Regional Operations (ROD)	1
Revision history.....	1
1.1 Preface.....	1
2 Introduction	3
2.1 Structure of this manual.....	3
2.2 Duties of Regional Operations.....	3
2.3 Role of Site Admin.....	3
2.4 Role of 1st Line Support.....	4
2.5 Role of Regional Operator (ROD).....	4
2.6 Role of Central COD (C-COD).....	4
3 Getting Started	5
3.1 First time for all roles.....	5
3.1.1 First time for 1st Line Support.....	6
3.1.2 First time for ROD.....	6
3.2 Modes of Operations.....	6
3.3 Mailing lists and follow-up archive.....	6
3.4 Emergency contacts.....	6
4 1st Line Support	7
4.1 Dashboard description.....	7
4.1.1 Monitoring.....	7
4.2 Duties.....	7
4.2.1 Assistance to sites.....	8
4.2.2 Handling new incidents (< 24 hours).....	8
4.2.3 Viewing old incidents (> 24 hours).....	8
4.2.4 Creating entries into knowledge base.....	8
4.2.5 Notify OSCT about urgent matters.....	8
4.2.6 Summary of 1st Line Support Duties.....	8
4.3 Handling tickets.....	9
4.3.1 Modifying tickets.....	9
4.3.2 Closing an incident.....	9
4.4 Communication Lines.....	9
5 ROD	10
5.1 Dashboard.....	10
5.1.1 Monitoring.....	10
5.2 Duties.....	10
5.2.1 Handling tickets.....	10
5.2.2 Propagate actions from C-COD down to sites.....	10
5.2.3 Creating entries into knowledge base.....	10
5.2.4 Putting a site in downtime for urgent matters.....	11
5.2.5 Notify C-COD and OSCT about core or urgent matters.....	11
5.2.6 Summary of ROD Duties.....	11
5.3 Handling tickets.....	12
5.3.1 Creating tickets.....	12
5.3.1.1 Creating tickets without an alarm.....	12
5.3.1.2 Ticket content templates.....	12
5.3.2 Changing the state of a ticket.....	13
5.3.2.1 Workflow and escalation procedure.....	13
5.3.3 Closing tickets.....	14
5.3.4 Escalation of ticket to C-COD.....	15
5.3.5 Ticket re-opening.....	15

Table of Contents

5 ROD

5.3.6 Ticket handling during Weekends.....	15
5.3.6.1 Ticket Handling during Public Holidays.....	15
5.4 Handling Sites and Nodes.....	15
5.4.1 Alarm raised to sites when monitoring is off.....	15
5.4.2 Sites with multiple tickets open.....	15
5.4.3 Downtime.....	16
5.4.3.1 Sites in downtime.....	16
5.4.3.2 Node in downtime.....	16
5.4.4 Specific accounting test failure instructions.....	16
5.4.5 Nodes not in production.....	17
5.4.6 Sites that fail Nagios tests but still continue to be operational.....	17
5.5 Best Practices which have turned into instructions.....	17
5.6 Handover log model.....	17
5.7 Communication Lines.....	18
5.7.1 ROD Communication Lines.....	18
6 Monitoring and problem tracking tools.....	19
6.1 Monitoring.....	19
6.1.1 NAGIOS Availability Monitoring (MyEGEE).....	19
6.1.1.1 ROC_OPERATORS profile.....	20
6.1.1.1.1 Procedure to add a test to the ROC_OPERATORS profile.....	20
6.1.1.2 Alarm generation in the Operations Dashboard.....	21
6.1.2 GIS Monitor.....	21
6.2 Problem tracking.....	22
6.2.1 GGUS.....	22
6.2.1.1 Creating tickets.....	22
7 Security Items and Daily Operations.....	24
7.1 Security matters.....	24
7.2 OSCT organization and OSCT-Duty Contact Role.....	24
7.3 Security incidents handling and Interaction with OSCT-DC.....	25
7.4 Grid Security Vulnerability Handling.....	25
Reason for a Vulnerability handling process.....	25
Reporting a Vulnerability.....	25
Handling of issues reported.....	26
Risk Categories.....	26
On resolution or reaching the Target Date.....	26
Further Details.....	26
Other notes.....	26
8 References.....	27

1 Operational Procedures Manual for Regional Operations (ROD)

Revision history

Comment	Date	Version	Author
Complete revision accounting for new NAGIOS tools	March 2010	2.0	Vera Hansper, Malgorzata Krakowian, Peter Gronbech
Procedures for Regional Operations in regional operations model	18 Sept 2009	1.0	Vera Hansper, Malgorzata Krakowian, Helene Cordier, Michaela Lechner, Ioannis Liabotis, Peter Gronbech
Split of manual into ROD and C-COD parts, including revisions	30 June 2009	0.3	Vera Hansper
First Draft of manual	4 March 2009	0.2	Malgorzata Krakowian, Vera Hansper
First merge of ROD model and COD ops manual	19 january 2009	0.1	Vera Hansper
Split from COD OPS manual	05 january 2009	0.0	Ioannis Liabotis

1.1 Preface

The EGEE Operational Procedures Manual (OPS Manual) defines the procedures and responsibilities of the various parties involved in the running of the EGEE infrastructure, namely the resource centers (also referred to as 'sites') consisting of local support and sites administrators, the staff of the Regional Operations Centres (ROCs) like the ROC Manager and the ROC support staff, the regional operations team consisting of the Regional Operator on Duty (ROD) and the 1st Line Support and the oversight grid monitoring operators (also referred to as 'C-COD'). The OPS manual is currently structured into three separate documents, one covering the responsibilities of ROCs and Sites, one detailing the procedures and responsibilities of the regional operations team and its ROC, the last detailing those for the C-COD team members. To avoid dispersing the same information on multiple documents, and to allow for an easier update of the information, there is a fourth separate document containing the sections that are of relevance to the other manuals, the OPS 'common sections' manual. Sections of this document will be included in the relevant sections of the other three manuals using the twiki INCLUDE mechanism.

The OPS Manual for regional operations related to ROCs and Sites can be found at:

<https://twiki.cern.ch/twiki/bin/view/EGEE/OperationalProceduresforROCsAndSitesObsolete09042010>

The OPS Manual for the regional operations team can be found at:

<https://twiki.cern.ch/twiki/bin/view/EGEE/OperationalProceduresforRODObsolate09042010>

The OPS Manual for C-COD can be found at:

<https://twiki.cern.ch/twiki/bin/view/EGEE/OperationalProceduresforCCODObsolate09042010>

The above procedures can be also found in EDMS at: <https://edms.cern.ch/document/840932>

Readers of any one of the above manuals are encouraged to also read the other manuals in order to have a complete picture of daily operations within EGEE.

Please verify that the document you are using is the current release. The document can be found from:

- the CERN twiki
- EDMS repository

This document does not describe future procedures. It describes the tools and procedures used currently to operate the EGEE production service according to the operation model, defined at:
<https://edms.cern.ch/document/971628>

Since operation of large scale production grids are not static we expect the document to be changed regularly. Major changes will be announced.

- Change requests come from users of the Operational Procedures Manual. Those are: Site managers, ROD, C-COD and SA1 Operational Teams
- To request a change in the manual any interested party should open a ticket via GGUS specifying the "Type of problem" as: "ROD and C-COD Operations";
- According to the type of change requested the following procedure is followed:
 - ◆ Significant changes in procedures and subsequent updates are discussed at C-COD/ARM meetings, which occur quarterly. These requests will be dealt with according to their priority and level of effort required to make the changes.
 - ◆ For urgent changes, proposals have to be discussed on the C-COD and ROC-managers mailing lists and agreed at the following Weekly Operations Meeting by a large majority of operational people.
 - ◆ When agreed and validated these changes are implemented and the procedure coordinator will release a new version of the document.
 - ◆ New versions of the Operations Manual that contain changes in the procedures will be BROADCASTED to all sites and ROCs via the broadcasting tool.
 - ◆ Small typographical and grammatical changes can be made without discussion or approval and published at short notice. No BROADCAST is sent for these types of changes.

2 Introduction

Staff responsible for the operations of the EGEE grid, are broken up into the following areas:

- Operations and Co-ordination Centre - OCC - top level management responsible for all operations.
- Oversight Team - C-COD (consisting of volunteer ROD representatives).
- Regional Operations Team(s) - ROD and 1st Line Support (can be one team or two separate teams).
- Regional Operations Centre - ROC Managers, ROC support staff.
- Resource Centres (sites) - local support, site admins.

The Regional Operations team is responsible for detecting problems, coordinating the diagnosis, and monitoring the problems through to a resolution. This has to be done in co-operation with the Regional Operations Centres to allow for a hierarchical approach and overall management of tasks. ROCs decide themselves on how to manage Regional Operations and whether they wish to have ROD and 1st Line Support as one team or two separate teams.

Procedures have to be followed according to the formal descriptions to ensure predictable work flow and reduce effort duplication or no action at all.

2.1 Structure of this manual

This document is based on a description of the operational procedures that were in use by the operations team at CERN in October 2004 and reflects the changes to the structure of EGEE and the outcome of the previous EGEE/LCG Operations workshops.

- Section 2 : Introduction to manual and describes the duties and roles of the regional operations model.
- Section 3 : Describes the actions needed for all roles to become operational within SA1, includes contact lists.
- Section 4 : Describes duties and tasks applicable to 1st Line Support.
- Section 5 : Describes duties and tasks applicable to ROD operators.
- Section 6 : Describes Common Monitoring tasks.
- Section 7 : Provides a description of the OSCT- Duty Contacts work.
- Section 8 : Provides a table of references including web addresses.

2.2 Duties of Regional Operations

Regional Operations monitor sites in their region, and react to problems identified by the monitors, either directly or indirectly, provide support to sites as needed, add to the knowledge base, and provide informational flow to oversight bodies in cases of non-reactive or non-responsive sites.

2.3 Role of Site Admin

In the scope of Regional Operations, site administrators primarily receive and react on notification of one or more incidents. They should also provide information in the site notepad, which is available on the dashboard.

2.4 Role of 1st Line Support

A team responsible for supporting the site administrators to solve operational problems. The team is provided by each ROC and requires technical skills for their work. Organization and the presence of such a team is optional. However, if this team does not exist explicitly, duties of 1st Line Support must be absorbed by the Regional Operator.

2.5 Role of Regional Operator (ROD)

A team responsible for solving problems on the infrastructure according to agreed procedures. They ensure that problems are properly recorded and progress according to specified time lines. They ensure that necessary information is available to all parties. The team is provided by each ROC and requires procedural knowledge on the process (rather than technical skills) for their work. However, if the team also encompasses the role of 1st Line Support, then the necessary technical skills will be required.

2.6 Role of Central COD (C-COD)

A small team responsible for coordination of RODs, provided on a global layer. C-COD represents the whole ROD structure at the political level. Support tools developers should interact with C-COD about the tools, especially when issues arise.

3 Getting Started

All new operations team members have to take certain steps to ensure that they can access the operations dashboard. Some choices in options may vary, depending on their role, which are further explained in the specific role duties.

- Have a valid certificate delivered by a CA;
- Subscribe to the LCG-ROLLOUT mailing list at the following URL:
<http://jiscmail.ac.uk/cgi-bin/webadmin?REPORT&z=3>.
- Register into the dteam VO (also known as the LCG deployment team) at the following URL:
<https://lcg-voms.cern.ch:8443/vo/dteam/vomrs>;
- Register into GGUS as support staff (<https://gus.fzk.de/admin/apply4staff.php>) and read the current manual (<https://gus.fzk.de/pages/docu.php>)
- Request GOC Database (GOCGB) read-only access by completing the form at the following <https://goc.gridops.org/user/register>. (Note, you will not be able to access this URL if you are already registered.) The GOCDB contains essential static information about the sites and is used by many tools for monitoring and accounting purposes. Specific roles have to be requested (outlined below) in the GOCDB at <https://goc.gridops.org/role/request>;

The necessary steps for each role will be repeated in the following sub-sections.

There are a few recommendations before starting the actual task. The new operator needs to be familiar with

- MyEGEE which replaces the old SAM pages. There is a page for each ROC, for example https://sam-%INSERT-YOUR_ROC_HERE%-roc.cern.ch/myegee. Details of each ROC's URL can be found on <https://twiki.cern.ch/twiki/bin/view/EGEE/NagiosROCURL>
- OLD Sites Functional Tests (SAM) can still be found at <https://lcg-sam.cern.ch:8443/sam/sam.py>
- The new GIIS: GSTAT 2 monitor is at <http://gstat-prod.cern.ch/gstat/summary/>
- For the older version of GIIS Monitoring (Gstat): <http://goc.grid.sinica.edu.tw/gstat/>

They should try to understand the errors that appear and find ones that they could not follow up if they are on duty. They can ask the C-COD mailing list or refer to the GOC Wiki pages for help. Typically, they should also read some emails which have been sent on the followup-list.

- Read the training material composed of a general presentation of the tool and a "how-to guide" at <https://edms.cern.ch/document/1015741>. This material is also available from the Operations Portal.
- Go to the operations dashboard manual and work through the functionality of the site;
- Take a look at the C-COD handover logs and previous minutes of Weekly Operations Meetings;
- Read the Glite User Guide and try submitting a "Hello World" job. This will give them valuable background information and with some hands on experience they can tell user errors from GRID service errors more easily;
- Ask questions. Find people who have done it before or even better join an experienced team for a few days and look over their shoulders while they do their work. Not everything can be written down.
- Read/Contribute to the Operations Best Practices Wiki, moderated by the C-COD team, at <https://twiki.cern.ch/twiki/bin/view/EGEE/EGEEOperationsBestPractices>
- If you spot a specific operational use-case which you do not know how to handle, please fill in the operational use case wiki at <https://twiki.cern.ch/twiki/bin/view/EGEE/OperationalUseCasesAndStatus>, so that the C-COD team can fix this in the operational procedure Manual or in the Best Practices Wiki.

3.1 First time for all roles

- Read and become familiar with this document, specifically the parts relevant to their role.

- Have a valid certificate delivered by a CA;
- Register into the dteam VO: <https://lcg-voms.cern.ch:8443/vo/dteam/vomrs>;
- Register into GGUS as support staff
- Request GOCDB read-only access by completing the form at the following <https://goc.gridops.org/user/register>

3.1.1 First time for 1st Line Support

- Request a **Regional 1st Line Support** role in the GOCDB at <https://goc.gridops.org/role/request> .

3.1.2 First time for ROD

- Request a **Regional Staff** role in the GOCDB at <https://goc.gridops.org/role/request> .

3.2 Modes of Operations

ROD and 1st Line Support are collectively known as Regional Support, and are organised internally in each ROC. They can be run as two separate teams or be one team that covers both sets of duties. The responsibility of the 1st Line Support team may differ in each ROC. The ROC determines how the work of the 1st Line Support team is organized in conjunction with the ROD team. Suggestions for several modes of operation of 1st Line Support are:

- minimal - there is almost no 1st Line Support, all responsibility for solving problems is left on sites and responsibilities for the project that are not implemented will be taken over by ROD.
- passive - they react only when a request for support comes from a site.
- pro-active - they react on requests, look at results and receive notifications from monitors and they contact sites when there is a suspicion of a problem, suggesting solutions.

3.3 Mailing lists and follow-up archive

- C-COD mailing list: project-eu-egEE-sa1-c-cod-followup@cernSPAMNOTSPAMNOT.ch internal communication for C-COD staff
- ROD mailing list: project-eu-egEE-sa1-cic-on-duty@cernSPAMNOTSPAMNOT.ch internal communication for operations staff. This list encompasses all ROD contact staff.

3.4 Emergency contacts

Currently the GOCDB also handles sites that are not committed to EGEE, but are part of the WLCG as far as EGEE/LCG operations are concerned. These sites are connected to ROCs outside of the EU: LA (Latin America), CA (Canada), IGALC (Latin America and Caribbean Grid Initiative).

Phone contacts for all staff connected to sites and ROCs are available within the GOCDB and VO contacts are available from the Operations Portal. Please see https://goc.gridops.org/user/security_contacts .

NB: Since a recent revision of the GOCDB it is now possible to download these data on a regular basis through GOCDBPI. It is advised that the operations teams download and update this list once a month.

4 1st Line Support

NOTE: Depending on the organisation of the ROC, 1st Line Support may exist as a separate team, or be part of the ROD team. Regardless of the organisation, the duties in this section **MUST** be assigned and executed.

4.1 Dashboard description

The Operations Dashboard <https://operations-portal.in2p3.fr/> should be used for 1st Line Support.

A HOWTO guide for the operation's Regional Dashboard and an overview presentation can be found at <https://edms.cern.ch/document/1015741> .

4.1.1 Monitoring

There are currently a variety of monitoring tools in EGEE/LCG which are used to detect problems with sites. They also provide useful information about sites. The operations dashboard <https://operations-portal.in2p3.fr/> provides links and utilises combined views of the most common monitoring tools for performing tasks. The links below are to some of the tools used by operators.

- Nagios monitoring: https://sam-%INSERT-YOUR_ROC_HERE%-roc.cern.ch/myegee. There is a page for each ROC, the details of each ROC's URL can be found on <https://twiki.cern.ch/twiki/bin/view/EGEE/NagiosROURL> ;
- The Nagios interface is also available directly at : https://sam-%INSERT-YOUR_ROC_HERE%-roc.cern.ch/nagios ;
- GUIS Monitor: <http://gstat-prod.cern.ch/gstat/summary/> ;
- GOC Database: <https://goc.gridops.org/> ;
- GridMap: <http://gridmap.cern.ch/gm/> .

There is a video available describing the transition from old style SAM to the Nagios based system.

Please also refer to the monitoring section in Section 6.

4.2 Duties

The 1st Line Support team is primarily expected to monitor and act on recent (less than 24 hours old) dashboard alarms. They should also provide technical assistance to sites directly. 1st Line Support members should be technically skilled in understanding and solving OPS problems. The following are recommended guidelines for ROCs which have 1st Line Support teams. Some steps might be redundant. For example, if the team is in continuous operation, then a handover might be irrelevant.

1. A shift, which should generally cover a full working week, Monday to Friday, should start with actions related to handovers. The format of the handover for 1st Line Support and how it is passed on to the next team is decided by the ROC.
2. Read the entries made in the previous week. If there is an open issue with a site, it should be acted on immediately.
3. Check relevant ROC mailing lists for any requests from sites.
4. Work on the operations dashboard at the following link: <https://operations-portal.in2p3.fr/> .
5. Note all new alarms that are in your scope, and contact relevant sites about the alarm(s).
6. Assist sites with incidents/alarms in general.
7. Respond to requests from sites for assistance.
8. Modify any GGUS ticket body up to the **solved by ROC** status. ROD will close the ticket accordingly.

4.2.1 Assistance to sites

Assistance to sites should be an ongoing task. Requests from sites for assistance should be handled in a timely manner, especially when the request is in relation to **recent** alarms. Assistance can be in any form that is most suitable to the situation.

4.2.2 Handling new incidents (< 24 hours)

- 1st Line Support should act immediately on all new alarms. This can be in the form of an email to the site, including a link to the alarm that is currently in an error state.
- Exceptions to this would be when the alarm is due to a time out, (generally network related), and it would be prudent to wait for the next occurrence of the alarm, where it might be in an OK state.
- A summary of the alarms and tickets in the scope of 1st Line Support is available The Operations Dashboard
- Details of the Alarms can be seen by clicking the left hand expansion icon on the site, and it is possible for 1st Line Support to switch alarms in an OK state to OFF. To switch off an alarm in an OK state:
 - ◆ click on the expansion icon to the left of the site name to open up the drop down information on the site. Then click on the expansion icon to expand the *New NAGIOS Alarms* drop down menu to access the area where you can handle the alarm.
 - ◆ select the left hand tick box for the alarm in the **OK** state
 - ◆ click on the **Close Selected Alarms** button to *Set status to "off"*

4.2.3 Viewing old incidents (> 24 hours)

Alarms or incidents older than 24 hours can be viewed from the Dashboard. These should already have (GGUS) tickets associated with them and are the responsibility of ROD. 1st Line Support, may, if they wish, communicate with ROD or the site through the relevant GGUS ticket ID about these alarms/incidents.

4.2.4 Creating entries into knowledge base

Insight on new errors not yet recorded and updates on existing entries should be added to the regional knowledge base, or in the case where no regional knowledge base exists, to the GOC wiki. Adding new entries to the GOC wiki can be done in two ways. The former is to choose the 'Add to wiki' button in the GGUS ticket with the solution and the latter is to add it directly on the GOC wiki page. However, before adding an entry, please refer to the GGUS FAQ <https://gus.fzk.de/pages/faq.php> and also use the GGUS Search tool <http://iwrugussema.ka.fzk.de/> and the GOCWIKI <http://goc.grid.sinica.edu.tw/gocwiki/FrontPage> to see if such an entry also exists.

If in doubt, contact ROD or your ROC manager for help. ROD is also responsible for ensuring that these are correctly forwarded and included.

4.2.5 Notify OSCT about urgent matters

For security related issues, 1st Line Support should also notify the OSCT duty contact.

4.2.6 Summary of 1st Line Support Duties

Duties of 1 st Line Support	Requirements
Receive incident notification from sites in the scope	Mandatory
Respond to site support requests	Optional – present in "passive" mode
Contact a site for incidents which are not being tackled	

	Optional – present in "pro-active" mode
Assist a site in solving incidents	Mandatory
Pass information to the ROD team via the dashboard "site notepad" or through an existing GGUS ticket for that site	Mandatory
Handle incidents less than 24h old	Mandatory
View incidents older than 24h	Optional
Modify any GGUS ticket body up to the "solved by ROC" status	Mandatory
Close incidents for "solved problems"	Mandatory
Create entries for the knowledge base	Mandatory
Create tickets to C-COD for core or urgent matters	Optional: submitted through ROD for validation

(Definitions in the "Requirements" column: Mandatory – must be covered by either 1st Line Support or the ROD team; Optional – the federation decides how to implement this.)

4.3 Handling tickets.

Tickets are generated for a site by ROD, but 1st Line Support can update tickets through the GGUS <https://gus.fzk.de/pages/home.php> interface. They can also communicate with the site about the ticket through this system.

4.3.1 Modifying tickets.

GGUS tickets can be modified up to the "solved by ROC" status.

4.3.2 Closing an incident

Tickets are closed by ROD and it is not the role of 1st Line Support to close tickets.

4.4 Communication Lines

In a pro-active role, 1st Line Support can contact site admins directly using the site contact email address registered in the GOCDB or provided by their ROC management. They can also use other communication lines, for instance, instant messenger services (IMS), or a local ticketing system, if provided by the ROC. Conversely, 1st Line Support can be contacted by sites through mailing lists, the ticketing system, whether local or GGUS, or IMS.

Generally, communication with ROD regarding a specific site is done through the dashboard where 1st Line Support can fill in entries into the "site notepad". Urgent matters can also be done through mailing lists or IMS where appropriate.

Communicating with C-COD should be done through either ROD or the ROC managers.

5 ROD

A ROD team is provided by each ROC. It is responsible for handling operational tickets for sites in their respective region. It is proposed that ROD has authority over 1st Line Support duties, which means that if some duties are not covered by 1st Line Support then they shall be done by ROD. This is reflected in ROD duties marked as Mandatory with a "if not handled by 1st Line Support" in the table in the following sections.

5.1 Dashboard

The dashboard for ROD is available from <https://operations-portal.in2p3.fr> page.

A HOWTO guide for the operation's Regional Dashboard and an overview presentation can be found at <https://edms.cern.ch/document/1015741> .

5.1.1 Monitoring

There are currently a variety of monitoring tools in EGEE/LCG which are used to detect problems with sites. They also provide useful information about sites. The operations dashboard <https://operations-portal.in2p3.fr/> provides links and utilises combined views of the most common monitoring tools for performing tasks. The links below are to some of the tools used by operators.

- Nagios monitoring: https://sam-%INSERT-YOUR_ROC_HERE%-roc.cern.ch/myegee. There is a page for each ROC, the details of each ROC's URL can be found on <https://twiki.cern.ch/twiki/bin/view/EGEE/NagiosROURL> ;
- The Nagios interface is also available directly at : https://sam-%INSERT-YOUR_ROC_HERE%-roc.cern.ch/nagios ;
- GIIS Monitor: <http://gstat-prod.cern.ch/gstat/summary/> ;
- GOC Database: <https://goc.gridops.org/> ;
- GridMap: <http://gridmap.cern.ch/gm/> .

There is a video available describing the transition from old style SAM to the Nagios based system.

Please also refer to the monitoring section in Section 6.

5.2 Duties

All duties listed in this section are mandatory for ROD team. In the case of no explicit 1st Line Support team in the ROC, duties of that team must be absorbed by the ROD.

5.2.1 Handling tickets

The main responsibility of ROD is to deal with tickets for sites in the region. This includes making sure that the tickets are opened and handled properly. The procedure for handling tickets is described in section 6.3.

5.2.2 Propagate actions from C-COD down to sites

ROD is responsible for ensuring that decisions taken on the C-COD level are propagated to sites.

5.2.3 Creating entries into knowledge base

Insight on new errors not yet recorded and updates on existing entries should be added to the regional

knowledge base, or in the case where no regional knowledge base exists, to the GOC wiki. Adding new entries to the GOC wiki can be done in two ways. The former is to choose the 'Add to wiki' button in the GGUS ticket with the solution and the latter is to add it directly on the GOC wiki page. However, before adding an entry, please refer to the GGUS FAQ <https://gus.fzk.de/pages/faq.php> and also use the GGUS Search tool <http://iwrgrussema.ka.fzk.de/> and the GOCWIKI <http://goc.grid.sinica.edu.tw/gocwiki/FrontPage> to see if such an entry also exists.

When a page is modified, ROD should send a mail about the changes to the C-COD mailing list. C-COD will ensure that the information is propagated correctly so others ROCs, sites and admins will know about new entries and updates.

5.2.4 Putting a site in downtime for urgent matters

In general, ROD can place a site in downtime (in the GOCDB) if it is either requested by the site, or ROD sees an urgent need to put the site into downtime.

ROD may also suspend a site, under exceptional circumstances, without going through all the steps of the escalation procedure. For example, if a security hazard occurs, ROD must suspend a site on the spot in the case of such an emergency. It is important to know that C-COD can also suspend a site in the case of an emergency e.g. security incidents or lack of response.

In both scenarios, it is important that communication channels between all parties involved are active.

5.2.5 Notify C-COD and OSCT about core or urgent matters

ROD should create tickets to C-COD in the case of core or urgent matters. For security related issues, 1st Line Support and/or ROD should also notify the OSCT duty contact.

5.2.6 Summary of ROD Duties

Duties of ROD	Requirements
Receive incident notification from sites in the scope	Mandatory (if not handled by 1 st Line Support)
Handle incidents less than 24h old	Mandatory (if not handled by 1 st Line Support)
Create tickets for alarms older than 24h and that are not in an OK state	Mandatory
View incidents older than 24h	Mandatory
Escalate tickets to C-COD if necessary: assignment to C-COD can be made directly through the dashboard.	Mandatory
Propagate actions from C-COD down to sites	Mandatory
Monitor and update any GGUS tickets up to the "solved by ROC" status (via the dashboard)	Mandatory
Close incidents for "solved problems"	Mandatory
Create entries for the knowledge base	Mandatory
Handle the final state of the incident: i.e "closed by ROD" once the ROD has verified that the solution provided at the "solved by ROC" level is correct and appropriately documented.	Mandatory
Put the site in downtime for urgent matters	Optional
Create tickets to C-COD for core or urgent matters	Mandatory

(Definitions in the "Requirements" column: Mandatory – must be covered by either 1st Line Support or the ROD team, Optional – the federation decides how to implement this.)

5.3 Handling tickets

5.3.1 Creating tickets

Ticket creation occurs when the age of an alarm in an error state has passed 24 hours, whether or not a site has already made some action on the alarm. A ticket can be created from the operations dashboard. The process can be summarised in the following list:

1. Click on the magnifying icon to the left of the site name to open up the drop down information on the site. This action also allows access to the area where a ticket can be created.
2. Check the site notepad to see if any action has been taken on the alarm.
3. Click on the **Add a ticket for this alarm** icon to the left of the alarm, and the ticket creation page will appear.
 - ◆ If more than one alarm should be handled by the same ticket, the alarms should be appropriately masked before hand.
4. Fill in the relevant information in the ticket section. If there was information in the site notepad, ensure that the ticket information reflects that information. Also ensure that the TO:, FROM: and SUBJECT: fields are all correct. Generally, a ticket should go to both the site and the ROC/ROD.
5. Select **submit ticket** and a pop up window will appear confirming that the ticket was correctly submitted. Your ticket has now been assigned an ID, a copy of this has been created as a GGUS ticket with its own GGUS ID and the ticket has now been sent to the site.
6. Note that although the ticket is also available from the GGUS system, it is important that escalation and closing procedures are all performed from the ROD dashboard, with the ROD ticket ID.

5.3.1.1 Creating tickets without an alarm.

It is also possible to create a ticket for a site without an alarm. For instance, if there is an issue with one of the tools (Gstat, for instance) that does not create an alarm in the dashboard. In this case, click on the button labeled "Create ticket without an alarm", and fill in the appropriate fields as when creating a ticket for an alarm. The icon for this is found at the right at the top of the site bar.

5.3.1.2 Ticket content templates

The email is addressed to the corresponding ROC, together with the site. ROC mail addresses are listed on the Operations Portal (<https://cic.gridops.org>) under ROC views.

```
Mail Info:
From: Regional Operator <rodcontactemail>
To: <sitecontactemail>, <rocontactemail>
Cc: <rodcontactemail>, GGUS helpdesk
Ticket info:
Subject: <problem> at <sitename>
```

The mail has to contain:

- Category of the error and the error message;
- Name and URL of the Nagios page, where the error can be seen;
- Any other information (like link from the GOC Wiki page) useful for new site administrators.

Of course, obvious errors (like an MDS restart) do not require all these steps as a one line mail will do.

The general template for the mail is as follows:

```
Dear Site Admins and ROC Helpdesk,
```

We have detected a problem at <sitename>

org.sam.CREAMCE-JobSubmit-ops is failing on : <nodename>

Failure detected on : <date>

View failure history and details on NAGIOS portal :

<https://samnagXXX.cern.ch/nagios/cgi-bin/avail.cgi?host=<sitename>&service=org.sam.CREAMCE-JobSubmit-ops>

View some details about the test description : <https://twiki.cern.ch/twiki/bin/view/LCG/SAMProbes>

Additional comments or logs for alarm org.sam.CREAMCE-JobSubmit-ops-test-lcgce.uibk.ac.at#4883

Could you please have a look ?

Thank you

<Regionname> - Regional Operator team

Link to Ticket : <GGUS_url>

5.3.2 Changing the state of a ticket

1. When the state of an alarm for a site with an open ticket changes to **OK** then the ticket associated with that alarm can be updated in the ROD dashboard. If the problem at the site has been fixed, then the procedure for closing the ticket can begin.
 - ◆ If the problem was trivial and required just a simple action (for example a GIIS service restart) without any configuration changes then the ticket can be closed.
2. If the Nagios alarm is in an unstable state, and the site has not responded to the problem in a reasonable amount of time (less than 2 days) then a 2nd email can be sent to the site without escalating the ticket.
 - ◆ This is done by opening the ticket in the ROD dashboard: click on the Update ticket icon on the left hand side of the ticket entry. This opens an 'Update a Ticket' page. The ticket is updated using the option **1st email to site admins**. Remember to change the expiration date to one day in the future.
 - ◆ If a site does not respond promptly (within a day) to such an email, then the ticket should be escalated. (**2nd email to site admins**)
3. If a site does not respond within 3 days to the first email upon creation of a ticket, then the ticket must be immediately escalated to the second stage (**2nd email to site admins**).
4. If a new failure is detected for the site, the existing ticket should not be modified (though the deadline can be extended) but a new ticket should be submitted for this new problem.
5. If the site's problem can not be fixed in a reasonable amount of time (2-3 days) then inform the site that they should go into unscheduled downtime. If they do not accept declaring downtime, then ROD proceeds with the regular escalation procedure at the agreed deadlines.

5.3.2.1 Workflow and escalation procedure

This section introduces a critical part of operations in terms of sites' problems detection, identification and solving. The escalation procedure is a procedure that operators must follow whenever any problem related to a site is detected. The main goal of the procedure is to track the problem follow-up process as a whole and keep the process consistent from the time of detection until the time when the ultimate solution is reached.

Moreover, the procedure is supposed to introduce a hierarchical structure and responsibility distribution in problem solving which should lead to significant improvement in the quality of the production grid service. Consequently, minimizing the delay between the steps of the procedure is of utmost importance. The regular procedure the operators follow can be considered in four phases.

- submitting problems into the problem tracking tool after they are detected using monitoring tools or by a task created by a regional operations team (ROC);

- updating the task when a site state changes which can be detected either by a comparison of the monitoring information with the current state of the task in the problem tracking tool, or by input from a ROC;
- closing tickets or escalating outdated tickets when deadlines are reached in the problem tracking tool;
- initiate last escalation step and/or communication with site administrators and ROCs.

Below are the detailed steps of the "escalation procedure" if no response is received for the notification of a problem or the problem has been unattended for:

Step [#]	Max. Duration [work days]	Escalation procedure
1	3	When an alarm appears on the ROD dashboard (>24 hours old): 1st mail to site admin and ROC
2	3	2nd mail to site admin and ROC; At the end of this period escalate to C-COD
3	5	Ticket escalated to C-COD, C-COD should in that week, act on the ticket by sending email to the ROC, ROD and site for immediate action and stating that representation at the next weekly operations meeting is requested. The discussion may also include site suspension.
4		(IF no response is obtained from either the site or ROC) C-COD will discuss the ticket at the FIRST Weekly Operations Meeting and involve the the Operation and Coordination Center (OCC) in the ticket
5	5	Discuss at the SECOND weekly operations meeting and assign the ticket to OCC
6		Where applicable, C-COD will request OCC to approve site suspension
7		C-COD will ask ROC to suspend the site

NB : Theoretically, the whole process could be covered in a 2-3 week period. Most often a site is either suspended on the spot for security reasons, or the problem is solved (or the site and the ROC reacts) well before operators need to escalate the issue to C-COD, who then determines whether to bring it to the Weekly Operations Meetings.

NB: After the first 3 days, at the 2nd escalation step, if the site has not solved its problem, ROD should suggest to the site to declare downtime until they solve the problem and the ROC should be notified. If they do not accept the downtime then C-COD will proceed with the regular escalation procedure at the agreed deadlines.

Detection, diagnosis and problem tracking tools are also described in section 6.

5.3.3 Closing tickets

The following steps describe the procedure to close a ticket:

1. If a ticket in the dashboard shows that the sites Alarm status is now OK, check the corresponding GGUS ticket for the current status of the ticket. (i.e. "Solved by ROC" state.)
2. If the site has solved the ticket, check that the Nagios tests show that the site status for the problem is now OK and stable.
3. If the above two conditions are suitably met, go to the dashboard and open the relevant ticket (via the "Update ticket" icon).
4. Set the following parameters:
 - ◆ Escalate: set to Site OK;
 - ◆ Fill in the solution;
 - ◆ Update the ticket;

A page giving the information about the ticket will show that the Ticket Status is set to "Closed".

Note that now no further action can be made on this ticket in the dashboard.

5.3.2.1 Workflow and escalation procedure

5.3.4 Escalation of ticket to C-COD

Communication with sites and ROCs is described in a somewhat formal manner because there have been some occurrences when the person in charge has not responded to the notification mails created by the problem tracking tool (GGUS). This escalated communication with partners that are not living up to their responsibilities is, unfortunately, necessary, but ROD is not required to deal with the problem directly. They can escalate the ticket in question to C-COD.

If, after 3 days, no email was received by ROD from the sites after the 2nd email to sites is sent, the ticket should be escalated to C-COD;

- On the dashboard, go to the ROD ticket ID, and open the ticket.
- Under the **UPDATE TICKET** section, at "Escalate(new action list):" choose "C-COD" from the list.
- Fill in the details in the "Mandatory" section as necessary. There is no need change the expiration date.
- Send (submit) the ticket.

Tickets will also be automatically escalated to C-COD if they are more than 30 days old. C-COD will then determine subsequent actions.

5.3.5 Ticket re-opening

When a site closes a GGUS ticket that ROD has issued ("Solved byROC"), ROD can re-open that ticket for problems that the site reported as solved but where the detected problem persists. Ticket re-opening is done from the dashboard interface, and in general it should be sufficient to pursue the issue with non-escalation emails. Note that ROD should only re-open tickets for THAT problem. If the problem is different then a new ticket should be opened.

5.3.6 Ticket handling during Weekends

Due to the fact that weekends are not considered working days it is noted that ROD teams do not have any responsibilities during weekends and that RODs should ensure that tickets do not expire during weekends.

5.3.6.1 Ticket Handling during Public Holidays

Currently there is no automatic mechanism for handling ticket expiration over public holiday periods. As this can vary from site to site, RODs are encouraged to get their sites to announce their public holidays so that ticket expiration can be set accordingly. (Correspondingly, ROD operators also have no duties when they are on public holidays.)

5.4 Handling Sites and Nodes

5.4.1 Alarm raised to sites when monitoring is off

If an alarm is raised for a service that has its monitoring status set to OFF then ROD should not open a ticket. ROD should open a ticket to GOCDB SU in GGUS notifying them about the problem and also report the incident to C-COD so that it is raised at the next Weekly Operations Meeting.

5.4.2 Sites with multiple tickets open

When opening a ticket against a site with existing tickets ROD should consider that these problems may be linked or dependant on pending solutions. If the problem is different but maybe linked the expiry dates for each ticket should be synchronized to the latest date.

In the event of more than one ticket being opened for the same problem ROD must decide which ticket has been active and then close those with no responses. ROD staff must comment in the ticket that they are closing a ticket which is linked to another and state the GGUS number for reference.

5.4.3 Downtime

To properly manage downtime it is important to highlight the differences between the possible types of downtime.

Downtime classification:

1. scheduled (e.g. for software/hardware upgrades) planned and agreed in advance
2. unscheduled (e.g. power outages) unplanned, usually triggered by an unexpected failure

Downtime severities:

1. At Risk (Resource will probably be working as normal, but may experience problems)
 - ◆ REMARK: This type of severity does not have operational consequences. It is only an information for users that some small temporary failures can appear. All failures during that time will be taking into account in reliability calculations.
2. Outage (Resource will be completely unavailable)
 - ◆ The site/node is completely unavailable and no tickets should be created. This does not affect site metrics.

More information about downtime can be found in GOCDB User Documentation:

http://goc.grid.sinica.edu.tw/gocwiki/GOCDB_User_Documentation

5.4.3.1 Sites in downtime

When a ticket has been raised against a site that subsequently enters downtime time, the expiry date on the ticket can be extended.

When a ticket is open against a site that continues to add downtime the ticket must be closed and the ROC requested to take action either by suspending or uncertifying the site until such time as the problem is resolved. This usually happens when a middleware upgrade is due or a bug in the middleware is causing a site to fail. Sites then may choose to wait for the next middleware release rather than spend effort trying to resolve the issue locally.

Sites that are in downtime will still have monitoring switched on and therefore may appear to be failing tests. ROD must take care that when opening tickets to ensure that they don't open tickets against sites in downtime.

If a site is in DOWNTIME for more than a month then it is advised that the site should go to the uncertified state.

5.4.3.2 Node in downtime

When a node of a site is in downtime alarms are generated but the Operations Portal distinguishes these alarms, and marks the downtime accordingly in the dashboard. ROD should not open tickets against nodes that are in downtime.

5.4.4 Specific accounting test failure instructions

1. If there is more than one APEL failure for a given site, leave one alarm active and mask all others by this one. Create a ticket for the remaining alarm.

2. Edit the description of the ticket to state clearly that even though the failure is reported for a given CE, this is not a CE failure but a failure on the APEL service for the whole site.
3. Proceed with all sites in the same way. Please beware: Do NOT recommend downtime at the second step of the escalation process for this test.

5.4.5 Nodes not in production

When a node of a production site is declared as non-production in the GOCDB or the node appears in BDII but is not declared in GOCDB then the ROD should do the following:

- Recommend to the sites to take these nodes out of their site BDII
- If this is not a possibility then the site should set those nodes in downtime in GOCDB
- If the node is a test node and is in BDII but not in GOCDB then the sites should register it to GOCDB and put monitoring off.

5.4.6 Sites that fail Nagios tests but still continue to be operational

Sites that fail NAGIOS tests where an alarm gets raised on the dashboard, but continue to be operational can be handled as follows: Operators need to set the ticket to "unsolvable" or set a long term deadline. A mail must be sent to the C-COD mailing list and a note put in the dashboard "site notepad". These sites should not be candidates for suspension.

5.5 Best Practices which have turned into instructions

1. Tickets assigned to developers should be followed up regularly.
2. Use the ROD (formerly known as CIC-on-duty) mailing list more frequently for getting help or instructions and important info such as Downtime for Operational tools; Nagios/GOCDB/GGUS/OPERATIONSPORTAL
3. Report problems with tests or cryptic error message in the ROD mailing list.
4. Close tickets that have changed problem type; also close if in doubt.
5. Do not escalate tickets where site admins replied.
6. Try to minimize the number of tickets per site.
7. Use masking of alarms.
8. Try to answer comments from site admins and avoid sending template escalation mails (modify them accordingly.)

5.6 Handover log model

At the end of a shift the current ROD team should prepare the handover for internal ROD matters. Each ROD can decide independently on what the handover should look like and how it should be passed on to the next team. This document just provides suggestions for how it could be:

1. List of tickets which will continue into the next week: name of Site, ROD ticket ID and GGUS Ticket number, current status of the ticket.
2. Report any problems with operational tools during the shift.
3. Did you encounter any issues with the ROD procedures, Operational Manual?
4. Report encountered problems with core grid services.
5. Did you encounter any tickets that changed 'character' ? (One that no longer is a simple incident that can easily be fixed, but rather a problem that may result in a Savannah bug) – This implies that the use-cases wiki needs to be updated.
6. Any alarms that could not be assigned to a ticket (or masked by another alarm)?
7. Any tickets opened that are not related to a particular alarm
8. Anything else the new team should know?

5.7 Communication Lines

ROD should provide an email contact to where all ticket information should be sent and also to make it possible for C-COD or other bodies to contact them directly. For internal communication ROD can use mailing list(s), instant messenger etc. – Each ROD is free to choose how the internal communication is established.

For communication purposes between 1st Line Support and ROD the "site notepad" field in the dashboard should be used. Any additional explanations can be done through e-mail or instant messenger service.

ROD should communicate with C-COD through the C-COD mailing list. For core and urgent matters, it should be done via a GGUS ticket assigned to C-COD to make tracking of the case possible.

5.7.1 ROD Communication Lines

For internal communications, C-COD uses the project-eu-egee-sa1-c-cod-followup@cernSPAMNOTSPAMNOT.ch mailing list, specially created for this purpose: This mailing list is also a place for direct contact with C-COD for other units.

C-COD and other RODs can communicate with RODs in two ways. The former is through the ROD representative in C-COD and the later via direct email to the ROD mailing list. (project-eu-egee-sa1-cic-on-duty@cernSPAMNOTSPAMNOT.ch)

Contact list of individual RODs:

- AP ROD (AsiaPacific): roc@listsSPAMNOTSPAMNOT.grid.sinica.edu.tw
- CA ROD (Canada): roc@triumfSPAMNOTSPAMNOT.ca
- CE ROD (CentralEurope): ce-rod@gridSPAMNOTSPAMNOT.cyfronet.pl
- CERN ROD (CERN): egee-rcod-cern@cernSPAMNOTSPAMNOT.ch
- DE/CH ROD (GermanySwitzerland): grid-support-dech@iwrSPAMNOTSPAMNOT.fzk.de
- FR ROD (France): grid-roc@ccSPAMNOTSPAMNOT.in2p3.fr
- IGALC ROD (ROC_IGALC): roc@igalcSPAMNOTSPAMNOT.org
- IT ROD (Italy): it-roc@infnSPAMNOTSPAMNOT.it
- LA ROD (LatinAmerica): support@roc-laSPAMNOTSPAMNOT.org
- NE ROD (NorthernEurope): roc@egee-neSPAMNOTSPAMNOT.org
- RU ROD (Russia): rcod@egeeSPAMNOTSPAMNOT.sinp.msu.ru
- SEE ROD (SouthEasternEurope): grid-support@egee-seeSPAMNOTSPAMNOT.org
- SWE ROD (SouthWesternEurope): grid.support@lipSPAMNOTSPAMNOT.pt
- UKI ROD (UK/Ireland): uki-grid-ops@cernSPAMNOTSPAMNOT.ch

There is also the handover section in the ROD dashboard which allows for C-COD and RODs to intercommunicate.

In the case of a non-responsive ROD, C-COD should create a GGUS ticket to appropriate ROC Support Unit.

C-COD communicates with other units like OCC, Weekly Operations Meeting, developers, ROC Managers, etc. mainly by emails and GGUS tickets.

6 Monitoring and problem tracking tools

There are currently a variety of monitoring tools in EGEE/LCG which are used to detect problems with sites. They also provide useful information about sites. The operations dashboard provides links and utilises combined views of the most common monitoring tools for performing tasks. The links below are for direct access to some of the monitoring tools used in the operations dashboard.

6.1 Monitoring

The links below are for direct access to some of the monitoring tools.

- Nagios monitoring: https://sam-%INSERT_YOUR_ROC%-roc.cern.ch/myegee. There is a page for each ROC and the details of each ROC's URL can be found on <https://twiki.cern.ch/twiki/bin/view/EGEE/NagiosROCURL> ;
- GIIS Monitor: <http://gstat-prod.cern.ch/gstat/summary/> ;
- GOC Database. <https://goc.gridops.org/> ;
- GOC Real Time Monitor. <http://gridportal.hep.ph.ic.ac.uk/rtm/> ;
- Google Earth. Add the link <http://dashb-earth.cern.ch/dashboard/dashb-earth-all.kmz> ;
- GridView. <http://gridview.cern.ch/GRIDVIEW/> ;
- GridMap. <http://gridmap.cern.ch/gm/> ;

While the above tools are used on a daily basis there are many more monitoring systems available. For a current overview the GOC page on monitoring can be consulted:

- <http://www.ukiroc.eu/content/view/117/265/> .

6.1.1 NAGIOS Availability Monitoring (MyEGEE)

One of the most detailed information pages about possible problems is the MyEGEE Portal, https://sam-%INSERT_YOUR_ROC%-roc.cern.ch/myegee (1). On the front page it also gives two options, *Resource Summary* and *Status History*. There is also a link to the help pages for that portal on the right hand side of this page. The more useful option for operations is the status history.

Status History:

In MyEGEE you can view the status of a site and service according to different profiles by selecting the relevant profile in the 'Profile Selection' drop-down menu. For operational purposes, the ROC_OPERATORS profile should be used. By careful manipulation of the parameters on the right side of the Status History page, you can select the sites and resources of interest to you for viewing. It will be useful to familiarise oneself with this tool by reading the relevant help pages at https://sam-%INSERT_YOUR_ROC%-roc.cern.ch/myegee/help.html .

Two options are possible for further analysis:

- clicking on the history bar at or near a point of failure,
- selecting the table tab.

(Note, it is useful to select a shorter date range at this point, or select the *Current SAM Status (2)* option.) Any failure observed here should be recognised, understood, diagnosed and the follow-up process should be started. This is especially important for failures of the critical tests, which should be treated with the highest priority.

The two options mentioned above provide an abbreviated status of the test results from the probes. They also contain detailed information about each test results by selecting the *Show Detail* widget of a particular result. The detailed reports should be studied to diagnose the problems.

(1) Please replace the whole string `%INSERT_YOUR_ROC%` with your ROC name in capitals, i.e. UKI or SWE.

(2) Please note that SAM in this context does not refer to the old SAM tests.

6.1.1.1 ROC_OPERATORS profile

In the Nagios system there is a set of profiles corresponding to groups of probes instead of a single list of critical tests. A profile is therefore a mapping from a service type to a list of metrics (tests) e.g. for a CE there are about 10 metrics gathered.

A profile may be used for different functionality requirements e.g. for raising notifications to operators (ROC_OPERATORS profile), or for the calculation of availability (ROC_CRITICAL profile - note that this will be renamed to ROC_AVAILABILITY). The list of tests in the ROC_OPERATORS profile for Nagios can be found here: <https://twiki.cern.ch/twiki/bin/view/LCG/SAMCriticalTestsForCODs> .

Over time more profiles will be created for specific tests, or tests which will be applied to specific sets of resources e.g. MPI tests, which should only run on resources which support MPI.

Currently the *old* SAM results are still used for site availability calculations. More information can be obtained on the (*old*) SAM wiki pages dedicated to the (*old*) SAM critical tests for Availability Metrics calculations: <https://twiki.cern.ch/twiki/bin/view/LCG/EGEEWLCGCriticalProbes>

6.1.1.1.1 Procedure to add a test to the ROC_OPERATORS profile

Tests can be added to the ROC_OPERATOR profile so that they generate an alarm in the Operations Dashboard when the tests return an error status.

This change to the ROC_OPERATOR profile must be agreed upon by various management boards, and the procedures outlined below to define a test as critical for the OPS VO must be scrupulously followed.

Please note that in the scope of this document only OPS critical tests are considered.

"Candidate critical tests requests" i.e. new tests which will raise alarms on the dashboard upon failure and which operators on shift should handle are reviewed during the quarterly ROD Forum meetings. Urgent requests can come from the ROCs directly.

In face to face meetings, regular phone meetings or by mail, Operations Procedures (aka 'Pole 2') members (currently project-eu-egEE-sa1-cod-pole2-proc@cernSPAMNOT.ch) will:

- gather input from people attending the ROD Forums meeting and make recommendations to the Nagios team,
- check that all the relevant activities and tools are ready to handle the new critical test.

This can be summarised in the following check-list:

1. Gather ROD feedback on the test implementation;
2. Gather ROD feedback on the impact of the general activity;
3. Record feedback and final recommendations in a GGUS ticket referenced in the wiki;
4. Check that the template mail in the dashboard accounts for the new critical test;

5. Check availability of appropriate links in the dashboard for the new critical test;
6. Check that appropriate instructions are defined in the Operations Procedure Manual.

Once ROC managers validate the new test to become critical for the OPS VO, it is announced to all the sites/ROCs/C-CODs via a BROADCAST during Week (W-2), and announced at the Weekly Operations Meetings one week later (W-1). Based on all feedback gathered in the process, and that they have been approved, these tests will be become critical on week W at the Weekly Operations Meetings time.

The above procedure is summarized in the following list:

1. A request for a new test comes from VO/ROC/Operations
2. The Nagios team evaluate and integrate the test. ROC managers are also officially informed of the new test.
3. The test put into a candidate status to be available on the dashboard as a non-critical test, but still with final "Error", "Warn" or "Ok" flags.
4. A report is submitted by VO/ROC/Operations to ROC managers on the progress of the test. This should include details of sites failing the test (by region).
5. ROCs review results with their sites until 75% of sites pass the new tests.
6. A standing item on the ROC managers meeting agenda is made to accept, reject or request more time until the test is validated. A target of two weeks should be put on this step.
7. Once the ROC managers accept the test, the acceptance is noted at the Weekly Operations Meeting. Wait one week.
8. A broadcast is sent to all sites one week before the test is set as critical. This is also mentioned at the Weekly Operations Meeting.
9. A Broadcast is sent to all sites one day before the test is set as critical.
10. Test is set as critical.

6.1.1.2 Alarm generation in the Operations Dashboard

Alarm generation in the operations dashboard relies on checks of service notifications. The ROC_OPERATORS profile (see the section on ROC_OPERATORS profile above) defines the services that are checked. The decision to send out notifications is made in the service check and host check logic. Host and service notifications occur in the following instances:

- When a hard state change occurs
- When a host or service remains in a hard non-OK state and the time specified by the `</notification_interval/>` option in the host or service definition has passed since the last notification was sent.

Information on state types and hard state changes can be found at the following URLs:

- http://nagios.sourceforge.net/docs/2_0/statetypes.html
- http://nagios.sourceforge.net/docs/2_0/notifications.html

The actual alarm creation is made through a filter, and if the service state changes, this is registered by the filter, stored in a data base and displayed on the dashboard.

6.1.2 GIIS Monitor

There is a new GIIS monitor at CERN: the GStat 2.0 Monitor. It is used to display information about grid services, the grid information system itself and related metrics.

GStat 2.0 does not rely on any submitted job, but rather scans all site GIISes/BDIIs to gather the information and perform sanity checks to point out any potential problems with the information system of individual sites.

The tool covers the following areas:

- Static information published by a site: site name, version number, contact details, runtime environment (installed software);
- Logical information about site's components: CE, number of processors, number of jobs, all SEs, summary storage space, etc;
- Information integrity: bindings between the CE and close SEs.
- Geographical Information
- LDAP query view
- Lists the top level bdiis status
- Useful statistics

The GStat 2.0 provides many different views of the grid; The Site View is similar to that provided by the old GSTAT tool. Filters can be applied to select by Country, EGEE_ROC, Grid, VO or WLCG_Tier, to select the sites of interest. A table is shown with summary information about the sites, including its status and stats for numbers of CPUs, Storage, and jobs. Each site is provided with an individual page with more detailed information about the results of tests and sanity checks that have been performed, and also several plots of historical values of critical parameters. These historical plots are useful for spotting intermittent problems with site's information systems.

Further information about the architecture of the new system.

6.2 Problem tracking

6.2.1 GGUS

In order to keep track of the follow-up process, all operators have to submit each detected problem to a problem tracking tool. The current problem tracking tool is the Global Grid User Support (GGUS) tool, based on Remedy, and run by FZK. It has been in use for grid operations since mid-April 2005. The GGUS ticketing system has two available interfaces:

- The operations dashboard, which should only be used by ROD to report new problems and assign them to ROCs;
- The generic GGUS interface, which should be used by ROCs once tickets are assigned to them. This may be via the local helpdesk if there is a local GGUS interface.

6.2.1.1 Creating tickets

Problem categorization in EGEE/LCG operations of a single problem at each individual site and the associated follow up process is represented by a single ticket in GGUS. In order to organise and categorise the tickets the following structure has been put in place:

- **Ticket:** each ticket represents a problem at a single site;
- **Category:** identifies a site by the site name;
- **Priority:** used internally to mark sites with higher operational importance according to the number of provided resources (big sites - high priority);
- **Item group:** represents a problem type, eg. LCG Version

The task fields which are introduced above describe the individual problems in terms of location (site), type, and importance.

Task field usage: apart from the information provided by the fields which were introduced above, there are a number of fields which describe the details of the problem and current status in terms of escalation procedure. These fields should be utilised as follows:

- **Should be Finished on** - the deadline for the current escalation step;
- **Assigned to** - ROCs are currently responsible for their particular problem;
- **Last action taken** - last action which was taken according to the escalation procedure;
- **Person contacted** - the name, email address and possibly phone number of the person who was contacted in the last action;
- **Response** - a summary of communication with the person responsible for the site in the last action;
- **Summary** - a summary of the problem, it is highly recommended to put the affected host's name in the first part of the summary;
- **Original submission** - the original error message plus any comments that may be useful for problem identification and solving.

NB: Please note that the ticket should not expire during the weekend.

7 Security Items and Daily Operations

7.1 Security matters

Specific security issues or questions can be sent to project-egge-security-support@cernSPAMNOTSPAMNOT.ch. This list contains a list of generic security contacts in each ROC, who will provide a reply. As it is rather difficult to ensure that GGUS tickets are readable only by the affected parties, one should refrain from using GGUS to track operational security issues.

All sites are bound by the JSPG policies listed at <http://cern.ch/osct/policies.html>. The policies cover many areas, including:

- "You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities. The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions." (Grid Acceptable Use Policy, <https://edms.cern.ch/document/428036>)
- "Sites accept the duty to co-operate with Grid Security Operations and others in investigating and resolving security incidents, and to take responsible action as necessary to safeguard resources during an incident in accordance with the Grid Security Incident Response Policy." (Grid Security Policy, <https://edms.cern.ch/document/428008/>)
- "You shall comply with the Grid incident response procedures and respond promptly to requests from Grid Security Operations. You shall inform users in cases where their access rights have changed." (Virtual Organisation Operations Policy, <https://edms.cern.ch/document/853968/>)

7.2 OSCT organization and OSCT-Duty Contact Role

The Operational Security Coordination Team (OSCT, <http://cern.ch/osct>) provides an operational response to security threats against the EGEE infrastructure. It focuses mainly on computer security incident handling, by providing reporting channels, pan-regional coordination and support. It also deals with security monitoring on the Grid and provides best practices and advice to Grid system administrators.

The OSCT is led by the EGEE Security Officer and includes security contacts from each EGEE region. The OSCT Duty Contact (OSCT-DC) role is assigned on a weekly basis to one of the ROC Security Contact persons who provide support for daily security operations, according to a schedule defined by the OSCT.

The OSCT-DC must perform the following actions:

1. All reported incidents **should** be coordinated by the ROC Security Contact of the site reporting the incident (although this responsibility **MAY** be delegated in the region), but the OSCT-DC **must** ensure a timely coordination of the incident effectively happens, which includes assuming responsibility to coordinate himself/herself in an appropriate time frame if needed. More details about the role of the incident coordinator are available in the EGEE incident response procedure.
2. Ensure that appropriate action is taken in a timely manner (often by the affected ROC) to solve ticket assigned to the GGUS Security Management unit or to any matter being raised on the team's mailing list.
3. If necessary, attend the weekly OPS meeting and report or follow-up as appropriate within the OSCT
4. Send a report to the OSCT list, before lunch time on the Monday following the duty week, containing a summary of the issues of the week and those that are carried over from a previous week. This handover should also be carried over the weekly security operations phone meeting to enable the current and next OSCT-DC to discuss open issues.

5. Write new (or update) 'best-practice' items for the security RSS feed, based on advisories from GSVG (items should be sent to project-egEE-security-officer@cernSPAMNOTSPAMNOT.ch to be published) If the issue posted by GSVG requires urgent action, raise it at the weekly OPS meeting and send a specific EGEE broadcast after consulting the rest of the OSCT

6. Monitor CA updates and monitor the update process as described in (http://goc.grid.sinica.edu.tw/gocwiki/Procedure_for_new_CA_release).

A backup OSCT-DC is defined in the same manner whose role is expected to cover situations such as prolonged unexpected network outage with the Lead site.

7.3 Security incidents handling and Interaction with OSCT-DC

OSCT- Duty Contacts (OSCT-DC) are members of the OSCT group that provide security coordination at a given week in tandem with the C-COD team. OSCT-DC has to be ready to respond to tickets created on security matters that given week.

If a security incident is suspected, the EGEE incident response procedure, which is available and maintained at <http://cern.ch/osct/incident-reporting.html>, being an excerpt from the full procedure https://edms.cern.ch/file/867454/2/EGEE_Incident_Response_Procedure.pdf, must be used.

When a security related ticket is created by a site, VO or user, the OSCT-DC should then assign the ticket to the Security Support unit. They then follow-up the issue according to the OSCT regulations summarized above, taking into consideration the restricted information and contact details they have access to.

Security incidents are handled via the communication channels described on the procedure and must not be discussed via GGUS. If a security incident is initially discovered via GGUS, communication with the affected parties must be switched to the appropriate channels and the existing ticket should be closed and only used later as a reference.

However, 1st Line Support may have to act rapidly according to OSCT-DC instructions depending on the severity of the incident. 1st Line Support should also inform ROD about the situation. ROD can then act as a follow up contact.

7.4 Grid Security Vulnerability Handling

Reason for a Vulnerability handling process

A lot of care is taken to ensure that Grid software and its deployment is secure, however from time to time, Grid Security Vulnerabilities are found. Grid Security Vulnerabilities are problems in the software or deployment which may be exploited in order to create an incident. Such problems need to be resolved in a timely manner in order to prevent incidents, and, while this is happening, it is important that they are not advertised to potential hackers. Hence, within EGEE a process has been established for reporting and handling vulnerabilities which is run by the EGEE Grid Security Vulnerability Group (GSVG).

Reporting a Vulnerability

If a possible vulnerability is found an e-mail should be sent to

grid-vulnerability-report@cernSPAMNOT.ch

Alternatively, the issue may be entered as a "bug" in the GSVG savannah at <https://savannah.cern.ch/projects/grid-vul/> for obvious reasons these bugs are set to "private" so only a limited number of people can browse them.

Note that if a vulnerability has been exploited, it is an incident and the incident handling procedure should be followed.

Handling of issues reported.

The GSVG will investigate the issue, and inform the reporter of the findings. If the issue is found to be valid then the Risk Assessment Team will place the issue in one of 4 Risk categories, each which has a corresponding Target Date.

Risk Categories

* Extremely Critical - Target Date = 2 days

* High - Target Date = 3 weeks

* Moderate - Target Date = 3 months

* Low - Target Date = 6 months

It is then the responsibility of the appropriate development team to produce a patch. This issue will be kept private until either a patch is issued to resolve it, or the target date is reached.

On resolution or reaching the Target Date

An advisory will be released. Hopefully, in most cases a patch will be issued in time for the Target Date. Advisories are now placed at <http://www.gridpp.ac.uk/gsvg/advisories/>. Advisories should reference the release, and release notes reference the advisory.

Further Details

Details of the issue handling process is available in the document entitled 'The Grid Security Vulnerability Group - Process and Risk Assessments for Specific Issues' at <https://edms.cern.ch/document/977396/1> .

More information on the Grid Security Vulnerability Group is available at <http://www.gridpp.ac.uk/gsvg/>.

Other notes

If the issue is found to be operational, rather than being due to a software bug, then an advisory will be set to the OSCT. Please refrain from discussing vulnerabilities on open mailing lists, logged mailing lists, or reporting them as 'bugs' in open bug reporting systems.

The GSVG was setup to primarily handle vulnerabilities and improve the security in EGEE gLite Middleware, and does not handle vulnerabilities in operating systems, or in non-Grid software. However, if such issues are reported to the GSVG they will attempt to pass information onto the relevant party.

8 References

- [1] CIC Portal
 - [2] Operations Dashboard
 - [3] GOCDB
 - [4] Global Grid User Support
 - [5] GIIS Monitoring pages
 - [6] Availability report page
 - [7] SAM Nagios Documentation page
 - [8] Generic Nagios Documentation (CGI)
 - [9] GOC Wiki page
 - [10] EGEE broadcast tool
 - [11] Dashboard HOWTO Guides
 - [12] Best Practices
 - [13] Intervention Procedures& Notification Mechanism
 - [14] Site/ROC Association document
-

This topic: EGEE > OperationalProceduresforROD

Topic revision: r44 - 12-Apr-2010 - 03:20:35 - VeraHansper

 Copyright &© by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

Ideas, requests, problems regarding TWiki? Ask a support question or Send feedback