EGI-InSPIRE

Dashboard Howto
User Guide

EGI-InSPIRE Technical Document
Andres Aeschlimann SWITCH
David Bouvet IN2P3
Esteban Freire García CESGA
Vera Hansper CSC
7. Apr 2011 version 4
https://documents.egi.eu/public/ShowDocument?docid=301

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Overview

The “Operational Dashboard” is a set of tools and interfaces dedicated to the daily work of Regional Staff (1st line support and ROD teams), Site Administrators and COD and can be accessed on the Operations Portal at: https://operations-portal.egi.eu/. It ensures smooth and effective Grid operations by having every necessary information ready at one place.

The Dashboard is primarily a graphical user interface. It contains a number of icons, which will be described and used throughout this documentation. For an effective and efficient workflow it is necessary that staff using the Dashboard are familiar with these icons.

This document is primarily aimed at Regional Staff, though Site Administrators and COD staff can also make use of the descriptions contained herein. A complimentary Operations Procedure Manual can be found on the EGI wiki at https://wiki.egi.eu/wiki/Operations_Manuals .

All acronyms used in this documentation are defined in the Glossary.

1.2 Prerequisites for accessing the Dashboard

The user must

- have a valid Grid certificate which is correctly imported into their web browser
- be defined in the GOCDB, with either a “Site” or “Regional” role.

Note that support staff with a Site role will only be able to view their site, and the actions available to this role are limited.

1.3 Connections to other systems

The “Operational Dashboard” is connected to other central Grid tools: the notification section of the Regional monitoring instances, the GOCDB and the GGUS system.

1.3.1 Notifications passed to the Dashboard

The monitoring systems are configured such that failing tests are automatically reported to the Dashboard system.

1.3.2 GOCDB

Static information about sites and nodes are taken from the GOCDB.

1.3.3 GGUS

The Dashboard is connected to the GGUS System through SOAP web services. The Dashboard can be used to create GGUS tickets, with many fields prefilled with the necessary information available in the Dashboard.

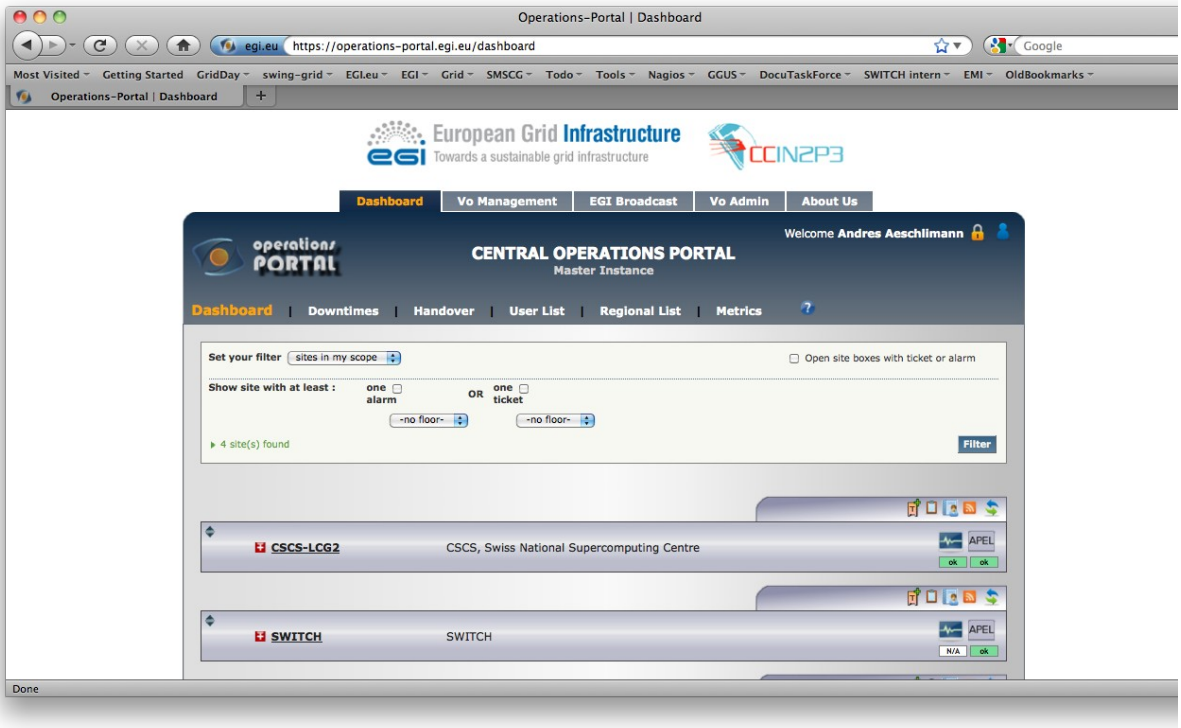
2 DASHBOARD/DASHBOARD MAIN PAGE

2.1 Overview

Please note that the notion “Dashboard” is used

1. as a tab on the first level (other tabs are VO Management, EGI Broadcast, VO Admin, About Us)
2. as a tab on the second level (other tabs are Downtimes, Handover, User List, Regional List, Metrics)
3. as the name of the system accessible on https://operations-portal.egi.eu/

We will use dashboard/dashboard to refer to the screen below, ie. with “Dashboard” selected on the first *and* second level. The content of the screen may vary depending on your role (defined in GOCDB).



The sections of the whole page include (from top to bottom):

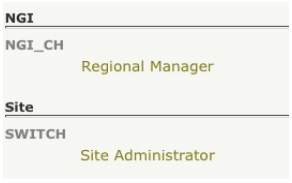
- a (dark blue) heading with general information
- a (beige) display options section used to filter the list of sites displayed according to your specifications
- a list of sites with additional information and manipulation options
- a footer with useful links

All subsections (Dashboard, Downtimes, Handover, User List, Regional List and Metrics) are presented in this document.

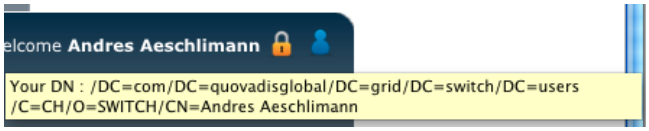
The Dashboard HOWTO is available through the link in the small blue question mark in the heading.

2.1.1 User information

Moving the mouse over the small blue profile in the top right corner of the heading will display your different roles defined in GOCDB, like eg.

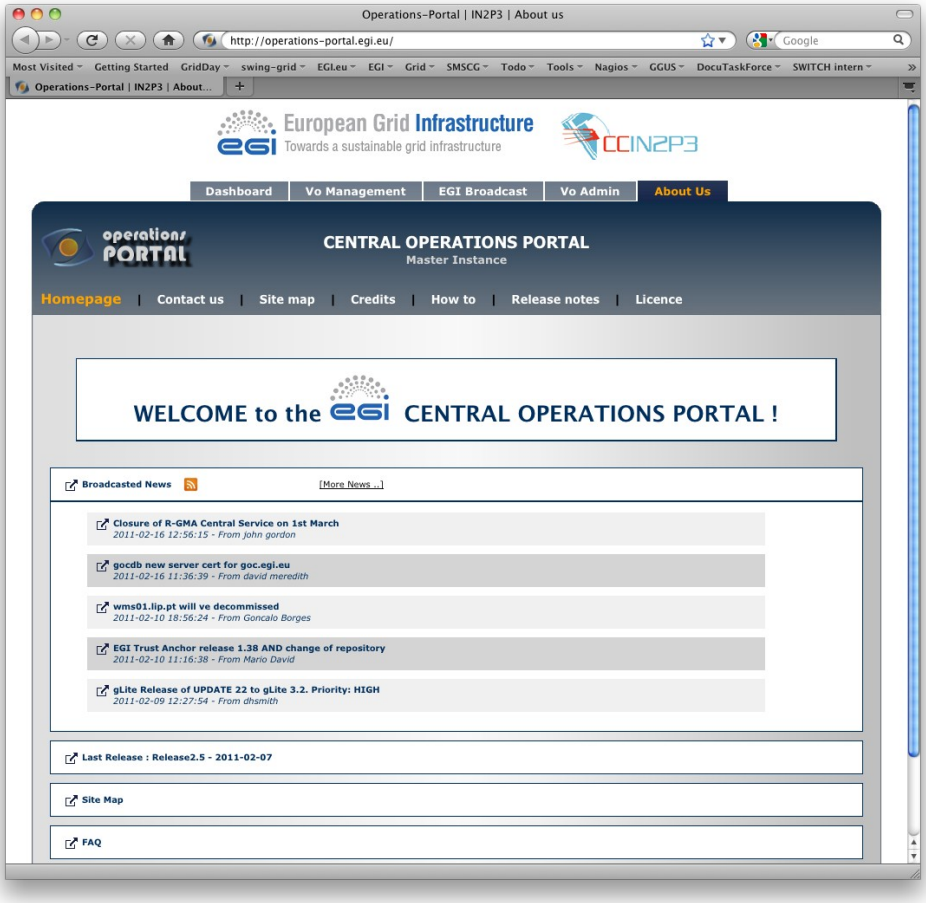


Moving the mouse over the lock icon will display the DN of the certificate you have presented:

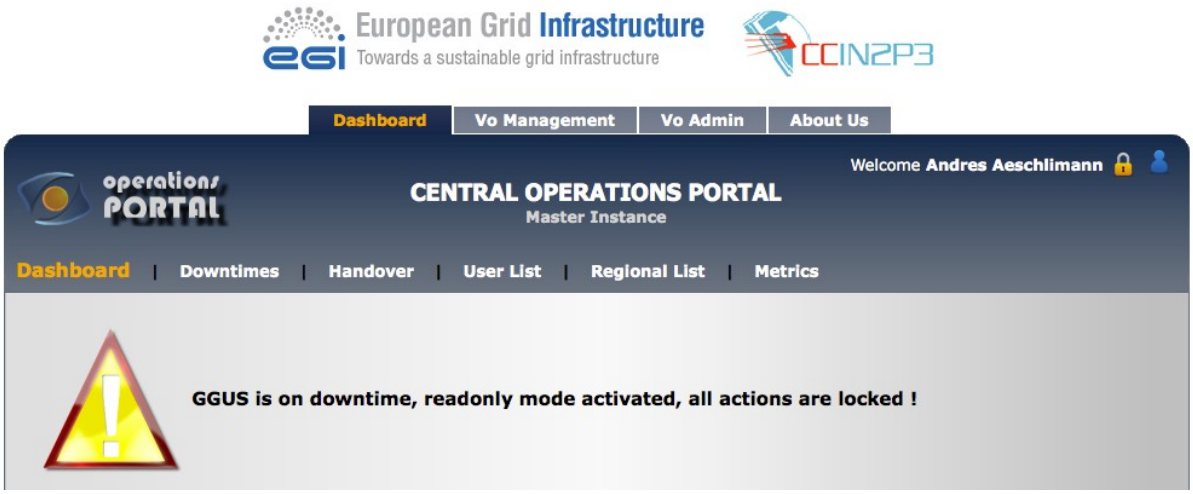


2.1.2 Entry screen

Generally, people access the Operations Portal via the home page of the portal:
https://operations-portal.egi.eu/
The first screen you may see is the following one:



Please carefully read the latest information there before switching to the dashboard/dashboard tab. You may also encounter important information like



2.1.3 Display options

This section is used to filter the list of sites displayed according to your specifications.

The filter section allows you to

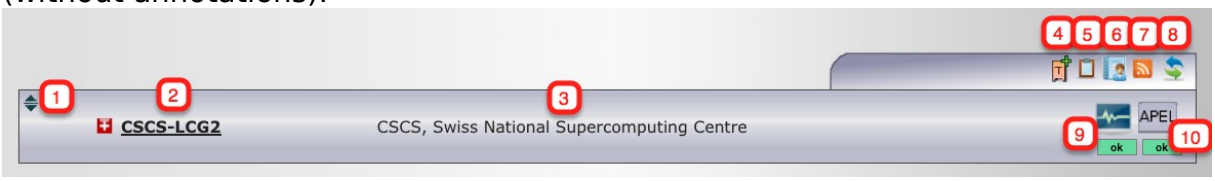
- display sites either within your scope or a specific NGI
- display only sites with at least one alarm, or more specifically, one alarm
  - in the last 24 hours,
  - in the period between 24 and 72 hours back,
  - older than 72 hours
- display only sites with at least one ticket, or more specifically,
  - at least one ongoing ticket,
  - at least one expiring ticket,
  - at least one expired ticket
- directly open the drop down site boxes with alarms and/or tickets by selecting “Open site boxes with ticket or alarm”

You will be prevented from acting upon sites not in your scope. These locked sites will appear with a lock sign at the left side of the country flag:

Personalised lists of sites can be configured out of the sites in your scope. For details please refer to the section User List tab.

2.2 Site Bar

When a site has neither alarms nor tickets open, it will look similar to this (without annotations):



Possible actions are:

1 Click on the drop down symbol to display site details Drop down menu at a site level

2 Click on the short name of the site to get the GOCDB information of a site

3 The long name of the site

4 Click on the ticket symbol to open a ticket (see What you should know about tickets)

5 Click on the notepad symbol to send a note to this site, the NGI (management) and/or the ROD team (see Notepad)

6 Click on the site report symbol to display the site report (see Site report)

7 Click on the RSS feed symbol to subscribe to the RSS feed for Nagios notifications

8 Click on to refresh the displayed data

9 Click on to display GStat information for the site

- ok indicates that all GStat data is provided for this site
- N/A indicates that no GStat data is provided for this site
- warn indicates that some GStat data is provided for this site
- crit indicates that the information is missing or out of date and should be checked

10 Click on APEL to display APEL information about the site

- ok indicates that APEL data is provided for this site
- N/A indicates that no APEL data is provided for this site

2.3 Additional icons and visual effects

These additional icons or visual effects may appear within the list of sites section:

indicates that new alarms have arrived. The number of new alarms is likewise indicated. (see New alarms).

indicates that <number> alarms have been masked, (see Masked alarms).

indicates one or more open tickets on the site (see What you should know about tickets).


indicates that the whole site is in a downtime period.


indicates that a node or a service (endpoint) at a site is in downtime (see Downtimes)

A site with a red border

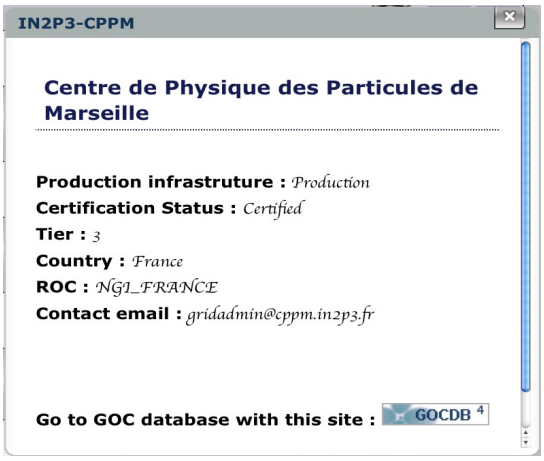
is visible in the COD-Dashboard. This indicates that either alarms or tickets have not been dealt with in a timely manner. See “escalating tickets” in the Tickets section.

2.4 General drop down information

This section aims at familiarising the operator with the existence of related tools. Detailed information about the use of the extra tools contained within this section are out of the scope of this HowTo.

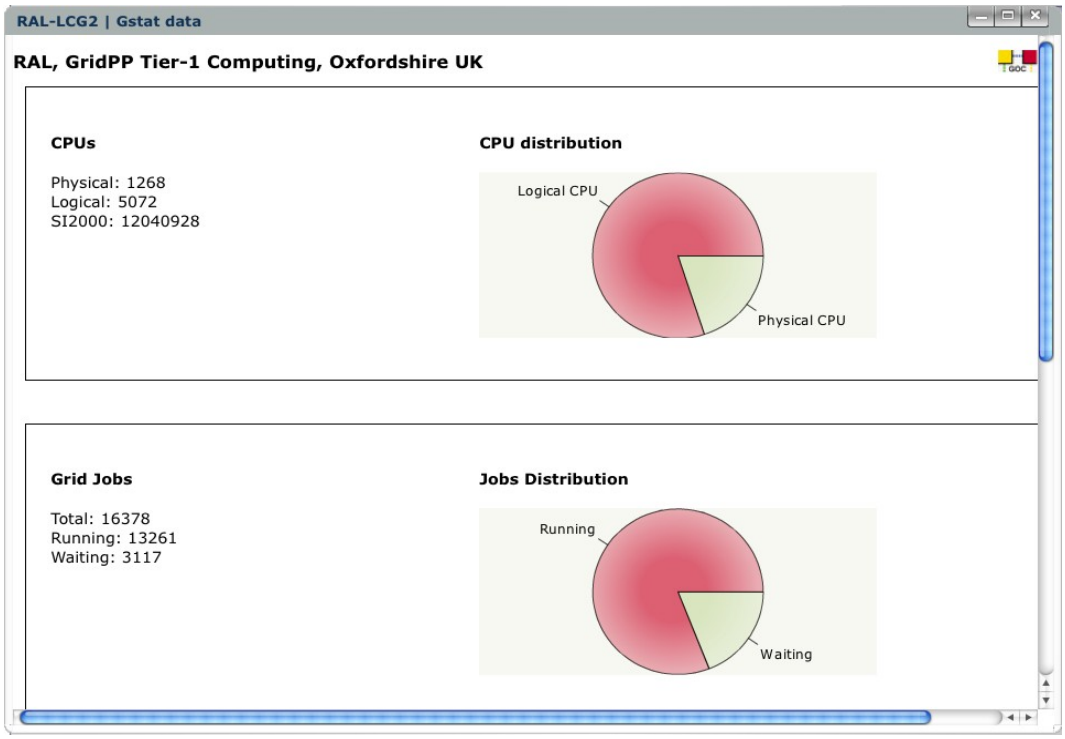
2.4.1 GOCDB information of a site

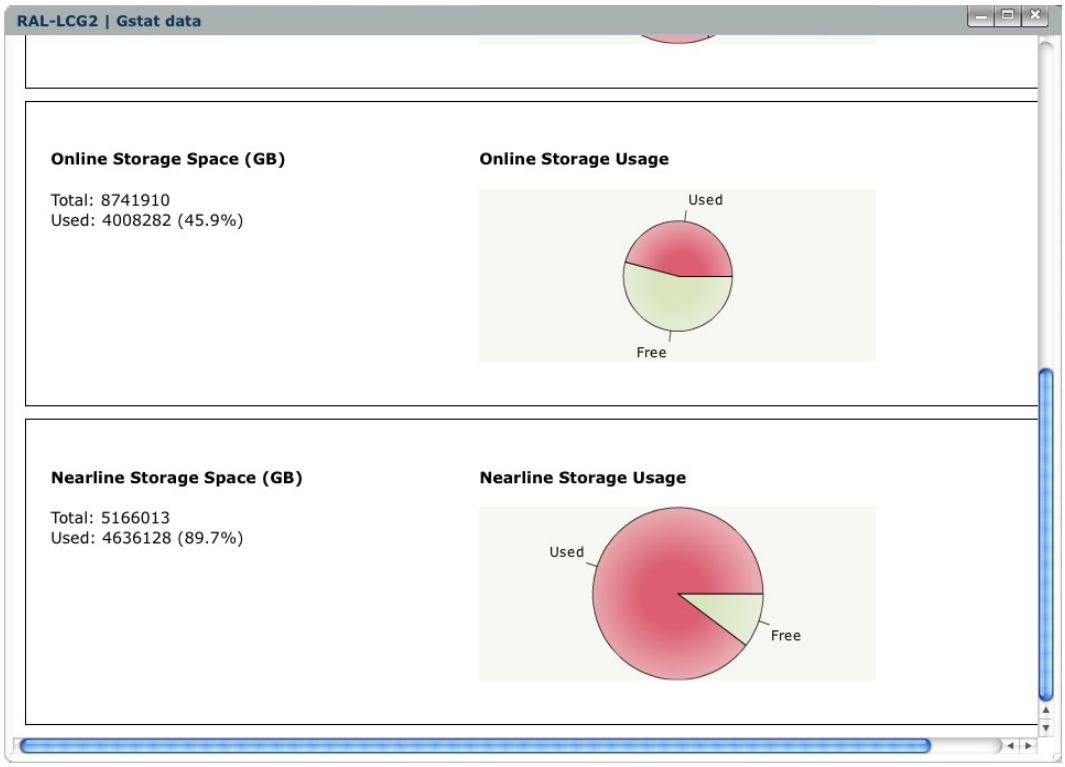
Click on the **name** of the site to get a pop-up window with summary information about the site stored in the GOCDB. A direct link to the GOCDB visualization portal is provided for more site details:



2.4.2 GStat information

The main aim of GStat [9] is to display information about grid services, the grid information system itself and related metrics. GStat information in the Dashboard may appear as follows:

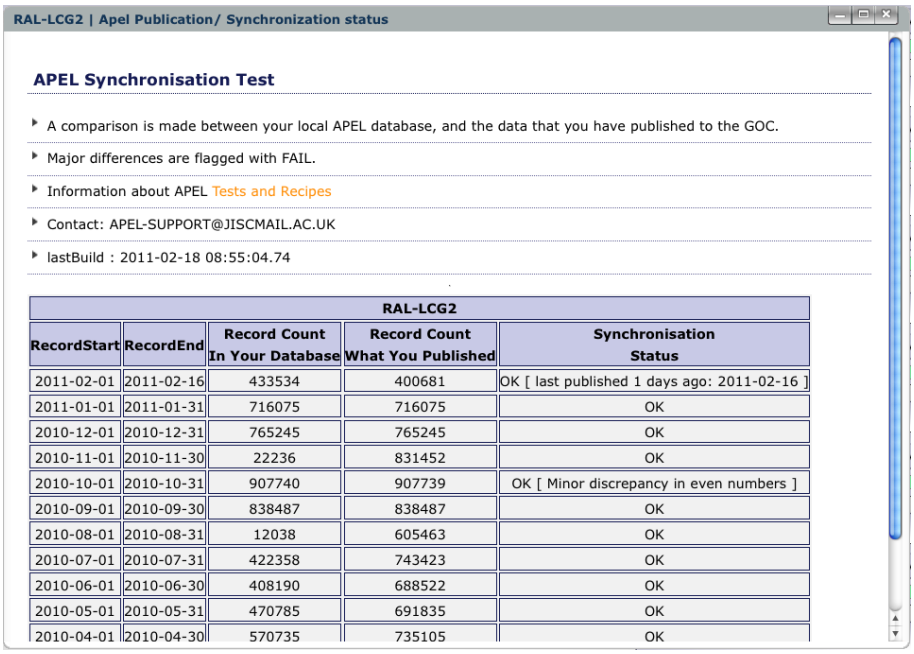




You may see an animation when opening the GStat window.

2.4.3 APEL information

APEL [10] compares published data in the local APEL database and GOCDB and flags major differences.



RAL-LCG2 | Apel Publication/ Synchronization status

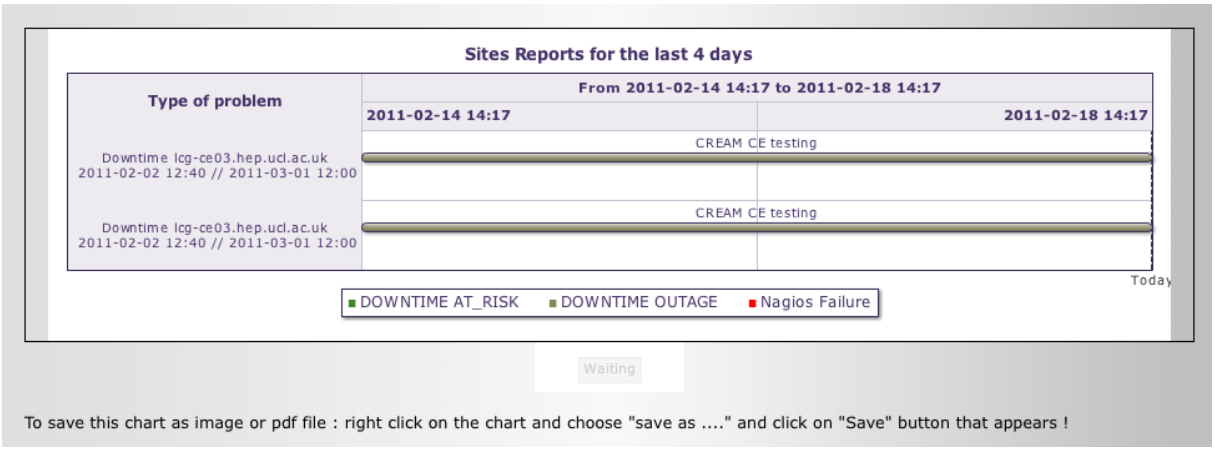
APEL Synchronisation Test

- A comparison is made between your local APEL database, and the data that you have published to the GOC.
- Major differences are flagged with FAIL.
- Information about APEL Tests and Recipes
- Contact: APEL-SUPPORT@JISCMAIL.AC.UK
- lastBuild : 2011-02-18 08:55:04.74

RAL-LCG2				
RecordStart	RecordEnd	Record Count In Your Database	Record Count What You Published	Synchronisation Status
2011-02-01	2011-02-16	433534	400681	OK [last published 1 days ago: 2011-02-16]
2011-01-01	2011-01-31	716075	716075	OK
2010-12-01	2010-12-31	765245	765245	OK
2010-11-01	2010-11-30	22236	831452	OK
2010-10-01	2010-10-31	907740	907739	OK [Minor discrepancy in even numbers]
2010-09-01	2010-09-30	838487	838487	OK
2010-08-01	2010-08-31	12038	605463	OK
2010-07-01	2010-07-31	422358	743423	OK
2010-06-01	2010-06-30	408190	688522	OK
2010-05-01	2010-05-31	470785	691835	OK
2010-04-01	2010-04-30	570735	735105	OK

2.4.4 Site report

A site report contains information about downtimes and Nagios failures in the last 4 days and may appear as follows:



If no nodes at the site are in downtime or failed the Nagios tests then the site report is empty.

2.5 What you should know about alarms

Problem detection on services is done by Nagios probes which have been implemented for the different services at the sites (CE, BDII, SRM…). The probes themselves can consist of single or multiple sets of tests for a specific functionality of a service. Each time an error is detected by one of the tests from these probes, a notification is sent. The Dashboard is connected to the notification section of the Nagios boxes. A filter is applied to only monitor the Operations tests. The notifications which successfully pass the filter are registered in the Dashboard DB with a problem ID and are displayed as an alarm in the dashboard. If the problem ID is already registered, the existing alarm is just updated (i.e. same problem but a change has occurred in the status) Note, the terms **test** and **Nagios test** will imply an **Operations Test**, from the NGI's regional Nagios instance, which may be used interchangeably in this document.

For each alarm, the following set of information is available:

- test that failed
- impacted node
- current status of the test
- output of the test
- date of the failure
- alarm age
- corresponding site

New alarms are shown in the Site Bar as well as in the New NAGIOS alarms drop down menu. Other alarms may appear in either of the two.

2.5.1 New alarms

When a Nagios test fails at a site, a new alarm (orange) appears in the Site Bar of the dashboard. The new alarm icon shows the presence and the number of new alarms. Moving the mouse over the icon displays the age of the alarms in hours:

This icon remains in the Site Bar as long as the alarm has not been handled. The next time a failure is registered for the same test on the same endpoint an alarm will not be triggered unless the existing one is set to off.

When an alarm has been masked by another alarm, which in turn is set to *off*, the masked alarm will then be shown as *new*.

2.5.2 Assigned alarms

When a ticket for an alarm has been created, the alarm is considered as *assigned*. It will then no longer appear in the site bar itself, but in the assigned alarms drop down menu of the site. In the site bar, a ticket symbol will appear instead (see Additional icons and visual effects).

2.5.3 Masked alarms

In certain cases, several Nagios tests on a given site may fail at the same time. If this happens, it can be useful for the site administrator and the ROD team to concentrate on specific alarms and mask the others, ie. temporarily ignoring them. Every masked alarm has, by definition, a corresponding masking or parent alarm.

The grey icon in the site bar indicates the presence and the number of masked alarms.

When the parent alarm is set to off, the previously masked alarm is *unmasked* and is set to

- **off** for the case where the corresponding test succeeds
- **new** otherwise.

2.6 What you should know about tickets

The tool used for ticket handling is GGUS. However, through the SOAP interface, the Dashboard is capable of handling specific tickets related to alarms at sites. When creating a ticket through the dashboard, many fields are automatically filled with the information available in the Dashboard. In order to create a ticket you need to be a member of your NGI's ROD team, and have a Regional role in the NGI. ROD staff should **only** use the Dashboard to create, update and close tickets against Dashboard alarms.

Once an alarm has been assigned to a ticket, this alarm will disappear from the site bar and a ticket symbol will be displayed.

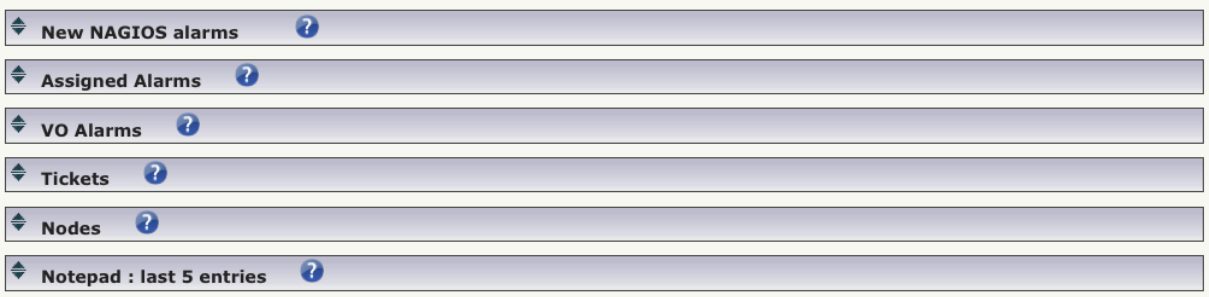
While ticket creation is best done through the alarms drop down menu, ticket update or closure is done through the ticket drop down menu. Please refer to the New NAGIOS alarms paragraph below for ticket creation and to the Tickets section below for ticket update and closure.

2.7 Drop down menu at a site level

Use this icon  in the upper left corner to get more information about an item. The following sub-items may appear for a site:

- New NAGIOS alarms (these are only displayed when new Nagios alarms are present)
- Assigned Alarms (these are only displayed when assigned alarms are present)
- VO Alarms
- Downtimes (these are only displayed when the site or an endpoint is on downtime)
- Tickets (these are only displayed when there are open tickets against this site)
- Nodes
- Notepad: last 5 entries

Example:

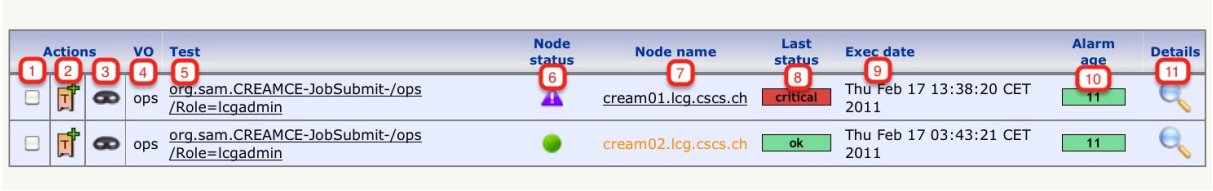


For every sub-item, an online help is available with the button. In this example, the “downtimes” sub-item is missing as no downtimes were relevant to the example site. The following sections deal with these sub-items in more detail. The system implements the following write and read access rules for site's items:

- Site (Resource Centre) staff can view alarms, tickets and add notes to the notepad for their site.
  - site administrators cannot act on the alarms or create tickets. They can use the notepad to provide information about the site to the ROD team.
- Regional Staff can act on alarms, create tickets, or add notes in the notepad for a site
- in the COD view tab, COD staff have the same privileges as Regional Staff, but they only see:
  - alarms in the “new” state for more than three days (72 hours)
  - open tickets which are older than 30 days
  - tickets which have passed their expiration by 3 or more days
  - tickets in the last escalation step

2.7.1 New NAGIOS alarms

Within the “New NAGIOS alarms” drop down list you see a list of alarms similar to this one (without annotations):



Possible actions are:

1 Select the appropriate alarms and click on Close selected alarms to close these alarms. This action *should* only be made on alarms in an **OK** state.

2 Click on to open a ticket for this alarm. See below for details. After successful creation of a ticket, the alarm will be filed under *Assigned Alarms*.

3 Click on to mask other alarms by this one, which will become the *parent alarm*.

4 The VO that the Nagios tests are run under, usually “ops”.

5 Exact name of the Nagios test, with a link to its description in the wiki.

6 The status of the service endpoint in question, see Nodes

7 Click on on the node name to get the Service Status Details from the Nagios server.

8 The result status of the last run of the Nagios test

9 The time stamp of the last run of the Nagios test

10 The age of the alarm (in hours)

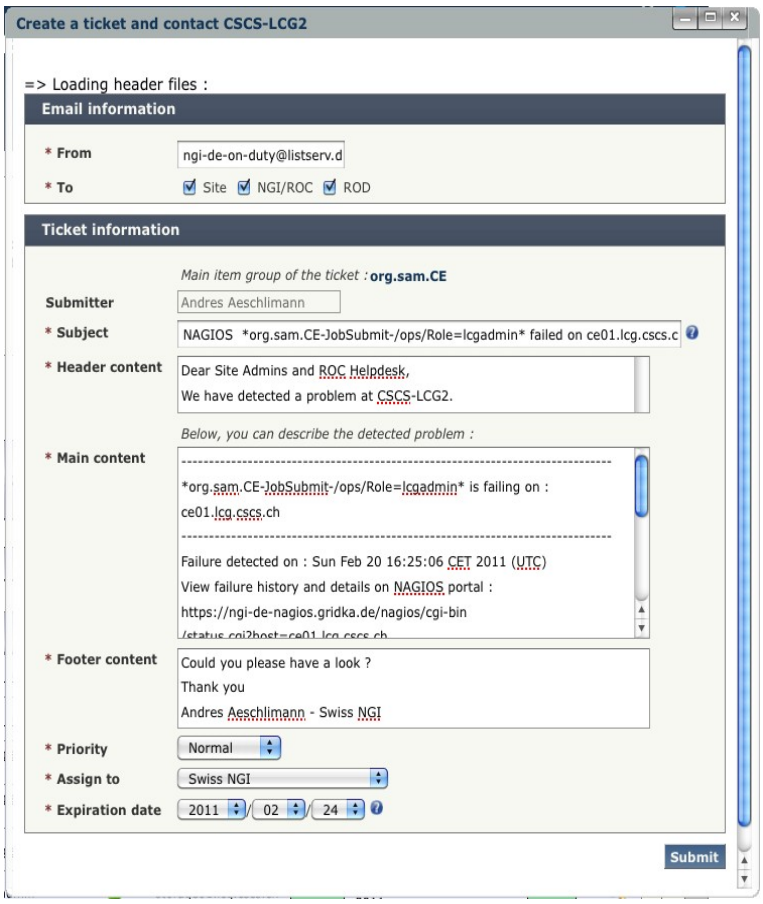
11 A history of the test results.

Ticket creation: The most common way of creating a ticket in the dashboard is through the create ticket button () for a specific new NAGIOS alarm. The create ticket button in the site bar should be used with caution, so consider creating a ticket for a specific alarm (see Tickets.) ROD staff must create a ticket for every alarm which is older than 24h.

Creating a ticket for a specific alarm assigns the alarm to the ticket. From then on, the alarm is defined as *assigned*.

If the assigned alarm was masking other alarms at ticket creation time, all masked alarms are still associated with the assigned alarm and appear in grey in the “Assigned Alarms” subsection. When the ticket is closed, the parent alarm is set to off. Masked alarms are “unmasked” and if the current status of the test is OK, the alarm is set to **off**. If not, the alarm is set to **new**.

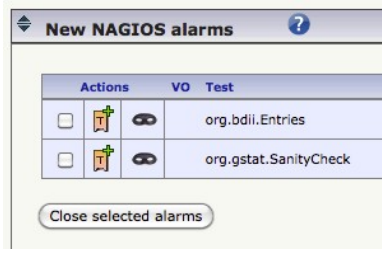
Creating a ticket for an alarm is done through the form below. Masked alarms will appear in the ticket under “Related problems detected” section in the ticket main content. All information is obtained automatically (site, NGI/RIP, Operations Centre, and COD contacts, site name, node, problem summary, ticket submission text and mail body). There is normally no need to change these entries unless you want to explicitly add information about the type of problem. “Subject” and “Main content” fields provide all the necessary information about the problem to create the GGUS ticket.



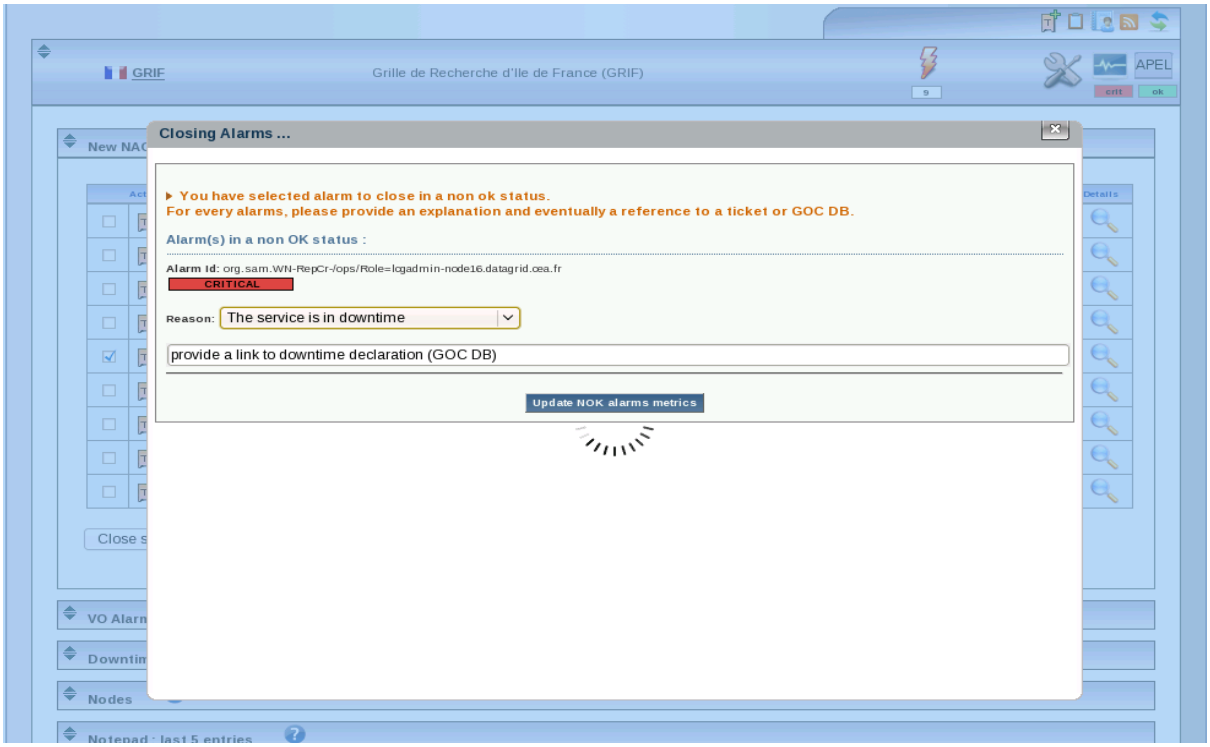
Masking of alarms: When an alarm has been masked, it will be shown by an appropriate icon on its line  . A masked alarm cannot be closed nor can a ticket for this alarm be created. This blocking action is indicated by the  icon. Click on the  button in order to unmask a masked alarm.

2.7.2 Closing Alarms

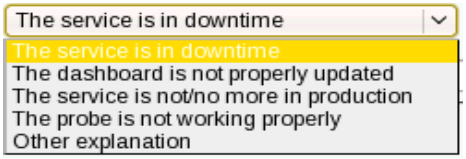
Once the reason for a failing Operations test has been removed, the test will again succeed and the corresponding alarm can be closed.



For the case where the Nagios test continues to fail, the ROD on shift will be asked to explain in a pop-up window why they are closing the failing alarm



with the following drop down menu

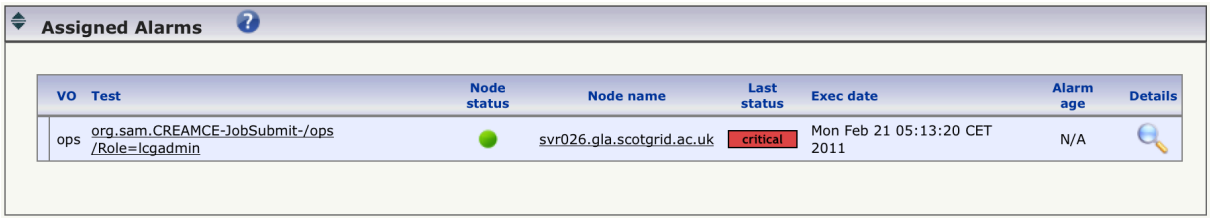


For the case where the alarm appeared during a downtime, the ROD on shift **MUST** provide the GOCDB downtime link.

The alarm will reappear with its age reset if the corresponding Nagios test fails again at the next check. COD uses the statistics of closed alarms in a failed state for its reporting. See also Metrics tab.

2.7.3 Assigned alarms

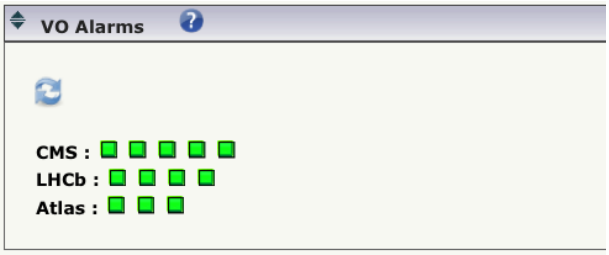
This subsection shows the alarms which are assigned to a ticket. The attributes are the same as for New NAGIOS alarms, however, the alarm age is now suppressed.



For any assigned alarm, a corresponding ticket exists under the ticket subsection.

2.7.4 VO alarms

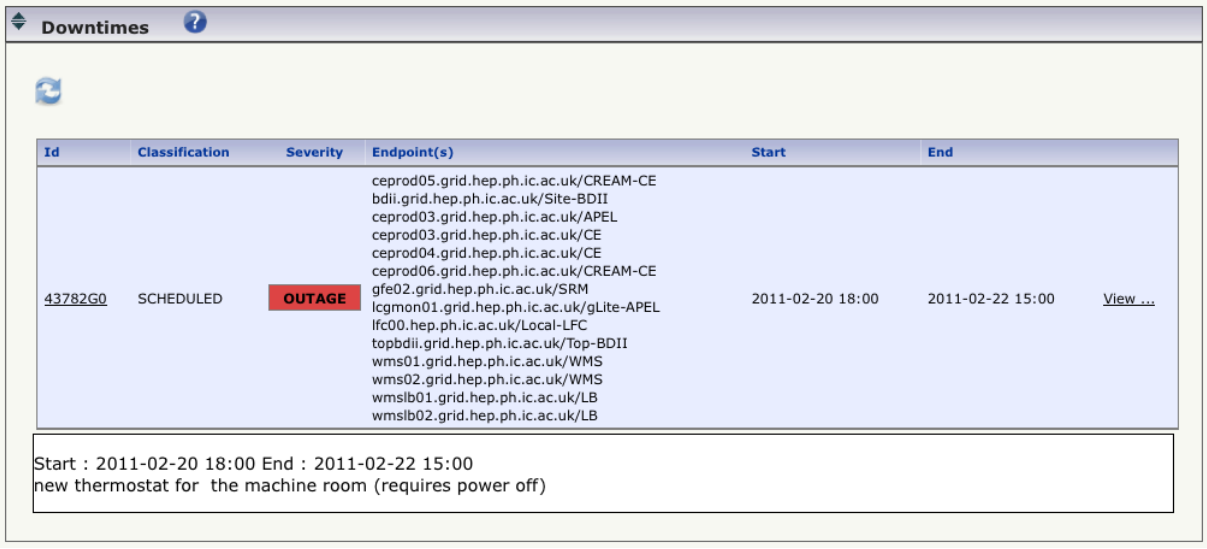
This sub-menu is a synthetic view of the last status of the nodes of the sites for LHC specific tests. By passing the mouse over the small coloured squares you can obtain some details about the status.
Example:



2.7.5 Downtimes

Downtimes details of service endpoints are reported here.

A site administrator may enter a downtime for some of the service endpoints through GOCDB. During the downtime period, the downtimes drop down subsection presents the actual downtimes for the service endpoints, with a link to the entry in the GOCDB.



At the same time, on the site bar, a summary is displayed when the mouse is over the  icon.
Example:

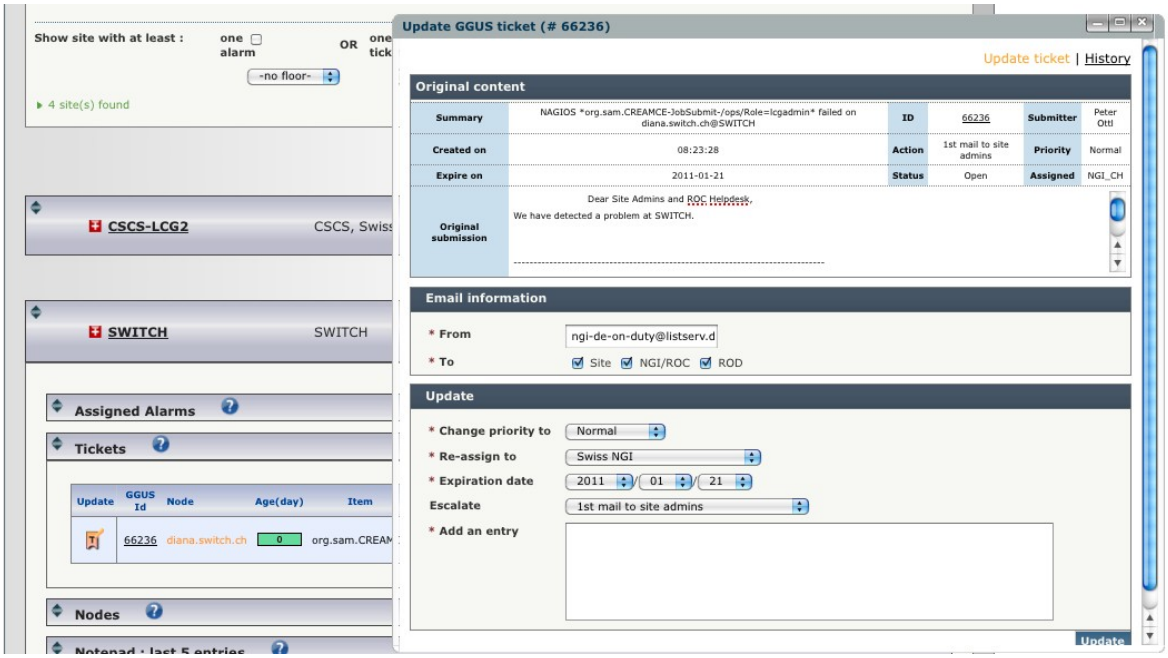
2.7.6 Tickets

For a given alarm, a ticket may already have been created using the buttons described in the section New NAGIOS alarms, which caused the alarm to move to the Assigned alarms section. The corresponding ticket will then appear in the current section about tickets.

Example:

Updating Tickets: Tickets which have been created through the Dashboard should **only** be updated through the Dashboard. A ticket can be updated without any escalation when providing information or further requests to the site. Note that the expiration date is **not** changed automatically, and it is important to change it accordingly.

Click on  to update, escalate or close an existing ticket through the form below.



Mandatory ticket attributes like the name of the submitter or the assigned support unit are denoted with a red star at their left side.

Escalating tickets:
There are certain escalation criteria for tickets:

- A ticket SHOULD be answered immediately and solved within 3 working days (72 hours)
  - A ticket not responded to after 72 hours MUST be escalated by the ROD staff as a 2nd reminder (2nd step in "Escalate "drop down menu)
  - After a further 72 hours, escalation must then be made to COD. (Political Procedure in "Escalate" drop down menu)
- A ticket which has expired for more than 72 hours will be automatically escalated to COD, and sites with such tickets will be shown with a red border around their site bar.

Again, note that when escalating a ticket, the expiration date is not updated automatically.

You can also click on the "GGUS Id" to directly view the ticket within GGUS. This can be useful for reading some of the history in the ticket which may not be displayed from within the Dashboard. However, you must use the Dashboard for updating and closing tickets which have been created by the Dashboard. Clicking on the node name leads to the Nagios service status for this node on the Regional Nagios instance. All further necessary information like Ticket Age, reference to the Alarm, submitter, NGI or RIP, expiration date, last action taken and alarm status is shown on the ticket line.

Closing tickets: When the cause for a failing Nagios test is removed, the test will become green again at the next run. These are the normal circumstances to close the tickets and the assigned alarms.

To close a ticket, click on the update ticket icon  , and then choose "Problem solved" or "Problem unsolvable" in the "Escalate" drop down menu. You will be invited to provide a solution if not already provided by the site.

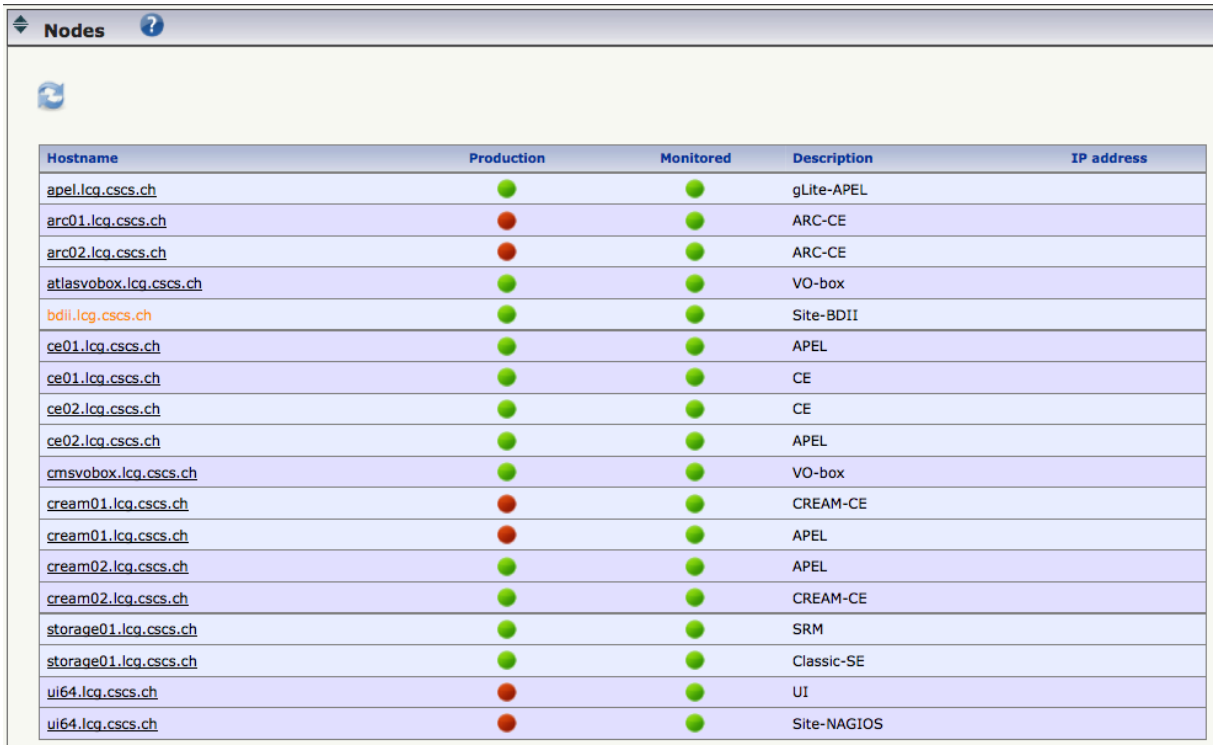
Tickets which have been created through the Dashboard should only be closed through the Dashboard.

When the ticket is closed, the parent alarm is set to off. Masked alarms are "unmasked" and if the current status of the test is OK, the alarm is set to **off**. If not, the alarm is set to **new**.

Cancelling a ticket modification: If for some reason you have made a mistake while attempting to update a ticket, simply close the pop-up window. Submission of the updates to the ticket only occur when the "Update" button is clicked.

2.7.7 Nodes

Nodes are also called services or service endpoints. Usually, a site will have a number of them. A list of nodes, which is queried from the GOCDB, may look similar to:



Nodes

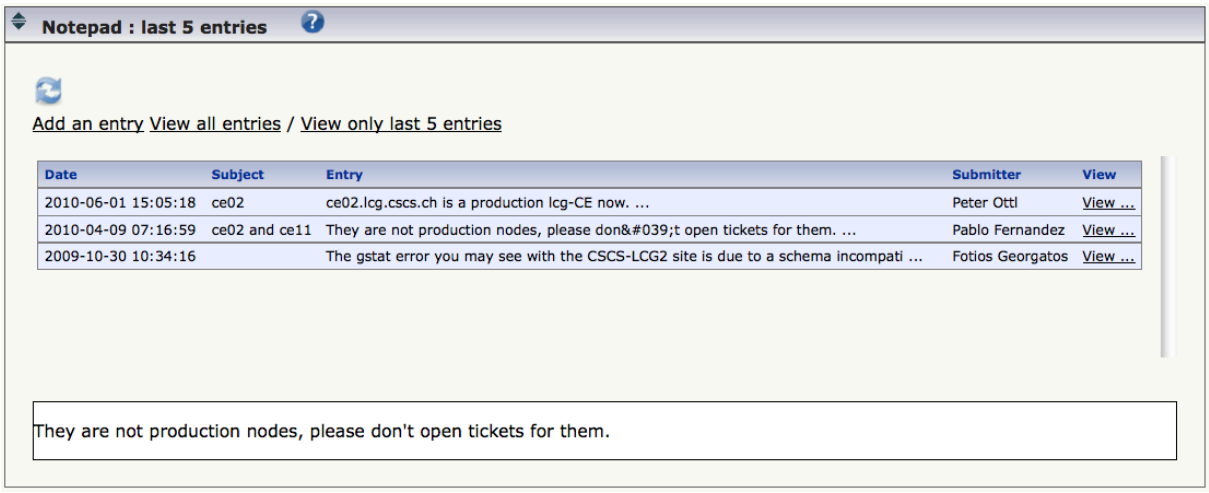
Hostname	Production	Monitored	Description	IP address
apel.lcg.cscs.ch			gLite-APEL	
arc01.lcg.cscs.ch			ARC-CE	
arc02.lcg.cscs.ch			ARC-CE	
atlasvobox.lcg.cscs.ch			VO-box	
bdii.lcg.cscs.ch			Site-BDII	
ce01.lcg.cscs.ch			APEL	
ce01.lcg.cscs.ch			CE	
ce02.lcg.cscs.ch			CE	
ce02.lcg.cscs.ch			APEL	
cmsvobox.lcg.cscs.ch			VO-box	
cream01.lcg.cscs.ch			CREAM-CE	
cream01.lcg.cscs.ch			APEL	
cream02.lcg.cscs.ch			APEL	
cream02.lcg.cscs.ch			CREAM-CE	
storage01.lcg.cscs.ch			SRM	
storage01.lcg.cscs.ch			Classic-SE	
ui64.lcg.cscs.ch			UI	
ui64.lcg.cscs.ch			Site-NAGIOS	

You may encounter either of the two notations for the production/monitored combination:

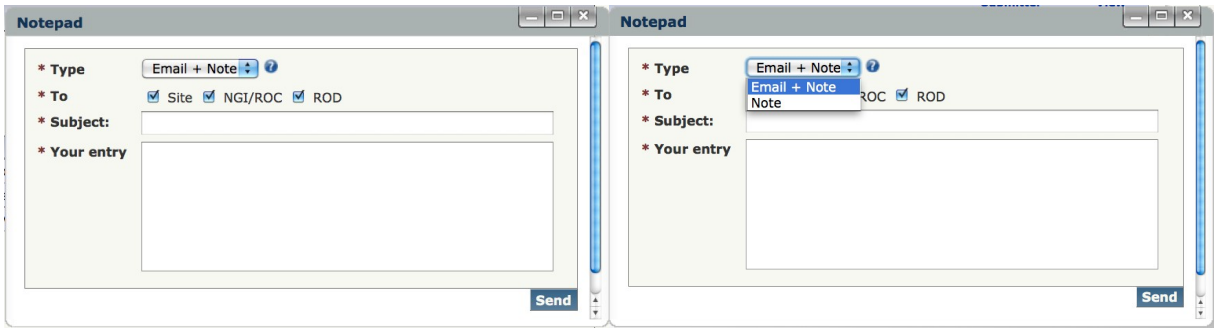
Production	Monitored	In Short	Description
			The service is not monitored and not in production
		N/A	Forbidden by configuration, not supported
			The service is not in production but monitored
			The service is monitored and in production
			The service is not registered in the GOCDB
			The service is not identified

2.7.8 Notepad

The notepad is a convenient tool for exchanging informal news or additional information between a site, its NGI and COD. It is particularly convenient for informing a site that a problem exist in the first 24 hours of an alarm appearing on the dashboard.



Adding an entry is done through this form (2 views):

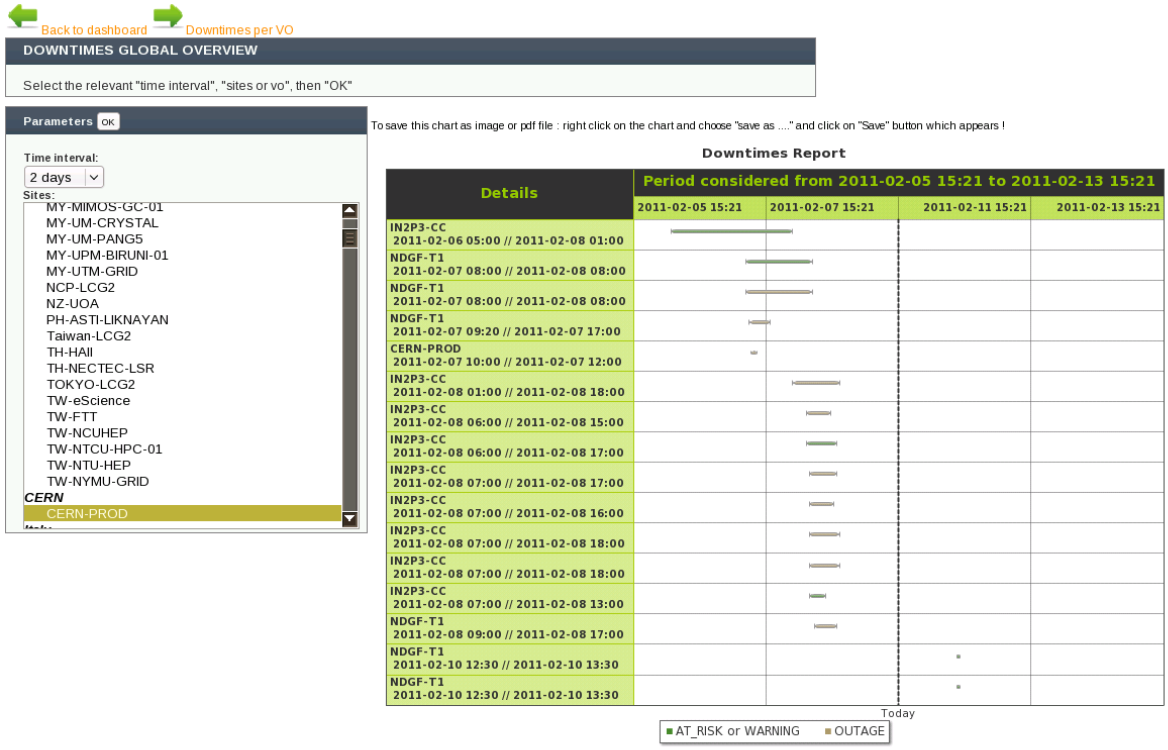


By default, an email notification is sent to the Site, the NGI OC (management) and/or the ROD team. Generally, the NGI OC (management) does not need to be informed of a site problem, so select the “To” options appropriately. It is possible to also only include a note in the Notepad without sending out an email.

3 OTHER DASHBOARD TABS

3.1 Downtimes tab

This page gives you an overview of the current, past and future downtimes registered in the GOCDB during a time interval for a VO or a list of selected sites.



Choose the time interval in the left menu and then a selection of sites for which you want to view downtimes. If you wish to view downtimes via a VO, first choose the “Downtime per VO” link next to top green right arrow.

Clicking on the “OK” button creates a chart on the right side if there are downtimes in both the past and future around the current date for the time interval selected. Note that the chart is Flash-based, and you will need to enable FLASH in your browser if it is disabled.

In the chart, the downtime per site/VO (shown in the left most column) is displayed as a bar in the duration period. The bar is coloured using the severity of the downtime declared. Rolling over the bar gives the downtime description. Clicking on the bar opens a downtime details page in the GOCDB.

For the case where no downtime for the time period selected is relevant to the site/VO the chart is not displayed. However, a message is displayed indicating that there are no downtimes in that period for the selection.

3.2 Handover tab

A handover log form is available under the “Handover” tab.

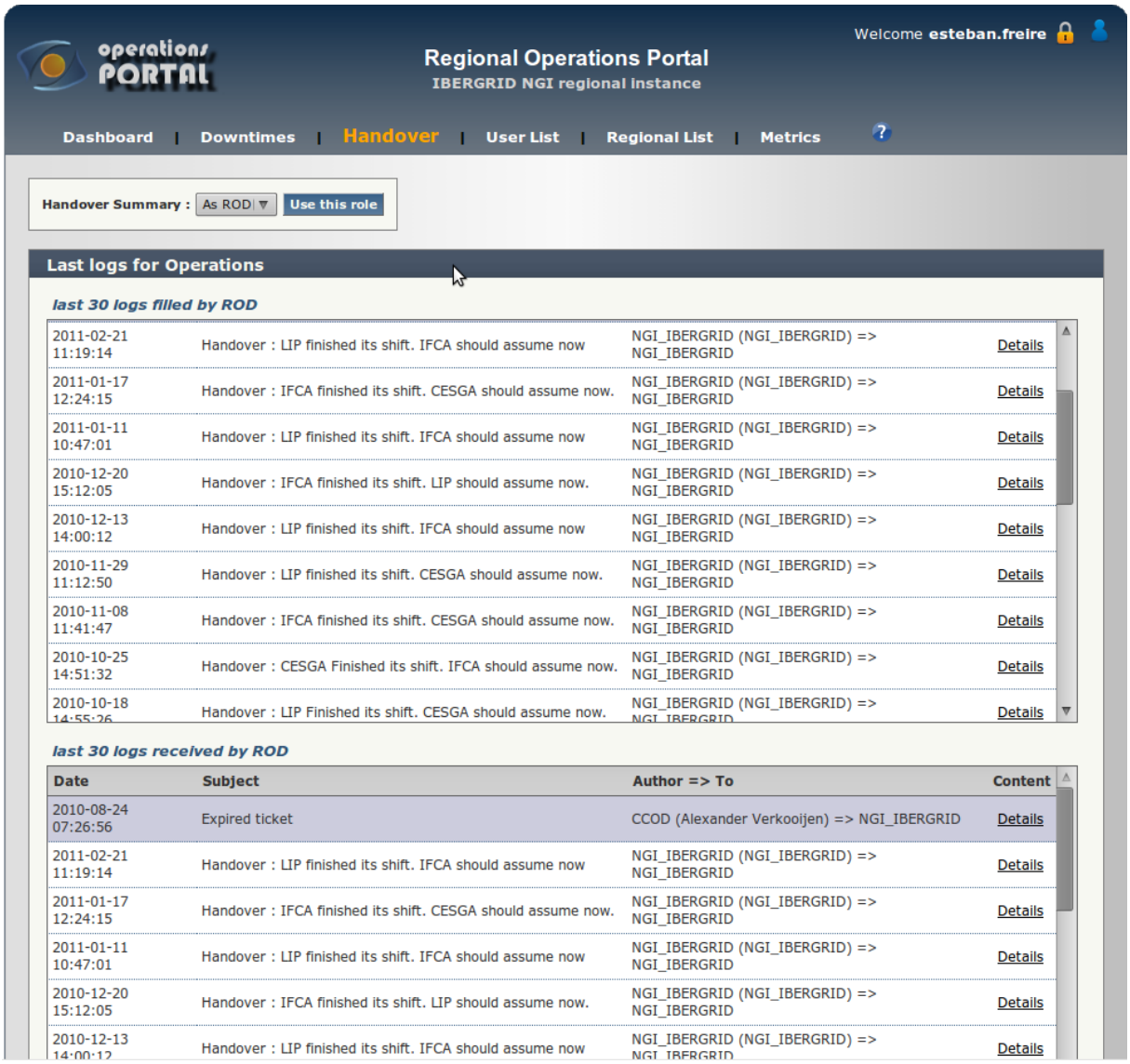
This can be useful for both making a summary of the past week and keeping a log information available for the next ROD shift.

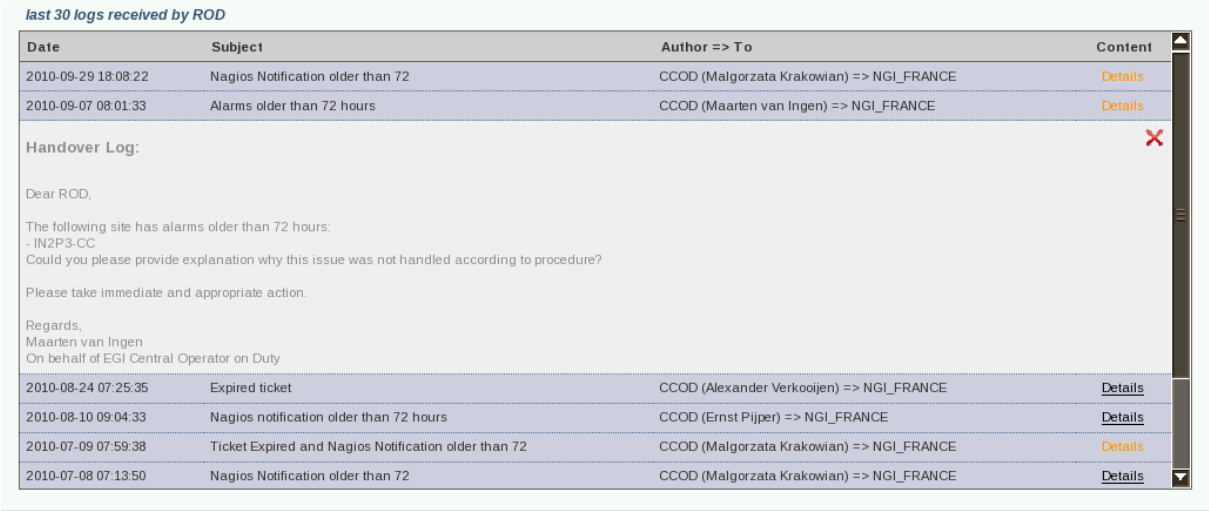
It can be also used to ask/give information to another ROD team and to communicate and/or reply to COD.

After selecting the “ROD” role, you will see:

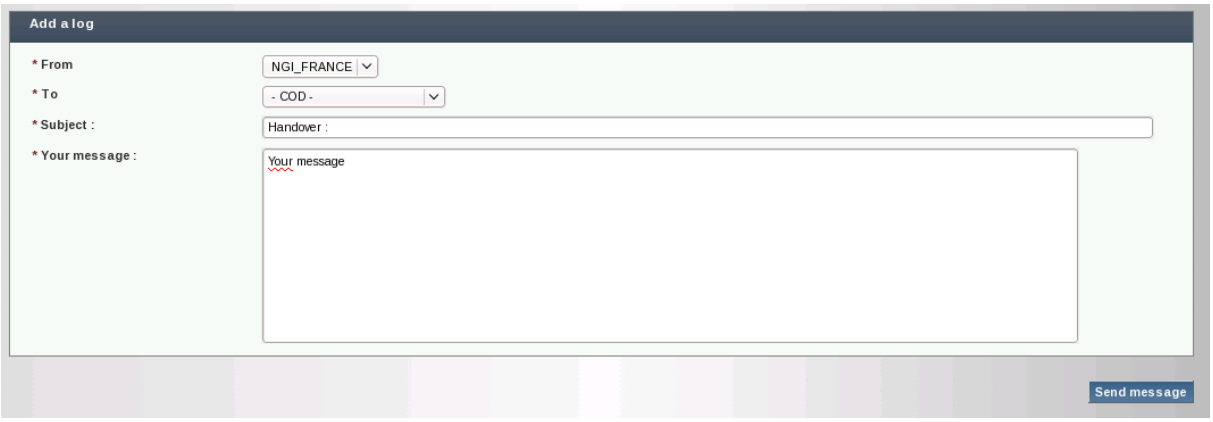
- history of the logs sent and received for your NGI
- a form to submit a log

Logs are listed by date and you can see the details by clicking on the “details...” link.


operations PORTAL
Regional Operations Portal
IBERGRID NGI regional instance
Welcome esteban.freire
Dashboard | Downtimes | Handover | User List | Regional List | Metrics
Handover Summary : As ROD Use this role
Last logs for Operations
last 30 logs filled by ROD
2011-02-21 11:19:14 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2011-01-17 12:24:15 Handover : IFCA finished its shift. CESGA should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2011-01-11 10:47:01 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-12-20 15:12:05 Handover : IFCA finished its shift. LIP should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-12-13 14:00:12 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-11-29 11:12:50 Handover : LIP finished its shift. CESGA should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-11-08 11:41:47 Handover : IFCA finished its shift. CESGA should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-10-25 14:51:32 Handover : CESGA Finished its shift. IFCA should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-10-18 Handover : LIP Finished its shift. CESGA should assume now. NGI_IBERGRID (NGI_IBERGRID) => Details
last 30 logs received by ROD
Date Subject Author => To Content
2010-08-24 07:26:56 Expired ticket CCOD (Alexander Verkooijen) => NGI_IBERGRID Details
2011-02-21 11:19:14 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2011-01-17 12:24:15 Handover : IFCA finished its shift. CESGA should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2011-01-11 10:47:01 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-12-20 15:12:05 Handover : IFCA finished its shift. LIP should assume now. NGI_IBERGRID (NGI_IBERGRID) => NGI_IBERGRID Details
2010-12-13 Handover : LIP finished its shift. IFCA should assume now NGI_IBERGRID (NGI_IBERGRID) => Details



At the end of the page, you will find the submit form:

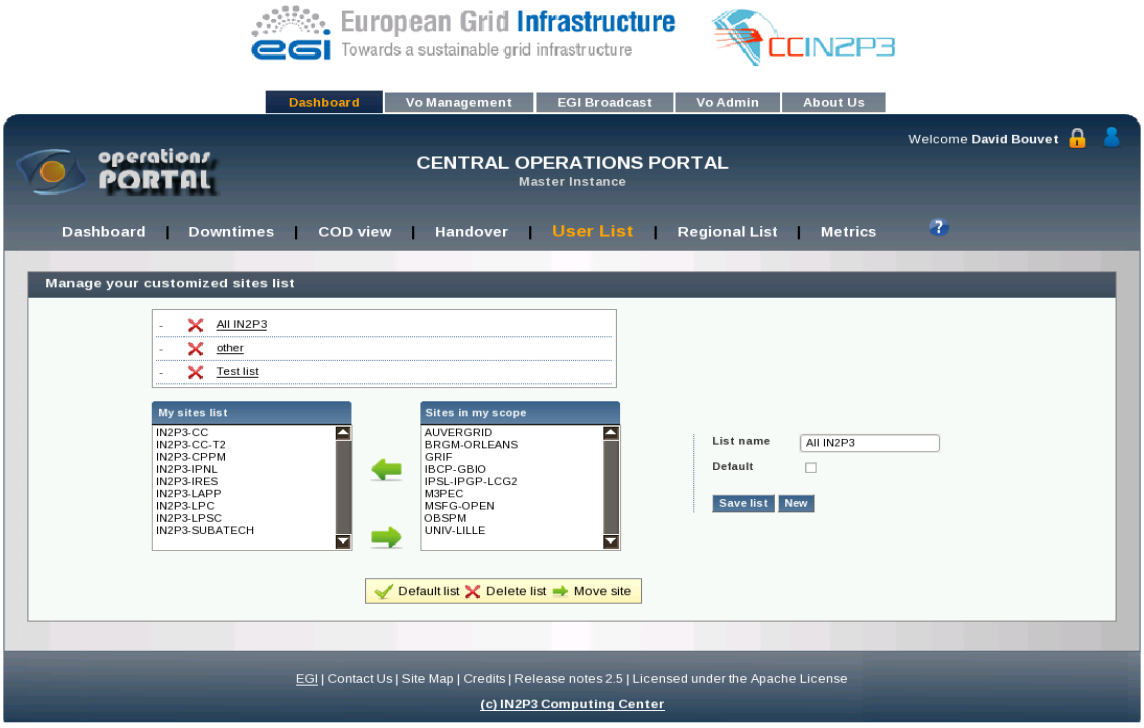


This example shows a log that will be sent by email from ROD to COD. The “To” field can be set to send to either COD or other ROD teams, including your own.

3.3 User List tab

By default, depending on your role in the GOCDB, you will see information about all the sites under your scope.

On this page, you can set different lists to view a subset of the sites and also define another default list.

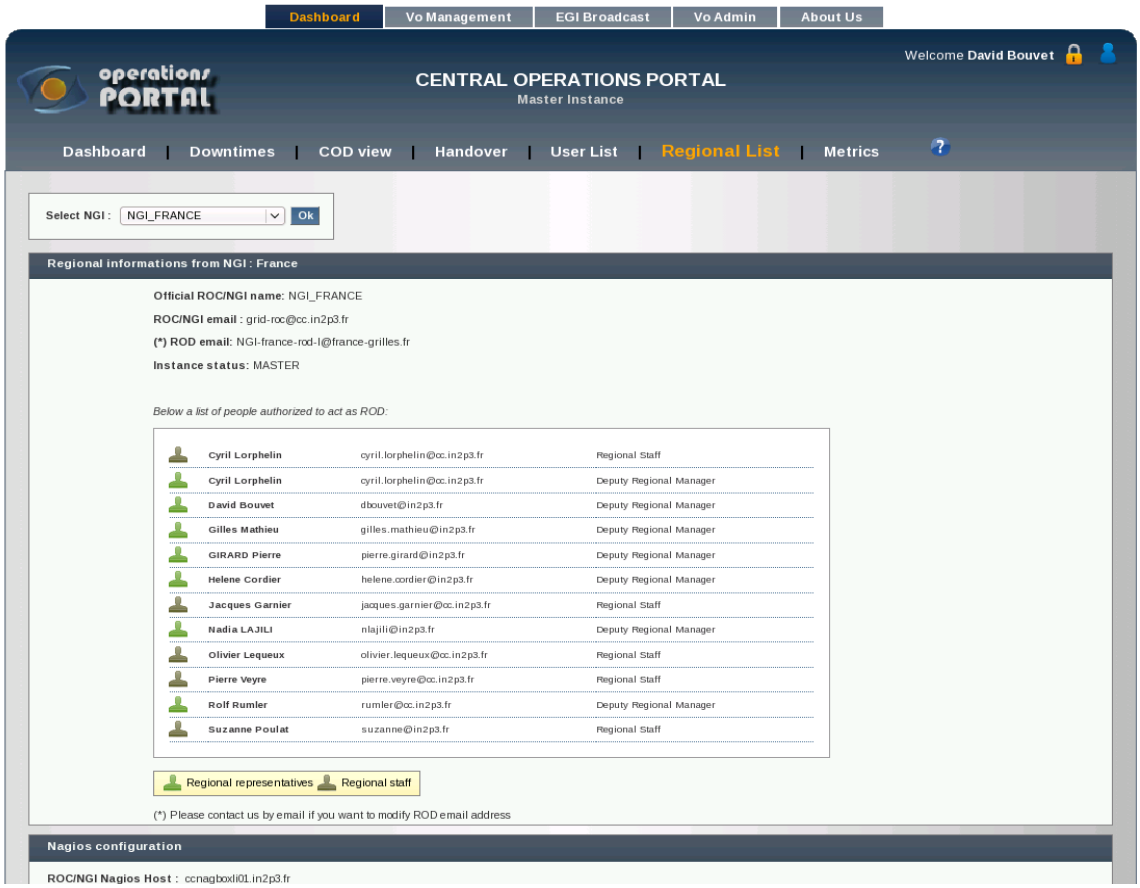


The lists which you have already defined appear just below the “Manage your customised sites list” bar.
Below that, you can add/remove site in the “My sites list” from the list of sites in your scope using the green arrows, . Once the sites you wish to have in the customised list are selected, you can define the list name in the field at the right and save it.
If you wish to define the new list as your default list, just check the “Default” box before saving the list. It will be marked with a green tick in your sites list.

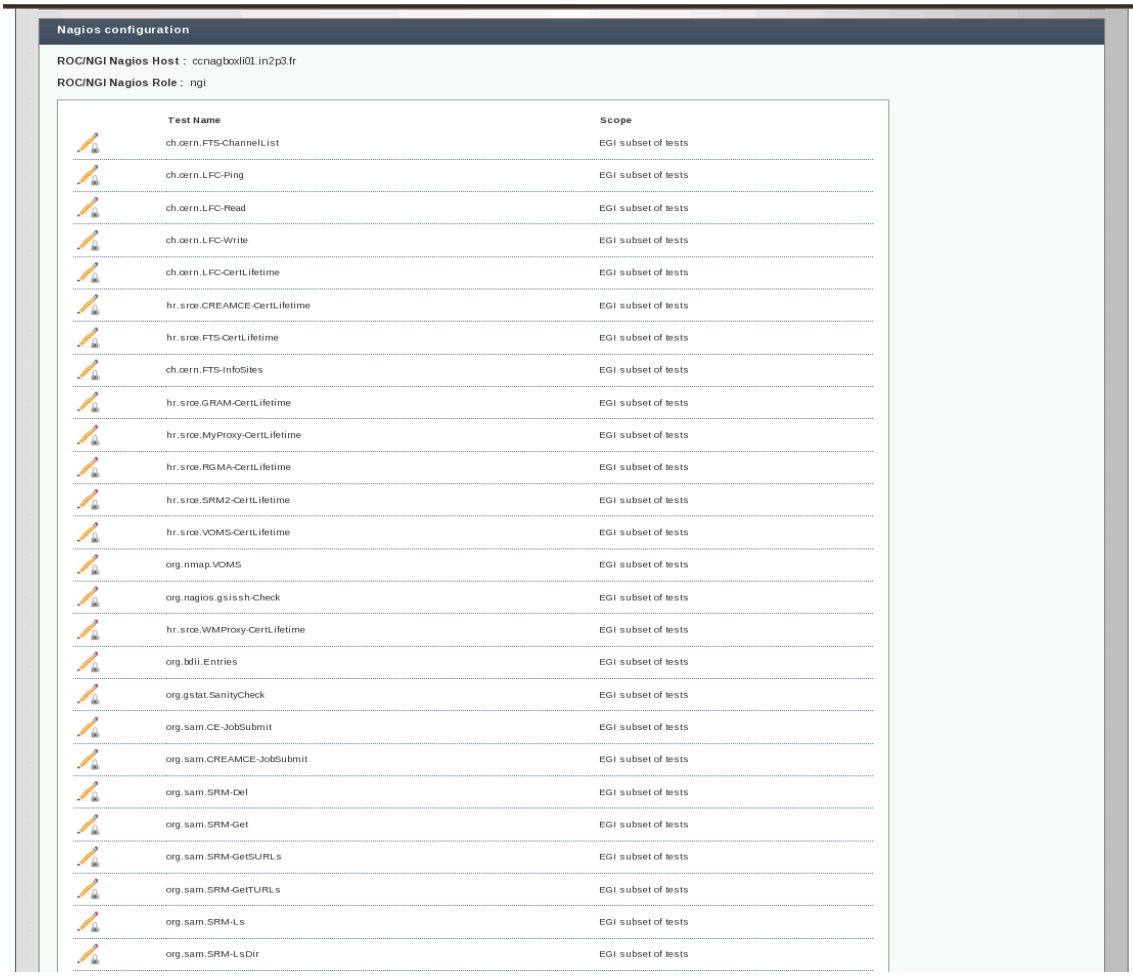
To modify a list, click on its name and use the green arrows to add or remove sites. Remember to save the list!

3.4 Regional List tab

Under this tab you will find the list of staff authorised for each region to act as ROD and contact emails. This first list is retrieved from the information registered in the GOCDB for the NGI.
Note that the ROD email list information does not come from the GOCDB. If you need to update this information, you should contact the portal administrators and COD, who separately maintain a mailing list for all ROD teams.



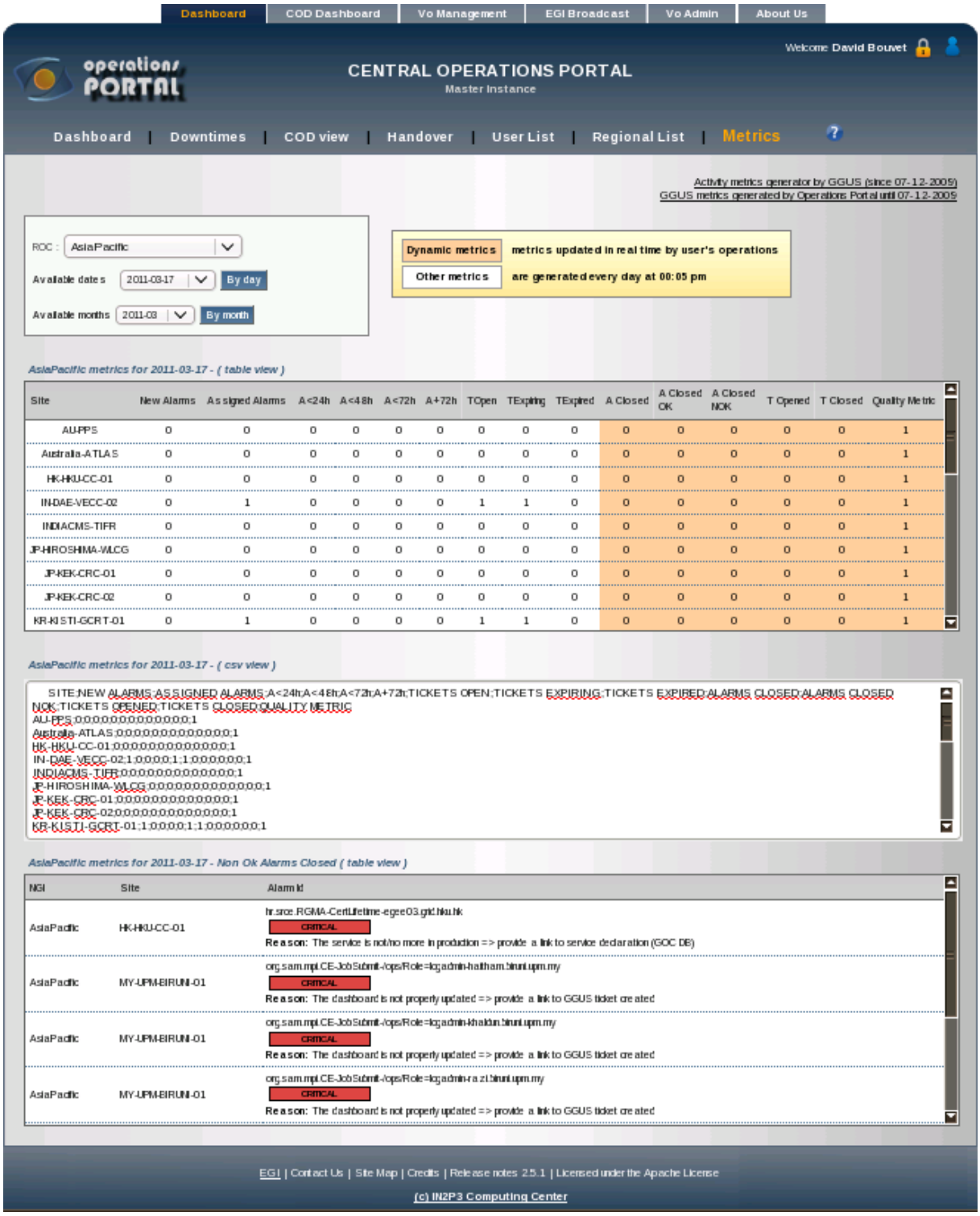
The second list on this page consists of the critical tests displayed in the dashboard. Note that this view is only seen for the tests applicable to your NGI.



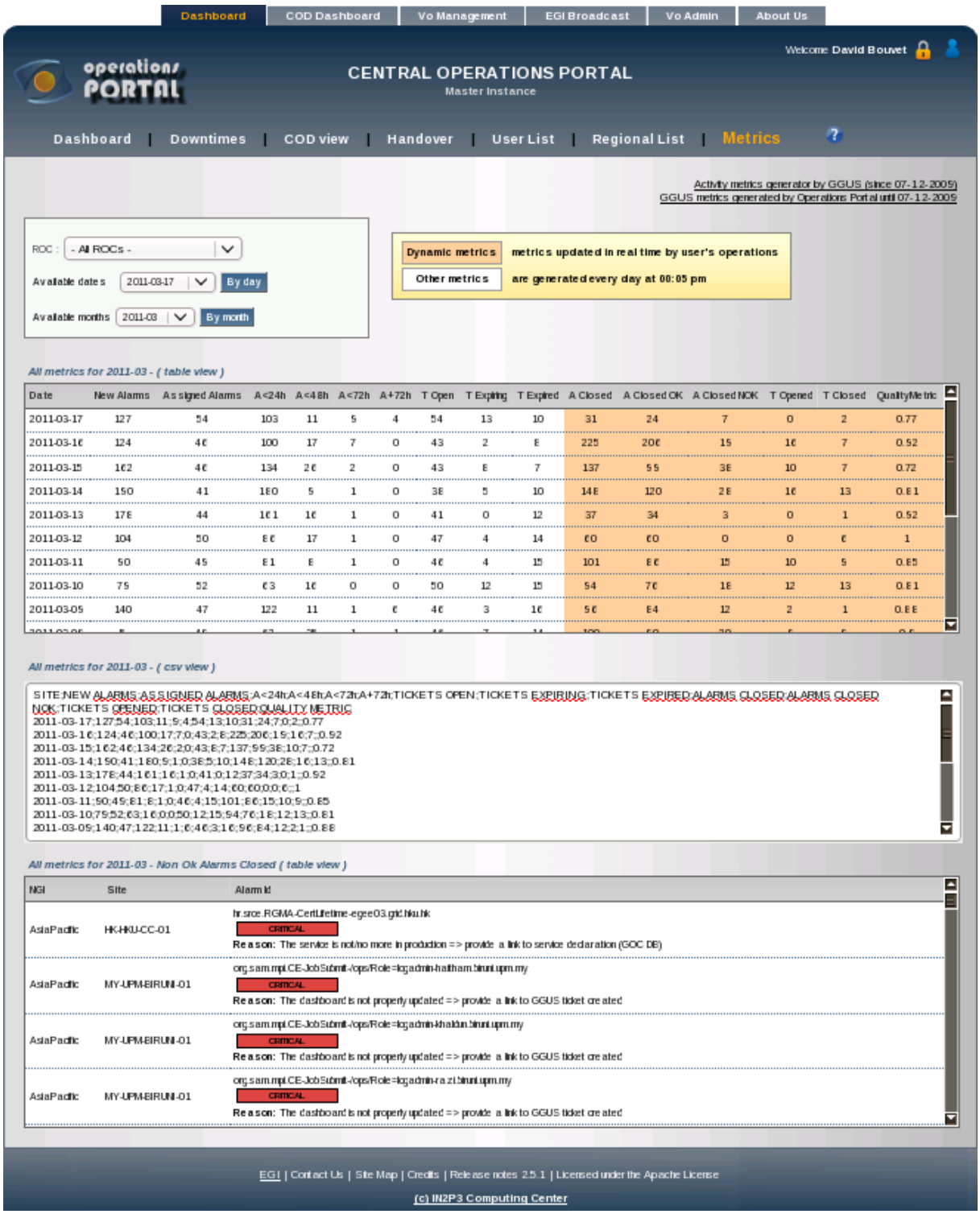
3.5 Metrics tab

The metrics tab is used to get a report of the number of alarms and tickets in their various states (age, opened, closed, etc.) and the metric value for each day/month.

You can choose the NGI/RIP or ALL NGIs (currently labelled “All ROCs”) and either a daily or month time frame. The month view gives daily results for a the whole NGI/RIP in the top screen. The middle screen gives the same metrics in csv format. The last screen gives the list of alarms closed in a “non OK” state with the reason given by the ROD team.



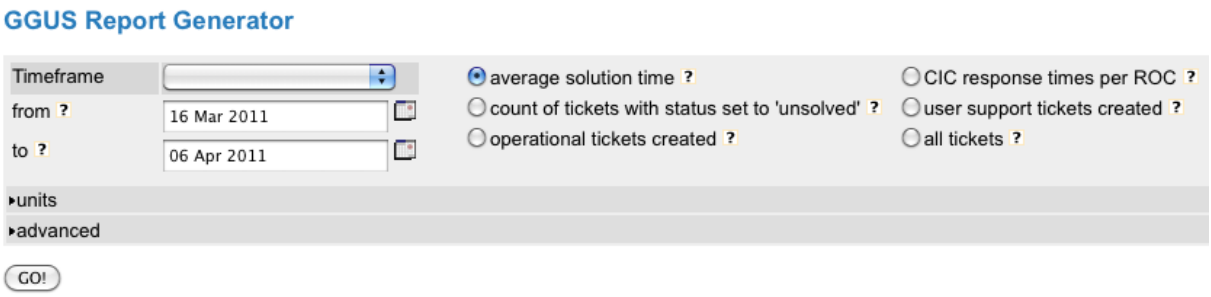
The daily view breaks down the metrics to the site level. This is useful for diagnosing how well sites perform.



On the top right side, there are two link which can also provide GGUS metrics about the tickets labelled:

- Activity metrics generator by GGUS (since 07-12-2009)
- GGUS metrics generated by Operations Portal until 07-12-2009

The first link relates to all GGUS tickets and Dashboard related tickets which can be selected appropriately. The GGUS Report Generator may look like this



The second link provides historical data prior to 07-12-2009.

4 OTHER TABS

The tabs “VO Management”, “EGI Broadcast”, “VO Admin”, “About Us” do not concern the Dashboard and will therefore not be covered by this document.

5 GLOSSARY

APEL	Accounting Processor for Event Logs https://wiki.egi.eu/wiki/APEL
COD	Central Operator on Duty https://wiki.egi.eu/wiki/Grid_operations_oversight
GGUS	Global Grid User Support https://gus.fzk.de/pages/home.php
GOCDB	Grid Operations Centre Database https://goc.egi.eu
GStat	http://gstat.egi.eu/gstat/geo/openlayers
Nagios probe	Synonym for Nagios test or Operations test
NGI	National Grid Infrastructure, synonymous with RIP
Node	Synonym for service or service endpoint
OC	Operations Centre, manages ROD teams, monitoring, etc. of an RIP
RC	Resource Centre, synonymous with Site
RIP	Regional Infrastructure Provider, synonymous with NGI
ROD	Regional Operator on Duty, usually a team working in shifts, aka Regional Staff
VO	Virtual Organization