

# Security Monitoring

*Romain Wartel*  
*EGEE 4 Conference, Pisa*



- 1. Policy issues and interaction with JSPG*
- 2. Monitoring infrastructure*
- 3. Metrics monitoring*

- *What documents do we need to write in order to perform security monitoring?*
- *What authorizations do we need? Who can deliver it?*
- *Can we enforce monitoring everywhere it is necessary?*

- *How will the information be displayed?*
- *How will authentication of trusted people be managed?*
- *How could that fit in existing non-monitoring infrastructure?*
- *How can we implement this?*

- *What are the core elements of the grid that need to be monitored?*
- *How can we retrieve appropriate information from these elements?*
- *How intrusive will this be?*
- *How can we implement this?*

Two main approaches:

- **Mandatory tests model**

- *tests are grid jobs, with no specific privileges*
- *tests are submitted to all the CEs, no exception*
- *General results (failed, passed, warning) are public*
- *Detailed results are only available to a group of authenticated people*

- **Subscription model**

- *tests are optional, sites have to ask for it*
- *CEs passing the tests receive an extra “security label”*
- *tests might sometimes require privileged access*
- *Detailed results are only available to a group of authenticated people*

- Ideally, mandatory tests should just be part of Site Functional Tests (SFTs):

Site Functional Tests report - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://lcg-sft.cern.ch:9443/sft/lastreport.cgi?action=Save&vo=dteam&rg=As

## Site Functional Tests report

2005-10-24 -- latest reports

Test abbreviations

csh	CSH test
swdir	VO software directory
rgma	R-GMA
wn	WN host name
ver	Software Version (WN)
ca	CA certs version
rm	Replica Management
votag	VO Tag management
js	Job submission
bi	BrokerInfo
apel	Apel test

Colours definition

SD	Scheduled downtime	#a3a3a3
JL	Job list match failed	#aab3ff
JS	Job submission failed	#f4876b
CT	Critical tests failed	#f9d48e
NT	Non-critical tests failed	#f2f98e
OK	OK	#b2f98e

Test summary

	SD	JL	JS	CT	OK	total
dteam	20	3	2	17	130	172

	St.	Region	Site Name	Site CE	VO dteam													
					St.	js	wn	ver	ca	rgma	bi	csh	rm	votag	swdir	apel		
1.	OK	SouthEasternEurope	AEGIS01-PHY-SCL	ce.phybg.ac.yu	OK	0	1	0	0	0	0	0	0	0	0	0	0	0
2.	OK	Canada	ALBERTA-LCG2	lcgce01.nic.ualberta.ca	OK	0	1	0	0	0	0	0	0	0	0	W	0	X
3.	OK	China	BEIJING-LCG2	lcg002.ihep.ac.cn	OK	0	1	0	0	X	0	0	0	0	0	0	0	X
4.	OK	NorthernEurope	BelGrid-UCL	ingrid.cism.ucl.ac.be	OK	0	1	0	0	0	0	0	0	0	W	0	X	
5.	OK	SouthEasternEurope	BG-INRNE	ce1.inrne.bas.bg	OK	0	1	0	0	0	0	0	0	0	0	0	0	X
6.	OK	SouthEasternEurope	BG01-IPP	ce001.grid.bas.bg	OK	0	1	0	0	0	0	0	0	0	0	0	0	0
7.	OK	SouthEasternEurope	BG02-IM	ce001.ibm.bas.bg	OK	0	1	0	0	0	0	0	0	0	0	0	0	X
8.	OK	SouthEasternEurope	BG04-ACAD	ce01.grid.acad.bg	OK	0	1	0	0	0	0	0	0	0	0	0	0	X
9.	OK	UKI	BHAM-LCG2	epgce1.ph.bham.ac.uk	OK	0	1	0	0	0	0	0	0	0	0	0	0	X
10.	OK	UKI	BHAM-LCG2	epbf005.ph.bham.ac.uk	OK	0	1	0	0	0	0	0	0	0	W	X	X	X
11.	OK	SouthWesternEurope	BIFI	ce-eg ee.bifi.unizar.es	OK	0	1	0	0	0	0	0	0	0	0	0	0	X
12.	OK	UKI	BITLab-LCG	dgc-grid-35.brunel.ac.uk	OK	0	1	0	0	0	0	0	0	0	W	0	0	X
13.	SD	BNL	BNL-LCG2	lcg-ce01.usatlas.bnl.gov	SD	X	??	??	??	??	??	??	??	??	??	??	??	??

Done

lcg-sft.cern.ch:9443

# First “security extension” to SFTs

- A first “security extension” called sft-crl has been developed for SFTs
- Piotr Nyczyk has added a secure area on the Site Functional Tests report page
- sft-crl is checking the timestamps of the CRL, for each valid certificate:
  - *A warning is issued if the CRL is more that 9 hours old, but less than 3 days.*
  - *An alert is issued if no CRL is found, or if it is older than 3 days.*
- The goal is too highlight outdated CRLs or certificates with no CRL
- General results are published on the main SFT report page (public access)
- Detailed results are available to authorized people only



# First “security extension” to SFTs

Site Functional Tests report - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://lcg-sft.cern.ch:9443/sft/lastreport.cgi?action=Save&vo=dteam&rg=AsiaPacific&rg=

## Site Functional Tests report

2005-10-24 -- latest reports

Test summary

	SD	JL	JS	CT	OK	total
dteam	20	3	2	17	130	172

Colours definition

SD	Scheduled downtime	#a3a3a3
JL	Job list match failed	#aab3ff
JS	Job submission failed	#f4876b
CT	Critical tests failed	#f9d48e
NT	Non-critical tests failed	#f2f98e
OK	OK	#b2f98e

Test abbreviations

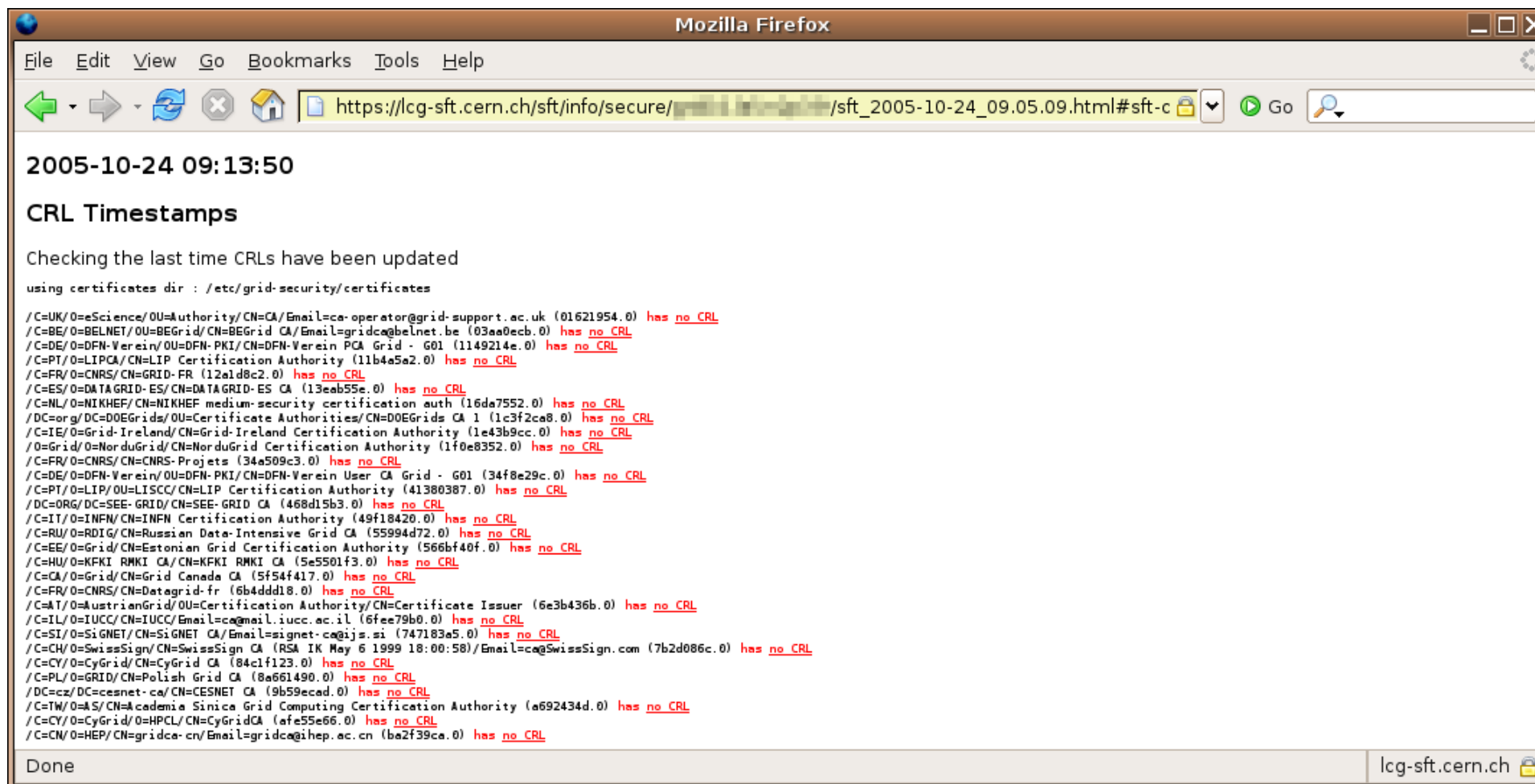
crl	CRL timestamp test
-----	--------------------

	St.	Region	Site Name	Site CE	VO dteam	
					St.	crl
1.	OK	SouthEasternEurope	AEGIS01-PHY-SCL	ce.phybg.ac.yu	OK	!!!
2.	OK	Canada	ALBERTA-LCG2	lcgce01.nic.ualberta.ca	OK	!!!
3.	OK	China	BEIJING-LCG2	lcg002.ihep.ac.cn	OK	!!!
4.	OK	NorthernEurope	BelGrid-UCL	ingrid.cism.ucl.ac.be	OK	!!!
5.	OK	SouthEasternEurope	BG-INRNE	ce1.inrne.bas.bg	OK	0
6.	OK	SouthEasternEurope	BG01-IPP	ce001.grid.bas.bg	OK	!!!
7.	OK	SouthEasternEurope	BG02-IM	ce001.ibm.bas.bg	OK	0
8.	OK	SouthEasternEurope	BG04-ACAD	ce01.grid.acad.bg	OK	!!!
9.	OK	UKI	BHAM-LCG2	epgce1.ph.bham.ac.uk	OK	0
10.	OK	UKI	BHAM-LCG2	epbf005.ph.bham.ac.uk	OK	!!!
11.	OK	SouthWesternEurope	BIFI	ce-egge.bifi.unizar.es	OK	0
12.	OK	UKI	BITLab-LCG	dgc-grid-35.brunel.ac.uk	OK	!!!
13.	SD	BNL	BNL-LCG2	lcg-ce01.usatlas.bnl.gov	SD	??
14.	OK	UKI	BRISTOL-PP-LCG	lcgce01.phybris.ac.uk	OK	!!!
15.	OK	CentralEurope	BUDAPEST	grid109.kfki.hu	OK	!!!
16.	SD	Canada	CARLETONU-LCG2	lca02.physics.carleton.ca	SD	??

Done

lcg-sft.cern.ch:9443

- **Surprise: 106 sites on 172 failed!**
- **Main causes: bugs in edg-fetch-crl, bad configuration, no mechanism to get CRLs**



2005-10-24 09:13:50

CRL Timestamps

Checking the last time CRLs have been updated

using certificates dir : /etc/grid-security/certificates

```

/C=UK/0=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk (01621954.0) has no CRL
/C=BE/0=BELNET/OU=BEGrid/CN=BEGrid/Email=gridca@belnet.be (03aa0ecb.0) has no CRL
/C=DE/0=DFN-Verrein/OU=DFN-PKI/CN=DFN-Verrein PCA Grid - G01 (1149214e.0) has no CRL
/C=PT/0=LIPCA/CN=LIP Certification Authority (11b4a5a2.0) has no CRL
/C=FR/0=CNRS/CN=GRID-FR (12ald8c2.0) has no CRL
/C=ES/0=DATA GRID-ES/CN=DATA GRID-ES CA (13eab55e.0) has no CRL
/C=NL/0=NIKHEF/CN=NIKHEF medium-security certification auth (16da7552.0) has no CRL
/DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1 (1c3f2ca8.0) has no CRL
/C=IE/0=Grid-Ireland/CN=Grid-Ireland Certification Authority (1e43b9cc.0) has no CRL
/0=Grid/0=NorduGrid/CN=NorduGrid Certification Authority (1f0e8352.0) has no CRL
/C=FR/0=CNRS/CN=CNRS-Projets (34a509c3.0) has no CRL
/C=DE/0=DFN-Verrein/OU=DFN-PKI/CN=DFN-Verrein User CA Grid - G01 (34f8e29c.0) has no CRL
/C=PT/0=LIP/OU=LISCC/CN=LIP Certification Authority (41380387.0) has no CRL
/DC=ORG/DC=SEE-GRID/CN=SEE-GRID CA (468d15b3.0) has no CRL
/C=IT/0=INFN/CN=INFN Certification Authority (49f18420.0) has no CRL
/C=RU/0=RDIG/CN=Russian Data-Intensive Grid CA (55994d72.0) has no CRL
/C=EE/0=Grid/CN=Estonian Grid Certification Authority (566bf40f.0) has no CRL
/C=HU/0=KFKI RMKI CA/CN=KFKI RMKI CA (5e5501f3.0) has no CRL
/C=CA/0=Grid/CN=Grid Canada CA (5f54f417.0) has no CRL
/C=FR/0=CNRS/CN=Datagrid-fr (6b4ddd18.0) has no CRL
/C=AT/0=AustrianGrid/OU=Certificate Authority/CN=Certificate Issuer (6e3b436b.0) has no CRL
/C=IL/0=IUCC/CN=IUCC/Email=ca@mail.iucc.ac.il (6fee79b0.0) has no CRL
/C=SI/0=SI-GNET/CN=SI-GNET CA/Email=signet-ca@ijs.si (747183a5.0) has no CRL
/C=CH/0=SwissSign/CN=SwissSign CA (RSA IK May 6 1999 18:00:58)/Email=ca@SwissSign.com (7b2d086c.0) has no CRL
/C=CY/0=CyGrid/CN=CyGrid CA (84c1f123.0) has no CRL
/C=PL/0=GRID/CN=Polish Grid CA (8a661490.0) has no CRL
/DC=cz/DC=cesnet-ca/CN=CESNET CA (9b59ecad.0) has no CRL
/C=TW/0=AS/CN=Academia Sinica Grid Computing Certification Authority (a692434d.0) has no CRL
/C=CY/0=CyGrid/0=HPCL/CN=CyGridCA (afe55e66.0) has no CRL
/C=CN/0=HEP/CN=gridca-cn/Email=gridca@ihep.ac.cn (ba2f39ca.0) has no CRL

```

Done

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://lcg-sft.cern.ch/sft/info/secure/

## CRL Timestamps

Checking the last time CRLs have been updated  
using certificates dir : /etc/grid-security/certificates

```

/C=UK/O=eScience/OU=Authority/CN=CA/emailAddress=ca-operator@grid-support.ac.uk (01621954.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=BE/O=BELNET/OU=BEGrid/CN=BEGrid CA/emailAddress=gridca@belnet.be (03aa0ecb.0) CRL is more than 3 days old (last updated at 10:23 on 23 Oct)
/O=Grid/O=UKHEP/CN=UK HEP Testbed CA (0ed6468a.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN-Verein PCA Grid - G01 (1149214e.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=PT/O=LIPCA/CN=LIP Certification Authority (11b4a5a2.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=FR/O=CNRS/CN=GRID-FR (12a1d8c2.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=ES/O=DATAGRID-ES/CN=DATAGRID-ES CA (13eab55e.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=NL/O=NIKHEF/CN=NIKHEF medium-security certification auth (16da7552.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=SK/O=IISAS/CN=IISAS CA (1aa81ac1.0) has no CRL
/DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1 (1c3f2ca8.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=IE/O=Grid-Ireland/CN=Grid-Ireland Certification Authority (1e43b9cc.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/O=Grid/O=NorduGrid/CN=NorduGrid Certification Authority (1f0e8352.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/O=dutchgrid/OU=Certificate Authorities/CN=EDG Tutorial Worthless Certification Authority (225860ae.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Top-Level CA (29021213.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=FR/O=CNRS/CN=CNRS-Projets (34a509c3.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN-Verein User CA Grid - G01 (34f8e29c.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=PT/O=LIP/OU=LISCC/CN=LIP Certification Authority (41380387.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/DC=ORG/DC=SEE-GRID/CN=SEE-GRID CA (468d15b3.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=IT/O=INFN/CN=INFN Certification Authority (49f18420.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)
/C=US/O=National Center for Supercomputing Applications/CN=Certification Authority (4a6cd8b1.0) has no CRL
/C=RU/O=RDIG/CN=Russian Data-Intensive Grid CA (55994d72.0) CRL is more than 3 days old (last updated at 15:33 on 8 Sep)
/C=EE/O=Grid/CN=Estonian Grid Certification Authority (566bf40f.0) CRL is more than 540 minutes old (last updated at 11:11 on 23 Oct)

```

Done

lcg-sft.cern.ch

- **Security extensions are useful**
- **Developing the tool was very easy (thanks to Piotr's secure area)**
- **Sites' configuration need to be more tested**
- **Some work still need to be done:**
  - *To authenticate people from the GOCDB*
  - *To have some more sft security extensions*
  - *Possibly to be able to launch sft tests on the CEs, not only on the WNs.*

In order to provide an efficient security monitoring on the Grid:

- *Some critical elements of the Grid requires dedicated monitoring (RBs, etc.)*
- *Some tests could require privileged access to gather information (for ex: from the log files)*

However:

- *None of this can be done via SFTs*
- *It would be difficult to “force” sites to install such monitoring tools (lots of policy issues)*

Therefore a subscription based model is being adopted.

## Current issues to be discussed:

- *What other SFT extension would be useful?*
- *How could we implement a mechanism to check patching status of Grid nodes?*
- *How to have sites to “buy” our subscription based model?*
- *Which parameters should be monitored on the core Grid elements?*

# Monitoring patching status of Grid nodes

- *It is extremely useful*
- *It should be part of next security service challenge*
- *How do we do this?*

## *Two proposals:*

- *Having a grid job that would:*
  - *Get the list of installed RPM and Linux distribution*
  - *Report it to one or more central service*
  - *The central server(s) will compare this list with the latest list of the vendor*
  - *Security patches will be highlighted from the list (how?)*
- *Having a program, install by local sysadmins that would:*
  - *Launch a command to retrieve the list of pending updates (a la Yumit)*
  - *Report the list to one or more central service*
  - *Security patches will be highlighted from the list (how?)*