EGI CSIRT Security Service Challenge SSC-19.03, final report

EGI CSIRT

GDB 10 Jul. 2019

EGI CSIRT

Introduction

- Recap from May GDB
- Evaluation
- LHCB IR

Goal of the SSC

Answer to the questions:

- what is the overall security situation?
- how well are the different IR procedures interfaced to each other?
- what are the pitfalls in IR?

EGI CSIRTs IRTF, in brief

EGI CSIRT Mission

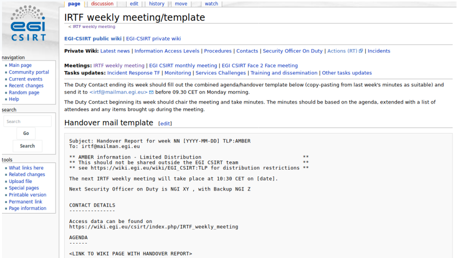
The EGI Computer Security and Incident Response Team (EGI-CSIRT) provides operational security for the EGI Infrastructure. This includes responding to computer security incidents affecting the infrastructure, which is carried out by co-ordinating the incident handling activities in the NGIs/EIROs, RCs, VOs, and where applicable interacting with partner Infrastructures CSIRTs and CSIRT communities with which EGI-CSIRT has a trust relationship.

https://documents.egi.eu/secure/ShowDocument?docid=385&version=12

Incident Prevention

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 8)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



IRTF weekly meeting/template

< IRTF weekly meeting

EGI-CSIRT public wiki | EGI-CSIRT private wiki

Private Wiki: Latest news | Information Access Levels | Procedures | Contacts | Security Officer On Duty | Actions (RT) | Incidents

Meetings: IRTF weekly meeting | EGI CSIRT monthly meeting | EGI CSIRT Face 2 Face meeting
Tasks updates: Incident Response TF | Monitoring | Services Challenges | Training and dissemination | Other tasks updates

The Duty Contact ending its week should fill out the combined agenda/handover template below (copy-pasting from last week's minutes as suitable) and send it to <irtf@mailman.egi.eu> before 09.30 CET on Monday morning.

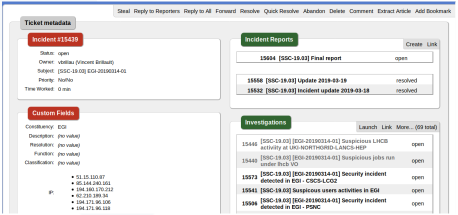
The Duty Contact beginning its week should chair the meeting and take minutes. The minutes should be based on the agenda, extended with a list of attendees and any items brought up during the meeting.

Handover mail template [edit]

```
Subject: Handover Report for week NN [YYYY-MM-DD] TLP:AMBER
To: irtf@mailman.egi.eu

** AMBER information - Limited Distribution                          **
** This should not be shared outside the EGI CSIRT team              **
** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions **

The next IRTF weekly meeting will take place at 10:30 CET on [date].

Next Security Officer on Duty is NGI XY , with Backup NGI Z


CONTACT DETAILS
---------------

Access data can be found on
https://wiki.egi.eu/csirt/index.php/IRTF_weekly_meeting

AGENDA
------

<LINK TO WIKI PAGE WITH HANDOVER REPORT>
```

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 8)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



Incident #15439

Status: open
Owner: vbrillau (Vincent Brillault)
Subject: [SSC-19.03] EGI-20190314-01
Priority: No/No
Time Worked: 0 min

Custom Fields

Constituency: EGI
Description: *(no value)*
Resolution: *(no value)*
Function: *(no value)*
Classification: *(no value)*
IP:
- 51.15.110.87
- 85.144.240.161
- 194.160.170.212
- 62.210.189.34
- 194.171.96.106
- 194.171.96.118

Incident Reports

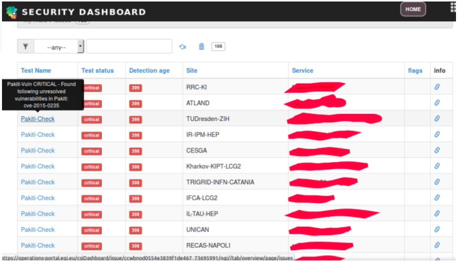
15604	[SSC-19.03] Final report	open
15558	[SSC-19.03] Update 2019-03-19	resolved
15532	[SSC-19.03] Incident update 2019-03-18	resolved

Investigations

15446	[SSC-19.03] [EGI-20190314-01] Suspicious LHCB activiity at UKI-NORTHGRID-LANCS-HEP	open
15440	[SSC-19.03] [EGI-20190314-01] Suspicious jobs run under lhcb VO	open
15573	[SSC-19.03] [EGI-20190314-01] Security incident detected in EGI - CSCS-LCG2	open
15541	[SSC-19.03] Suspicous users activities in EGI	open
15506	[SSC-19.03] [EGI-20190314-01] Security incident detected in EGI - PSNC	open

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 8)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested


SECURITY DASHBOARD

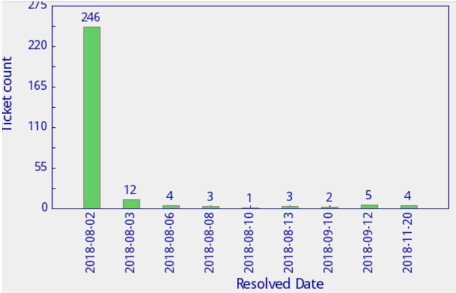
Pakiti-Vuln CRITICAL - Found following unresolved vulnerabilities in Pakiti: cve-2015-0235

Test Name	Test status	Detection age	Site	Service	flags	info
	critical	399	RRC-KI	[redacted]		🔗
	critical	399	ATLAND	[redacted]		🔗
Pakiti-Check	critical	399	TUDresden-ZIH	[redacted]		🔗
Pakiti-Check	critical	398	IR-IPM-HEP	[redacted]		🔗
Pakiti-Check	critical	398	CESGA	[redacted]		🔗
Pakiti-Check	critical	398	Kharkov-KIPT-LCG2	[redacted]		🔗
Pakiti-Check	critical	398	TRIGRID-INFN-CATANIA	[redacted]		🔗
Pakiti-Check	critical	398	IFCA-LCG2	[redacted]		🔗
Pakiti-Check	critical	398	IL-TAU-HEP	[redacted]		🔗
Pakiti-Check	critical	398	UNICAN	[redacted]		🔗
Pakiti-Check	critical	398	RECAS-NAPOLI	[redacted]		🔗

ttps://operations-portal.egi.eu/csiDashboard/issue/ccwbnod0554e3839f1de467_73695991/ngi//tab/overview/page/issues

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 8)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



Communication Challenge 2018

see Presentations by Vincent Brillault (OMB)

Incident Response

Incident Response in EGI

Incidents: historical list . . .

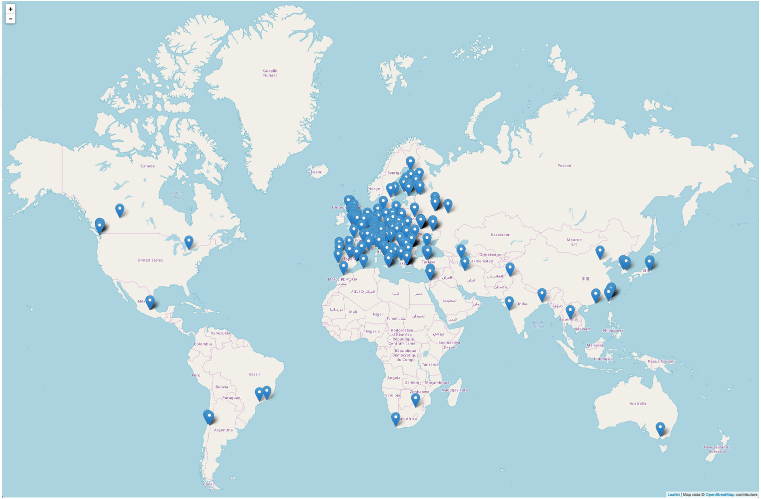
EGI-20150925-01	stole ssh user pw / root compromise / bitcoin mi
EGI-20150519-01	Vulnerable VA in appdb, Root compromise **clou**
EGI-20140113-01	BitCoin Mining **using grid technology**
EGI-20110418-01	stolen ssh credentials
EGI-20110301-01	bruteforce ssh **quite a few of this type**
EGI-20110121	web server misconfig
EGI-20100929-01	stolen ssh credentials
EGI-20100722	bruteforce ssh
EGI-20100707-01	stolen ssh credentials/remote vulns in CMSes
EGEE-20091204	stolen ssh credentials/X keyboard sniffing
GRID-SEC-001	stolen ssh credentials

Incident Response in EGI

Actions, Incident Response Procedure

- EGI CSIRT https://wiki.egi.eu/wiki/SEC01
- Incident is detected/reported, gets recorded in ticket sysem
- affected ResourceCenter(s) get contacted, asked for confirmation
- if confirmed a heads up gets issued infrastructure wide
- When and how an identity should get suspended (locally and centrally) is in SEC01.
- Local team is responsible for incident resolution (close out report), EGI forensics experts support local team on request
- Procedures need to be aligned across security teams, here in particular the VO procedures (see Chris' slides)

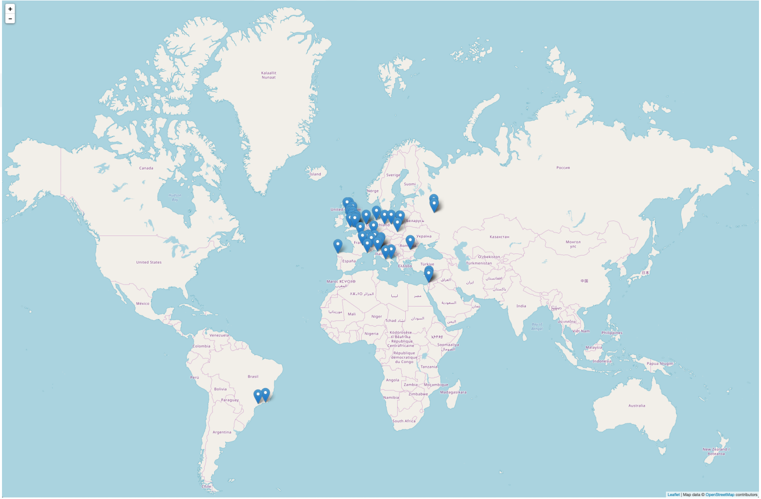
Incidents: How they spread out . . . all infra



Leaflet | Map data © OpenStreetMap contributors

Incident Response in EGI

Incidents: How they spread out . . . all sites supporting VO LHCB



Leaflet | Map data © OpenStreetMap contributors

The Environment

- EGI/NGI/ResourceCenter model seems to work quite well. (Local teams get support by experts).
- According to our policies: Security is a site decision.
- EGI CSIRT coordinates operational security activities.
- VO Security team, needs to be part of the IR.
- Practicalities:
    - Who/Which CSIRT has access to which information
    - Who/Which has access to which access controls
- Can one security team deal with an incident involving compromised credentials? → **No!**

Security Service Challenges

SSC what,why,how we did

See slides from May GDB

SSC Dirac

SSC-19.03
The Situation

Situation

- Someone massively submitted malware through accepted channels.
- Malware creates a botnet, CnC hidden behind TOR.
- Botnet can take malicious actions:
  - *Crypto-currency mining* (heavy CPU load)
  - DDOS against remote targets

The Challenge

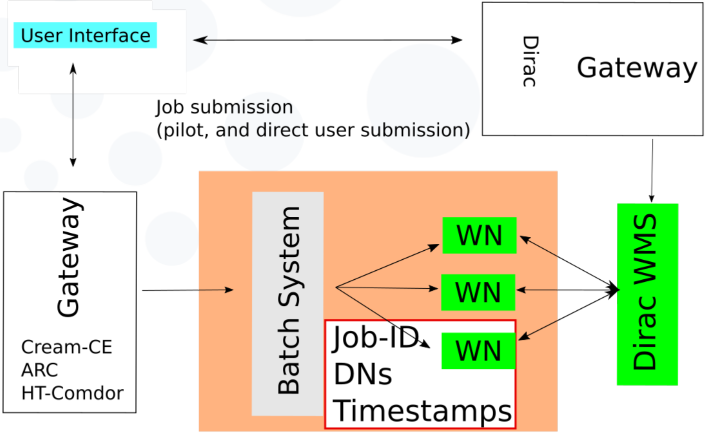
Challenge

Respond to the above created situation

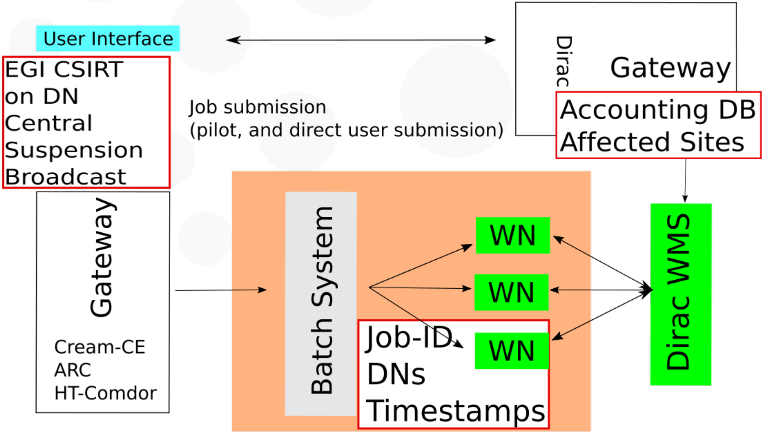
The Challenge

- Observe/Orient
  - Confirm it is an incident.
  - Find out what is the extent of the incident
  - Which DNs are involved, which DNs have to be suspended.
- Decide/Act Stop the incident from further spreading
  - Suspend the DN, prevent more malicious jobs started.
  - Stop malicious jobs
  - Understand the latencies of the various countermeasures.
- Understand the incident, forensics needed.

Security Drills Info gathering



Security Drills IR actions



SSC-19.03 timeline

See slides from May GDB

Report

Report Generation

Evaluation is based on communications (tickets) with 62 RCs and logged information from the SSC framework.
Some tickets got scrambled, the results may change a bit after RCs feedback on the per RC report.

Report Generation Data sources

- Transactions in tickets (free text)
- SSC-Monitor log data (bot connectivity, jobs send, jobs started, etc)
- Suspension monitor

Suspension-Monitor

- from cron (30 min) uberftp to gatekeepers
- uberftp ran via tor to not loose the monitor
- list of gatekeepers from bdii
- /usr/bin/torify’, ’uberftp’, host.strip(),
- writen to file: Banned/NotBanned, Site, Sevice, Host

Report Generation Ticket transactions

- Use RT’s rest API to obtain 500+ transactions
- Automated analysis: looking for keywords
  - Reply to broadcast usually contain original mail
  - After a broadcast all keywords in it have to be ignored
- Automation (python script):
  - Parsing all input (text, gpg-encrypted, tar, zip, etc)
  - Logic: Matching keywords, excluding after broadcasts
- Problem: The more ’specific the questions’ the easier to parse, but you give away too much information the RC should find out.

Report Generation Metrics/Keywords

- Working well:
    - RT: First reaction from site (report/response)
    - RT: Submitted glite/Dirac job ID (per site)
    - RT: Uniq UUID hidden in jobs (per site)
    - SSCMonitor: Last ping from malicious payload
- With false positives (present in broadcasts):
    - RT: Malicious user
    - RT: Payload files, behavior (IoCs)
    - RT: Malicious IPs (IoCs)
- Partial/Missing data:
    - Not collected: Affected worker nodes IPs
    - BanMonitor: Proxy expired quickly after ban in VOMS

Report Generation
Exact keywords

- Malicious user:
  - Firstname Lastname
  - Username
- Payload files, behavior (IoCs)
  - *ratatosk.sh*
  - *aria2*
  - *Tor*, *tor-browser.tar.xz*, *download-tor.sh*, *torrent*
  - *elf*
- Malicious IPs (IoCs)
  - 194.171.96.118: Malicious submission
  - 194.171.96.106: DDOS victim

Report Generation

- Set of scripts to extract data from RT-IR, output as CSV
- Ingest into SQLite DB (tagged by metric)
- Calculate site scores
- Generate Site/NGI/Project reports using PyLaTeX

Report Generation

- For each metric, used last mention as timestamp (or last communication if no mention)

Report Generation

- Note where a site doesn’t reply to the broadcast
- Note where there is no data for a particular metric
  - because it’s not relevant (DIRAC vs glite submission), or
  - because it wasn’t recorded

Report Generation - Scoring

- For each metric, a score is given as follows:

$$Score = Min\left(100, DONE \times 100 \times \frac{TargetTime}{ActualTime}\right)$$

- 100 is the max. score obtainable for fulfilling the objective
- Timing starts from initial broadcast on afternoon Friday 15th March
- Responses before that time get max score

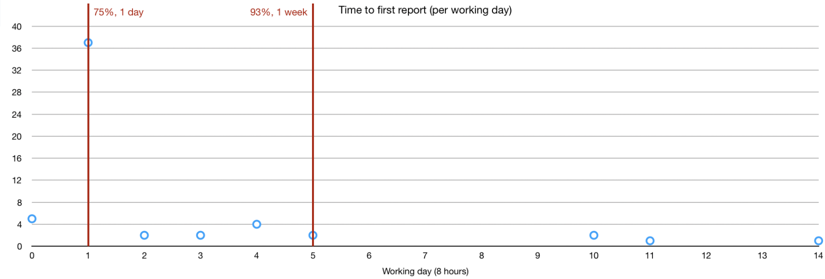
Report Generation - Sections

- Each site report will have three sections:
  - Reporting/Communication
  - Containment/Operations
  - Forensics (General, Network traffic, Payload binary)
- For each section, score is average of scores for each metric
- Final score is average of the three sections

Report Generation: Reporting/Communication

- First Report to CSIRT (target 4 working hours, source RT-IR)
- Max: 109 hr Mean: 11.4 hr Min: 0 hr
- Includes responses before initial broadcast
- Sites within target for first report: 66%
- Number of sites with no reply: 5
- Max score: 100.0 — Mean score: 69.1 — Min score: 0.0

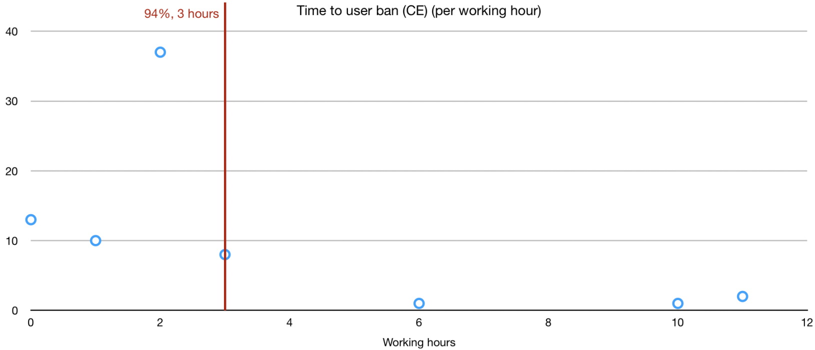
Report Generation: Reporting/Communication



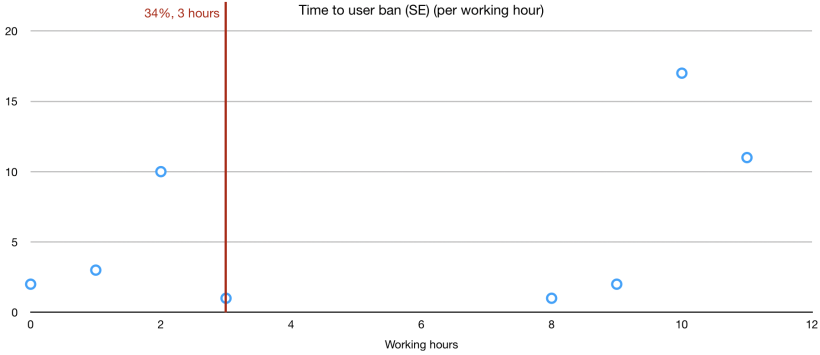
Report Generation: Containment/Operations

- User suspended (CE) (target 4 working hours, source BanMonitor)
  - Max: 10 hr Mean: 1.7 hr Min: 0 hr
- User suspended (SE) (target 4 working hours, source BanMonitor)
  - Max: 10 hr Mean: 6.9 hr Min: 0 hr
- Bot last seen (target 8 working hours, source SSCMonitor)
  - Max: 387 hr Mean: 16.9 hr Min: 0 hr
- Max score: 100.0 — Mean score: 83.0 — Min score: 0.0

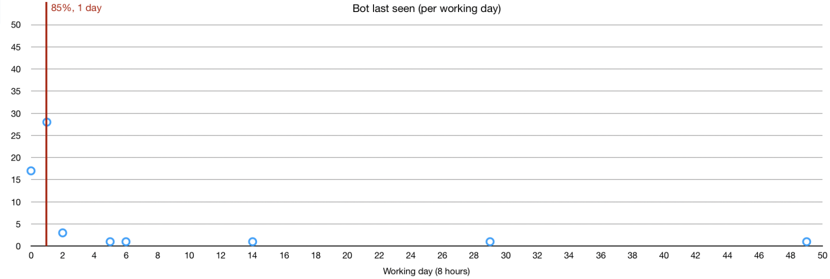
Report Generation: Containment/Suspend DN



Report Generation: Containment/Suspend DN



Report Generation: Containment/Kill malicious proc's



Report Generation: Forensics

- Found user (target 8 working hours, source RT-IR)
- Found DIRAC,glite JobID,UUID
- Found indicator of compromise
- Found payload binary
- Max score: 47.0 — Mean score: 7.2 — Min score: 0.0

Report Generation: Notes

- For forensics, many jobs died over initial weekend, which made it difficult to carry out forensics
- Scores are necessarily a mix of site performance and circumstance
- Factors into interpretation
- Broad conclusions can be drawn

Report Generation: Next steps

- Because of automated process, need validation step
  - c.f. WLCG Availability reports
- Propose to send round reports to sites and give window for comment
- Following this prepare final reports
- Complete this step by end of July followed by submission of final reports to management
- In parallel, send closing announcement to security contacts

Summary

Summary

Incident response landscape in distributed infrastructures is complex. If we adhere to our policies, i.e. act predictably for all involved security teams, we can largely minimize the impact of a large scale incident. If we don’t, chances are that the service availability for a VO will be largely degraded.

Goal of the SSC

Answer to the questions:

- what is the overall security situation?
- → In general good
- how well are the different IR procedures interfaced to each other?
- → could/needs to be better
- what are the pitfalls in IR?
- → lack of collaboration of the Security Teams, unpredictable behaviour of the partners

SSC: how did it go and what we learned

Christophe HAEN

On behalf of the LHCb Computing group

10.07.2019

How it went ?

1) First contact

Email sent to the mailing list declared in the VOCard
⇒ No answer

2) After a reminder

One person (let's call him *Paul*) from the mailing list forwarded to another operational mailing list
⇒ Not followed up

3) After more reminders

Experts gave instructions to Paul how to get the required info
⇒ Took a while, but Paul sent back the information

Why it took so long?

Mailing list in the VOCard

Clearly, not the good one:

- Operational team was not aware at first
- Paul did not know how to retrieve the info
- Paul did not even have enough karma to get them

Timing of the SSC was quite unfortunate

The exercise was triggered right when we started a big and difficult release.

Lack of procedure documentation

No clear guideline on who should react.

What we learned

Another mailing list in the VOCard

Contains people on shift and experts

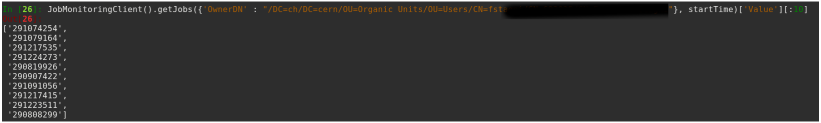
Defined clear guidelines for shifters

Who should react when, what can be asked, whom to ask for help, etc

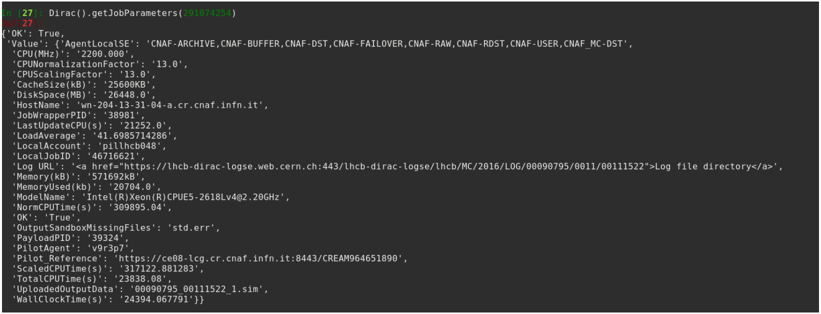
Technical improvements

- Easier to find some information (already developed before the SSC, waiting for release)
- Better banning system on the VO side

Jobs from DN

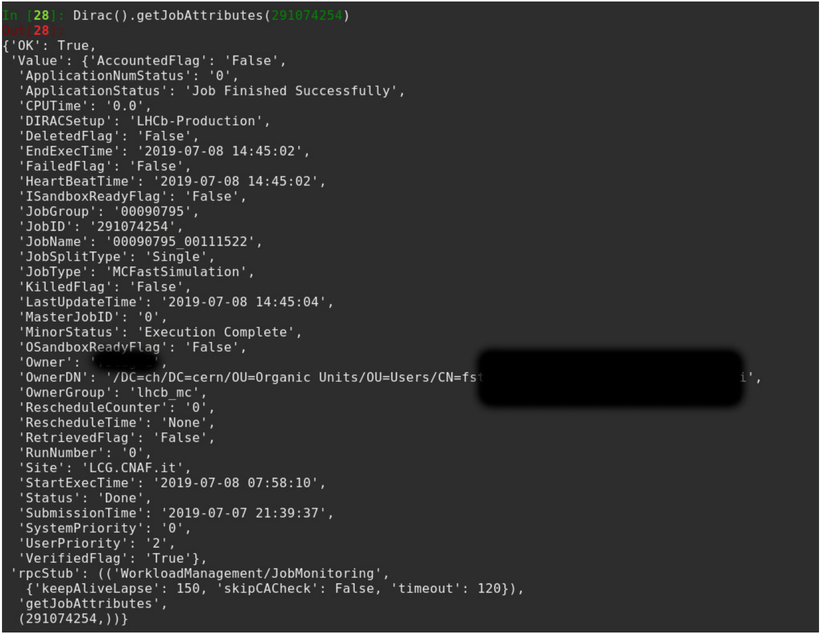


```
In [26]: JobMonitoringClient().getJobs({'OwnerDN' : "/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=fst[redacted]"}, startTime)['Value'][:10]
Out[26]:
['291074254',
 '291079164',
 '291217535',
 '291224273',
 '290819926',
 '290907422',
 '291091056',
 '291217415',
 '291223511',
 '290808299']
```



```
In [27]: Dirac().getJobParameters(291074254)
Out[27]:
{'OK': True,
 'Value': {'AgentLocalSE': 'CNAF-ARCHIVE,CNAF-BUFFER,CNAF-DST,CNAF-FAILOVER,CNAF-RAW,CNAF-RDST,CNAF-USER,CNAF_MC-DST',
  'CPU(MHz)': '2200.000',
  'CPUNormalizationFactor': '13.0',
  'CPUScalingFactor': '13.0',
  'CacheSize(kB)': '25600KB',
  'DiskSpace(MB)': '26448.0',
  'HostName': 'wn-204-13-31-04-a.cr.cnaf.infn.it',
  'JobWrapperPID': '38981',
  'LastUpdateCPU(s)': '21252.0',
  'LoadAverage': '41.6985714286',
  'LocalAccount': 'pillhcb048',
  'LocalJobID': '46716621',
  'Log URL': '<a href="https://lhcb-dirac-logse.web.cern.ch:443/lhcb-dirac-logse/lhcb/MC/2016/LOG/00090795/0011/00111522">Log file directory</a>',
  'Memory(kB)': '571692kB',
  'MemoryUsed(kb)': '20704.0',
  'ModelName': 'Intel(R)Xeon(R)CPUE5-2618Lv4@2.20GHz',
  'NormCPUTime(s)': '309895.04',
  'OK': 'True',
  'OutputSandboxMissingFiles': 'std.err',
  'PayloadPID': '39324',
  'PilotAgent': 'v9r3p7',
  'Pilot_Reference': 'https://ce08-lcg.cr.cnaf.infn.it:8443/CREAM964651890',
  'ScaledCPUTime(s)': '317122.881283',
  'TotalCPUTime(s)': '23838.08',
  'UploadedOutputData': '00090795_00111522_1.sim',
  'WallClockTime(s)': '24394.067791'}}
```

Job attributes



```
In [28]: Dirac().getJobAttributes(291074254)
Out[28]:
{'OK': True,
 'Value': {'AccountedFlag': 'False',
  'ApplicationNumStatus': '0',
  'ApplicationStatus': 'Job Finished Successfully',
  'CPUTime': '0.0',
  'DIRACSetup': 'LHCb-Production',
  'DeletedFlag': 'False',
  'EndExecTime': '2019-07-08 14:45:02',
  'FailedFlag': 'False',
  'HeartBeatTime': '2019-07-08 14:45:02',
  'ISandboxReadyFlag': 'False',
  'JobGroup': '00090795',
  'JobID': '291074254',
  'JobName': '00090795_00111522',
  'JobSplitType': 'Single',
  'JobType': 'MCFastSimulation',
  'KilledFlag': 'False',
  'LastUpdateTime': '2019-07-08 14:45:04',
  'MasterJobID': '0',
  'MinorStatus': 'Execution Complete',
  'OSandboxReadyFlag': 'False',
  'Owner': '[redacted]',
  'OwnerDN': '/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=fs[redacted]i',
  'OwnerGroup': 'lhcb_mc',
  'RescheduleCounter': '0',
  'RescheduleTime': 'None',
  'RetrievedFlag': 'False',
  'RunNumber': '0',
  'Site': 'LCG.CNAF.it',
  'StartExecTime': '2019-07-08 07:58:10',
  'Status': 'Done',
  'SubmissionTime': '2019-07-07 21:39:37',
  'SystemPriority': '0',
  'UserPriority': '2',
  'VerifiedFlag': 'True'},
 'rpcStub': (('WorkloadManagement/JobMonitoring',
   {'keepAliveLapse': 150, 'skipCACheck': False, 'timeout': 120}),
  'getJobAttributes',
  (291074254,))}
```

Questions, comments