

Security Service Challenge 3 @ TU Dortmund

GridKa Summer School 2009

Stefan Freitag

Robotics Research Institute
TU Dortmund

4. September 2009

 technische universität
dortmund

Contents

Security
Service
Challenge 3 @
TU Dortmund

S. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

1 Grid @ TU Dortmund

2 Before the incident

3 Incident reaction

4 Conclusion

Supported Middlewares

Security
Service

Challenge 3 @
TU Dortmund

5. Freitag

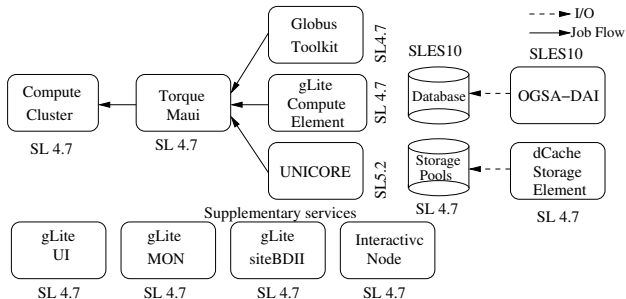
Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

- Compute services
 - gLite 3.1
 - Globus Toolkit 4.0.x
 - UNICORE5/ UNICORE6
- Storage services
 - dCache 1.8/1.9
 - OGSA-DAI 2.2



System 1 (ITMC, compute center)

- 256 Blade-Server, each 2 Intel Xeon Quadcore
- 8 Fileserver, 108 TByte capacity
- all nodes para-virtualized
- workernodes: 8 cores, 12 GB RAM

System 2 (Robotics Research Institute)

- 50 Blade-Server, each 2 Intel Xeon Dualcore
- 1 Fileserver, 6 TByte capacity
- workernodes: 4 cores, 4 GB RAM

Administration

- System 1 & System 2 administered by same staff
- Quantity of staff: 1 (no backup!)
- Staff not belonging to ITMC
- Best effort - administration is not part of my contract

Security

- Two site security officers (Klaus & myself)
- Grid cluster layout not document, Sitemap exists in my head
- Compute center security team: 3 people, no Grid exp.

Current situation

- Self-scripted installer for Grid service
- bash-based
- Templates for the different services

Possible future

- Use workflow processes for installation & configuration of basic operating system, Grid middleware services, and virtual appliance.

Security/ Monitoring

- Firewall (System 1: ssh not really restricted to limited list of IPs)
- Intrusion Detection System with central logging
- Nagios/ Ganglia

Time before Test Incident

15.07.09 received „[Heads up] Security Services Challenge (SSC)„

16.07.09

Mail from Klaus

Hello Stefan, have you seen this? I am afraid that something's gonna happen. [...]

17.07.09 received „Info: Incident response procedure“ noticed mail, but skipped reading the attachment as it was 5.30 pm → weekend!

20.07.09 received „[THIS IS A TEST] UNI-DORTMUND“ back from weekend a lot of other stuff was to do

Incident reaction

Security
Service
Challenge 3 @
TU Dortmund

5. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

20.07.2009

- Sent E-Mail to Ursula
- Read Incident response procedure
- Informed Klaus and local security team

Answer from Klaus

In the afternoon he will be out → excursion with physics department

- Disconnected affected workernodes from network
- E-Mail to VO manager of compromised user
- Contacted CA of the user

User Banning

Security
Service

Challenge 3 @
TU Dortmund

S. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

```
/var/log/globus-gatekeeper.log
```

```
TIME: Mon Jul 20 08:29:31 2009
PID: 25741 -- Notice: 6: Got connection XXX.XXX.XXX.
      XXX at Mon Jul [...]
[...]
2009-07-20.08:29:32.0000025749.0000000000 for
/O=XX/O=XX/O=XX/CN=XX on XXX.XXX.XXX.XXX
JMA 2009/07/20 08:29:32 GATEKEEPER_JM_ID
2009-07-20.08:29:32.0000025749.0000000000 has
      EDG_WL_JOBID
' https://logging&bookkeepingserver:9000/someJobID '
GATEKEEPER_DGAS_FD=8
[...]
PID: 25749 -- Notice: 0: Child 25751 started
```

User Banning

Security
Service

Challenge 3 @
TU Dortmund

5. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

- udo-ce01 and udo-ce03: added DN to
`/opt/glite/etc/lcas/ban_users.db`

```
"/C=XX/O=XX/OU=XX/CN=XX"
```

Listing 1: Example ban_users.db

- udo-dcache01 and udo-dcache03: user was NOT banned

A problem arose with gPlazma vorole-mapping

What do I have to ban?

- Distinguished Name?
- Distinguished Name + compromised VO/Role?
- assuming user is in multiple VOs: Distinguished Name + all VOs/Roles the user can obtain?

Incident reaction

Security
Service
Challenge 3 @
TU Dortmund

S. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

21.07.2009

- Arranged meeting with local security team
 - was advised to use signed mails for communication
 - contacted network admins and forwarded netflow to me
 - received no further support from security team
- Created downtime for udo-ce01/ udo-dcache01
- Asked Manfred Alef for support in finding affected UI
- Received information concerning UI from Angela Poschlad
- Analysed executables and found SSC3 raffle string
- Updates of incident report, changed time format to UTC

Incident reaction

Security
Service

Challenge 3 @
TU Dortmund

S. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

22.07.2009

- Analyzed netflow to/fro affected workernode
 - found no anomalies
 - requested a netflow for a larger time interval
 - heard nothing more from local security team/ network admins
- Preparation and submission of final report
- Re-installation of affected workernodes

Conclusion

Security
Service

Challenge 3 @
TU Dortmund

S. Freitag

Grid @ TU
Dortmund

Before the
incident

Incident
reaction

Conclusion

- + Increased level of security (disabling crontab, atd for users)
- + Helped to classify latest Kernel vulnerability as serious issue
- + Another test for our template-based installation
 - Incident happend at a bad moment (Murphys Law)