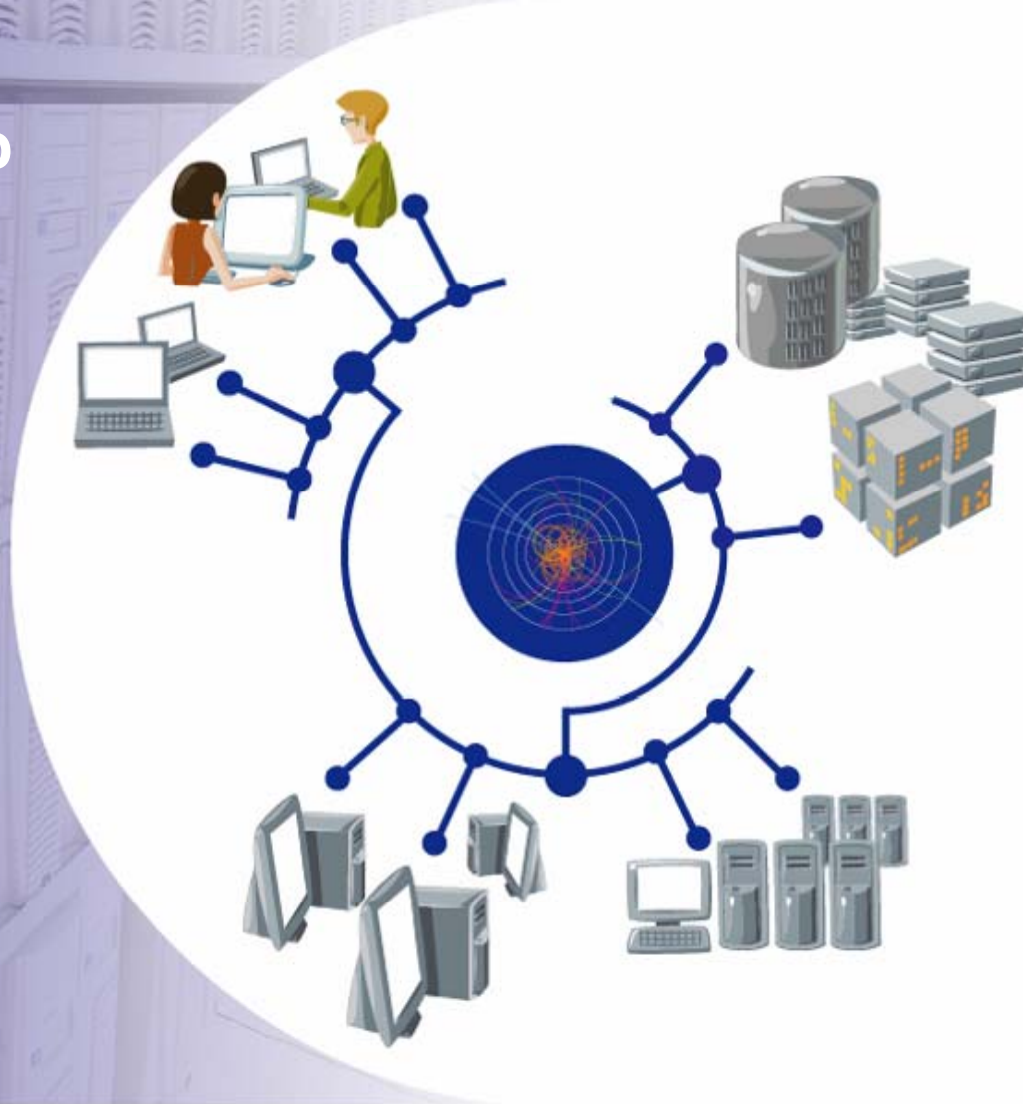




# On the transition to EGI – Requirements from WLCG

WLCG Workshop  
24<sup>th</sup> April 2008

Ian Bird  
LCG Project Leader





# Agenda

- EGEE Operations today
    - Operations, middleware, security, support, policy
  - EGEE Operations tomorrow – EGEE-III
    - What changes now, how does it evolve to 2010?
    - What EGEE ops will look like in 2010 → reduced effort for operations
  - EGI/NGI operations in future
    - Must have a smooth transition
    - What does LCG rely on (vs what is useful)?
    - What must we see:
      - NGI functions
      - EGI functions
      - Middleware – what does LCG rely on?
      - Interoperability with other infrastructures
- ✘ At no time can there be an interruption to the WLCG service !!



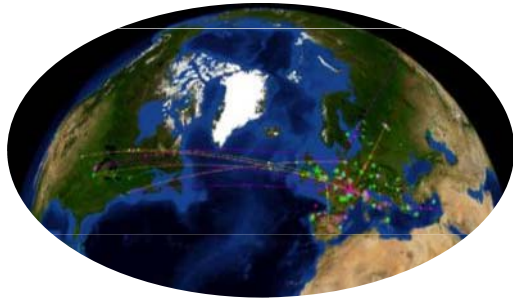
## EGEE Operations Now

NB.

In discussing “operations” I will mix SA1, SA3, JRA1 and etc.

NB2:

Most of this is what “LCG Deployment” started out doing, and then passed responsibility to EGEE (in Europe!)



## Test-beds & Services

Production Service

Pre-production service

Certification test-beds (SA3)

Training infrastructure (NA4)

## Support Structures & Processes

Operations Coordination Centre

Regional Operations Centres

Global Grid User Support

EGEE Network Operations Centre (SA2)

Operational Security Coordination Team

Training activities (NA3)

## Security & Policy Groups

Joint Security Policy Group

EuGridPMA (& IGTF)

Grid Security Vulnerability Group

Operations Advisory Group (+NA4)



# Operations

- Grid Operations:

- Regional Operations Centres (ROCs) – responsible for operations within a region (large country ... regions of many countries) (11)
  - ROCs responsible for “management” (== coordination) of sites in the region
- Coordination by the Operations Coordination Centre (OCC)
- Features:
  - Grid Operator on Duty (“COD”) – staffed by ROCs, coordinated by IN2P3; weekly rotation of teams: monitoring tools used to spot problems and then open tickets to sites and/or ROCs; ticket follow up
  - Central tools e.g. SAM, accounting, GOCDB, etc.
  - Start to see connection of SAM tests to site fabric monitors
  - Start to see SLAs between sites and ROCs
  - Rather complete set of operations procedures, including interop with OSG



The “COD” is labour-intensive, BUT has been critical is getting the operation into the good state it now is, and improving site reliability



# Support

- GGUS is used in several ways – user support, network, and operations support
    - Interconnected ticketing systems with ROCs
  - Operations support
    - COD opens tickets – sent to ROCs and sites
  - User support
    - Used as central “helpdesk” – tickets managed by TPMs:
      - Categorize, dispatch, follow up
      - TPMs are responsibility of ROCs
    - Issues around use for “urgent” operations issues – should be direct dispatch and not via TPM -> need to separate “expert” and “user”
  - Network operations
    - GGUS is used to track all network interventions
- ↪ GGUS has been essential in
- providing central (known!) access point;
  - enabling a managed and tracked process (cannot have reliable ops without this).



# Security

- Operational security
  - Bridges between individual site security – does not replace it
  - Coordination at OCC
  - Should have responsible in each ROC (failed in EGEE-2); use NREN CERTs where possible
  - Full set of procedures to manage incidents, best practices, etc.
  - “Fire drills”, and probing to see if sites are using appropriate tools
- Vulnerability group
  - Set up to look at security vulnerabilities before they became problems
  - Very active in first year of EGEE-II; very quiet now (lack of effort?)
  - Effort was largely “voluntary”
  - Useful function – uncovered some real issues
  - Publishing policy (and practice) is tricky (and not fully resolved...)



# Policy

- JSPG
  - Key group in writing and agreeing policies
  - The wide variety of policies have been key in allowing the overall operation to be implemented
    - E.g. Addressing privacy issues, publication of data, etc.
  - Has been a group with broad membership
  - Has succeeded in producing portable (and hence common) policies in key areas
  - An area where EGEE is well advanced compared to others?
  
- IGTF/EUGridPMA
  - And local CAs and RAs (and catch-all CA)
  - Essential for the infrastructure





# Middleware

- **Development**
  - We have a fairly complete set of services essential for WLCG (with some holes – glEXEC, etc)
  - Many of the issues of reliability, manageability, scalability, etc. have (still) not been adequately addressed
  - Some solutions are probably too complex for the WLCG needs
  - Producing new middleware services and getting them to production has not been very easy ...
- **Integration/cert/testing etc. → Building a common m/w distribution**
  - Certification testing has been critical in producing middleware that can manage the stress we expose it to
  - The process is maligned – it is usually not the certification itself that is slow – but it does what it should – it uncovers problems
  - The gLite distribution is unwieldy ... overall the middleware is probably too complex



# Operations in EGEE-III

How does it evolve?



# Operations evolution

- Anticipates ending EGEE-III with the ability to run operations with significantly less (50%?) effort
  - Moving responsibility for daily operations from COD to ROCs and sites
  - Automation of monitoring tools – generating alarms at sites directly
  - Site fabric monitors should incorporate local and grid level monitoring
    - Need to ensure all sites have adequate monitoring
    - Need to provide full set of monitoring for grid services
  - The manual oversight and tickets should be replaced by automation
    - Remove need for COD teams
  - Operations support should have streamlined paths to service managers
    - Eliminate need for TPMs for operations
  - Need to insist on full checklist (sensors, docs, etc) from middleware
  - This process is the subject of formal milestones in the project



# Other operational aspects

- **User support**
  - Streamlining process for operations
  - Focus of TPM effort on real user “helpdesk” functions – TPMs now explicitly staffed by ROCs (were not in EGEE-II)
- **Security**
  - Operational security team also have explicit staffing from regions to ensure adequate coverage of issues
  - Focus on implementing best practices at sites
- **Policy**
  - Efforts should continue at the current level



# Middleware ?

- In EGEE-III the focus on middleware is the support of the foundation services
  - These map almost directly to the services WLCG relies on
  - Should include addressing the issues with these services exposed with large scale production
  - Should also address still missing services (SCAS, glexec, etc)
  - Should also address the issues of portability, interoperability, manageability, scalability, etc.
  - Little effort is available for new developments
  - (NB tools like SAM, accounting, monitoring etc are part of Operations and not middleware)
- Integration/certification/testing
  - Becomes more distributed – more partners are involved
    - In principle should be closer to the developers
  - ETICS is used as the build system
  - Probably not enough effort to make major changes in process



# EGEE Operations in 2010 ...

- Most operational responsibilities should have devolved to
  - The ROCs, and
  - The sites – hopefully sites should have well developed fabric monitors that monitor local and grid services in a common way and trigger alarms directly
    - Receive triggers also from ROC, Operators, VOs, etc.; and tools like SAM
- The central organisation of EGEE ops (the “OCC”) should become:
  - Coordination body to ensure common tools, common understanding, etc.
  - Coordination of operational issues that cross regional boundaries
    - The ROCs should manage inter-site issues within a region
  - Maintain common tools (SAM, accounting, GOCDDB, etc.)
    - Of course, the effort in these things may come from ROCs
  - Integration/testing/certification of middleware (SA3)
  - Monitor of SLA’s, etc. (and provide mechanisms for WLCG to monitor MoU adherence)
  - ...



## ... Operations in 2010

- Ideally we should have an operational model with daily operational responsibility at the regional or national level (i.e. the ROCs)
- This will make the organisational transition to NGIs simpler – if the NGIs see their role as taking on this responsibility ...



# Transition to NGI/EGI

## What and how?

- In order to describe how we must propose what the model looks like
- This is my view of what a future European infrastructure should have in order to continue to provide services to WLCG





# The role of the NGI

- The NGI operations centres (NGOC) should assume the roles of the ROCs as they are at the end of EGEE-III
  - In large countries this might be a 1:1 mapping – the ROCs exist
  - In smaller countries could still foresee regional agreement on a common regional operations centre
- Roles:
  - Grid operations oversight (but most should be automated!!) and follow up
    - Oversight of SLAs, reliability, resource delivery, etc.
  - Operational security management
  - User support (regional helpdesks already exist in many ROCs) – but with connection to EGI for cross-NGI applications
  - Etc. →the daily operation
  - But, as the NGI (should be!) part of a larger infrastructure, must use compatible tools/metrics/reporting as other NGIs



# The role of EGI

- **Coordination across the NGIs**
  - Operations – overall SLAs, reporting, accounting, reliability, etc.
    - Cross NGI operations issues should be an agreed process for the NGIs (EGI should broker these processes)
  - Brokering of resources for applications with the NGIs
  - Operational security coordination – e.g. Incident response
  - Common policy brokering
  - Support for international VO's (like WLCG) – should they really negotiate with 35 NGIs?
  
- **Integration/certification/testing of middleware**
  - Whatever this means – many different stacks will be existing
  - Work on “interoperability” is difficult and slow, but running parallel middleware stacks on a site is also very costly



# Middleware evolution

- WLCG requires above all effort to ensure that issues that arise in real use are addressed:
  - By fixes
  - By focussed re-developments where needed
  - New use cases may arise or new services might be required after some experience
- Currently many different middlewares are proposed to be deployed in many NGIs
  - Risk that the effort required is not supportable
- We should aim to have a common repository of best (i.e. That are really used) services that slowly converges the differing implementations (or maintains several for different use cases)

WLCG Needs these things to be provided by EGI/NGI

## Test-beds & Services

Production Service

Pre-production service

Certification test-beds (SA3)

Training infrastructure (NA4)

## Support Structures & Processes

Operations Coordination Centre

Regional Operations Centres

Global Grid User Support

EGEE Network Operations Centre (SA2)

Operational Security Coordination Team

Training activities (NA3)

## Security & Policy Groups

Joint Security Policy Group

EuGridPMA (& IGTF)

Grid Security Vulnerability Group

Operations Advisory Group (+NA4)



# Summary

- EGEE is undergoing a natural transition to a more distributed model
  - The somewhat centralised model was necessary to get to this point
  - EGEE operations have always been a distributed effort
- This is driven by:
  - Practicality – it is simpler to solve service problems if the service manager detects them
  - Cost – it is unsustainable to maintain the current level of effort
- EGEE-III should already achieve a significant part of this evolution
- EGI/NGI can be a natural continuation of this process, BUT:
  - Must ensure that we do not break the global infrastructure we have by encouraging NGIs to be really autonomous
  - Must ensure that the EGI organisation is strong enough to tie this all together and provide a coherent, integrated service for those that need it
  - Must be very careful with middleware strategies in order to make the best use of what is available and not get bogged down in complexity



# Summary

- WLCG needs this process to be smooth and needs to understand very soon (i.e. this summer) what the landscape will look like in 2010
- The operation at the end of EGEE-III should be the EGI/NGI model – there is a very close match
  - However, many details to address between now and June!
- Concern that many current EGEE (and WLCG Tier 1 and Tier 2) partners are not well represented in the NGIs
  - This must change – we must be part of the process or we risk to have the wrong outcome

 **Please engage with your NGIs immediately!!**