Network and Grid Monitoring

Ludek Matyska
CESNET
Czech Republic
GRIDs – Basic Concepts

• Distributed Systems
  – Large scale
  – Spanning administrative domains
  – Heterogeneous
• Provide *processing* and *services*
• Very complex jobs
  – Workflows including data staging
  – Interaction of many components
Networks for GRIDs

- Basic underlying infrastructure
- Provide data transfer capability
- Usually not directly exposed
  - Except for data transfer planning
Network Information for GRIDs

• Availability and quality of paths
  – Network capacity prediction
  – Monitoring of actual data transfers
    • Fulfillment of SLA (implicit/explicit)

• Failover
  – Implicit
  – Explicit – new search for appropriate path
Network Capacity Prediction

• How/when I can transfer amount X of data from A to B?
• I have two sets of sites: \{A, B, C, \ldots\} (data sources) and \{X, Y, Z, \ldots\} (using data). Find me one node from the first and one node from the second set such that the transfer of data will be the fastest.
Network Monitoring Role

• The Network Capacity prediction needs a network monitoring data
  – Flow and flow patterns are needed

• NRENs collects this data to some extent only
  – And usually do not provide it to third parties
Network Weather Service (NWS)

• Collects information about flows through network
• Provides interface for predicted link/path capacity
• Challenges
  – Completeness of the information
    • Is deployed as a NREN service?
  – Unpredicted reaction of NWS users
    • Their reaction synchronized if not under control
  – Prediction is hard/impossible
Monitoring of Data Transfers

• Purpose:
  – Check the SLA
  – Provide data for prediction improvement
  – Look for patterns

• Identification of a particular flow
• Authorization to use such service
• Authorization to access data
  – At the end of data transfer
  – In real time
• Not (yet) commonly available
CESNET Systems

• G3 system
  – Infrastructure monitoring
  – SNMP based
  – High detail (e.g. history of virtual port related data)

• FTAS (Flow-based Traffic Analysis System)
  – Aggregate and individual flow information
  – Both IPv4 and IPv6 supported
  – Heavily used for security related incidents
    • DoS and DDoS attacks

• None currently used by the Grid community
Grid Information and Monitoring Services

• Almost every Grid component relies on some external information
• Information provides every Grid element
  – Distributed producers
• Distributed Use
• Classical separation
  – Grid Information services
  – Grid Monitoring services
Grid Information Services

• “Static” information about elements
  – Number of CPUs
  – GPS location of nodes
  – Users and their affiliation
  – Actual length of a queue
  – Number of free CPUs

• Usually does not check itself
Grid Monitoring

• Infrastructure/status monitoring
  – Nodes
  – Services
    • May be distributed/duplicated/migrating
  – Jobs and their workflows

• Application monitoring
  – Infrastructure part
  – Particular application oriented part
Grid infrastructure monitoring

• Structure of service
  – Centralized
    • Easier to deploy
    • Scalability problems
  – Distributed/Hierarchical
    • Higher overhead
    • Reliability of monitoring components
Grid infrastructure monitoring

Nodes

• Monitor properties of nodes
  – Configuration
  – Services associated with nodes
    • Examples:
      – Job acceptance
      – Compiler availability

• Could run complex checks
  – Checkout a CVS and compile a program
Example of Node Monitoring

<table>
<thead>
<tr>
<th>Testbed Status</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The table shows test results for various nodes, with colors indicating the status of each test.
Grid infrastructure monitoring
Services

- General Grid services
- Service discovery
  - Where the service run now
- Redundancy
  - Check the service or all its copies?
- Grid monitoring itself a service
Grid infrastructure monitoring

Jobs

• Information about job flows through the Grid middleware
  – Distributed gathering of monitoring data
  – Must be somewhere completed

• Complex jobs/workflows

• EGEE Logging and Bookkeeping (LB)
  – Collects events triggered by job flow through the middleware
  – Computes job states on the fly
  – Provides user access to the job states
LB Service Architecture
Middleware instrumentation

• Idea to collect data from running middleware
  – Similar to the LB service, but more general
• Large number of sources
  – Distributed collection and processing
• SNMP ≠ SGMP?
Monitoring information dissemination

• Many places/services look for the data
• Streams of data
  – Monitoring data discovery
    • What is available where
• Events
  – Subscription/Notification
• Cross organizational data flow
  – Sharing monitoring data
Privacy/Security Considerations

• Potentially sensitive data collected
  – When/where to aggregate
  – Access authorization

• Extended use of mutual authentication of monitoring elements

• Not always required
  – Provision of alternate less secure (faster/low overhead) monitoring infrastructure
NRENs and GRIDs

• Role for NRENs
  – Provide information about the network
    • What is available where
  – Provide information and monitoring services for Grids
• In some aspects analogy to PERT/PACE
• Major challenges
  – Grids are multi-NRENs
  – (Much) more “users”
  – Privacy/Security
  – Heterogeneity of monitored elements
  – Portal and service access to the collected data
Questions?