Policy Management in Grids

(Aka "Identity Federation Management")

Marty Humphrey

Assistant Professor
Department of Computer Science
University of Virginia
Charlottesville, VA

Early Career Principal Investigator Program in Applied Mathematics, Collaboratory Research, Computer Science, and High-Performance Networks

Problem Statement (1)

- **Policy: preferences, rules, goals, conditions, obligations, and acceptable procedures**
- **Policies in VOs are everywhere**
  - Resource provider: *What is the order in which I will service requests?*
  - Resource consumer: *What are my requirements for data storage (e.g., availability)?*
  - Site-wide: *What authentication mechanism is required?*
  - VO-wide: *What experiments get preference? (e.g., Open Science Grid)*
- **Problem: today, policies are only implicit**
- **Why is this a problem?**
  - What went wrong? Why is my QoS so poor?

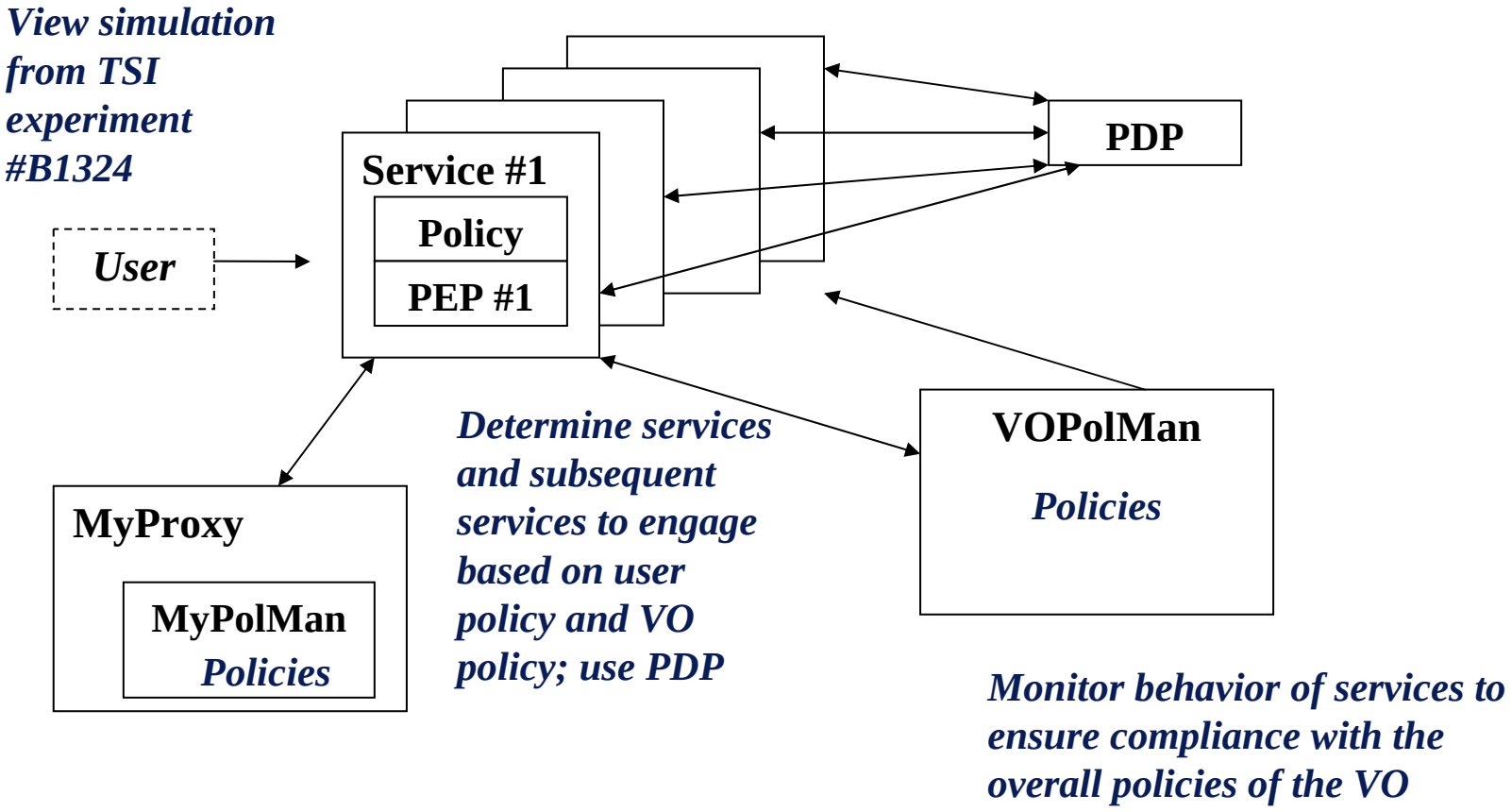
Problem Statement (2)

- **Lack of acceptable policy languages**
- **Humans cannot easily express their policies**
- **Software components cannot find relevant policies**
- **Policies cannot be matched/resolved**

Approach

- **MyPolMan**
  - Leveraging MyProxy to store/manage/retrieve my policies
    - “My credential can be retrieved by superschedulers but only for the purpose of querying candidate resources for my allocations”
    - “For services running under my credential, serve requests from users at ORNL before users from *.edu”
- **VoPolMan**
  - For physical organizations and virtual organizations
    - “All services must allow password authentication by prefer X.509-based authentication.”
    - “Each physical organization in the VO must contribute 10 Terabytes disk storage with an availability of 99%.”
    - “All work is to be performed on large queuing systems from 9 am – 5 pm and on PC clusters after hours.”

Grid Policy Management Architecture



Building Blocks

- **MyProxy (http://myproxy.ncsa.uiuc.edu)**
- **CredEx (ICWS'2005)**
- **SAML**
- **XACML**
- **WS-Policy**

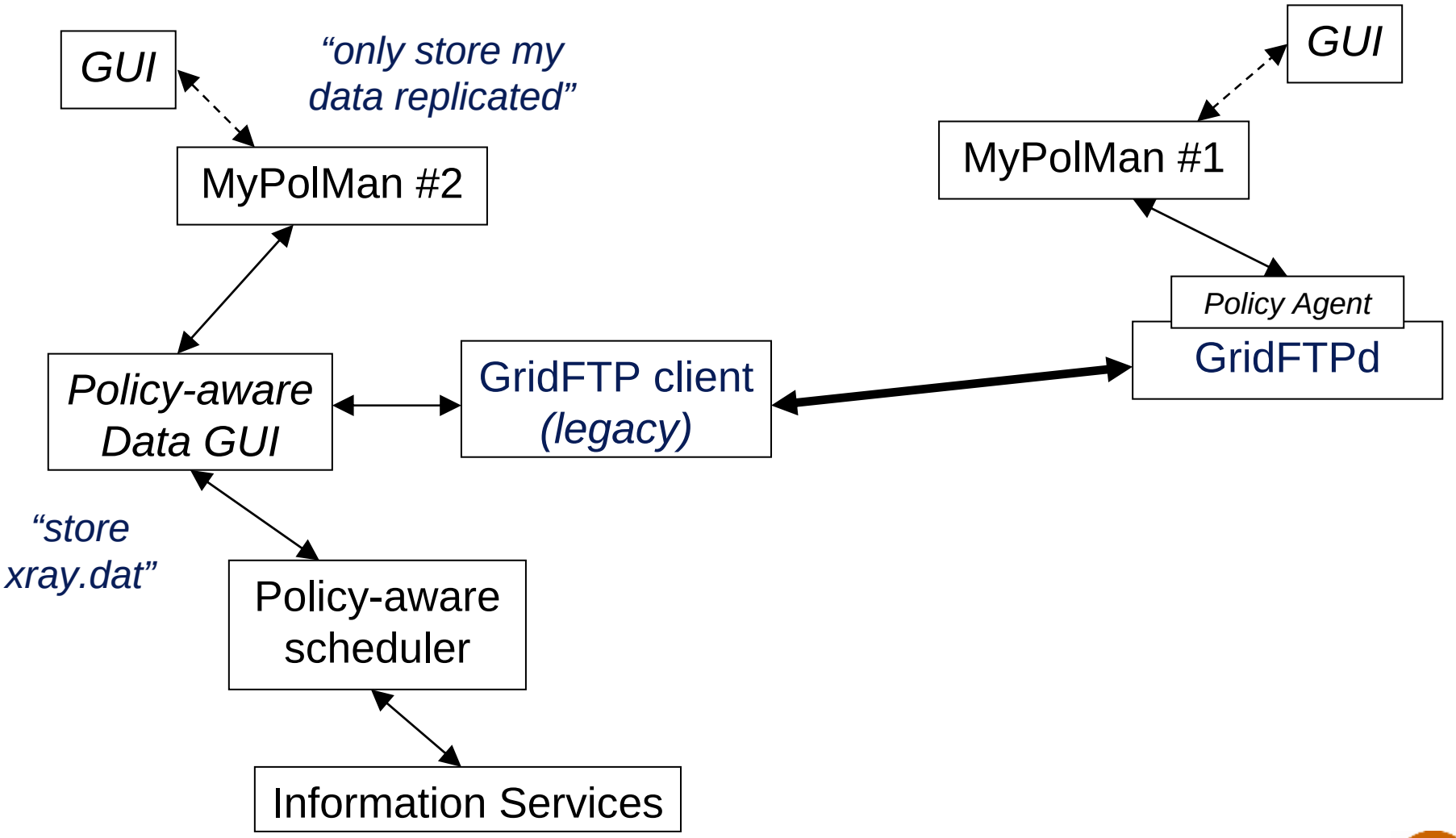
- ***All messages use WS-Security and/or SSL***

Requirements

- **Policy language**
- **Client-side GUI**
- **Publish/Subscribe/Discovery**
- **Policy evaluator**
- **Auditing**

- ***Interoperability: Standards-based***

Policy-Aware Data Movement



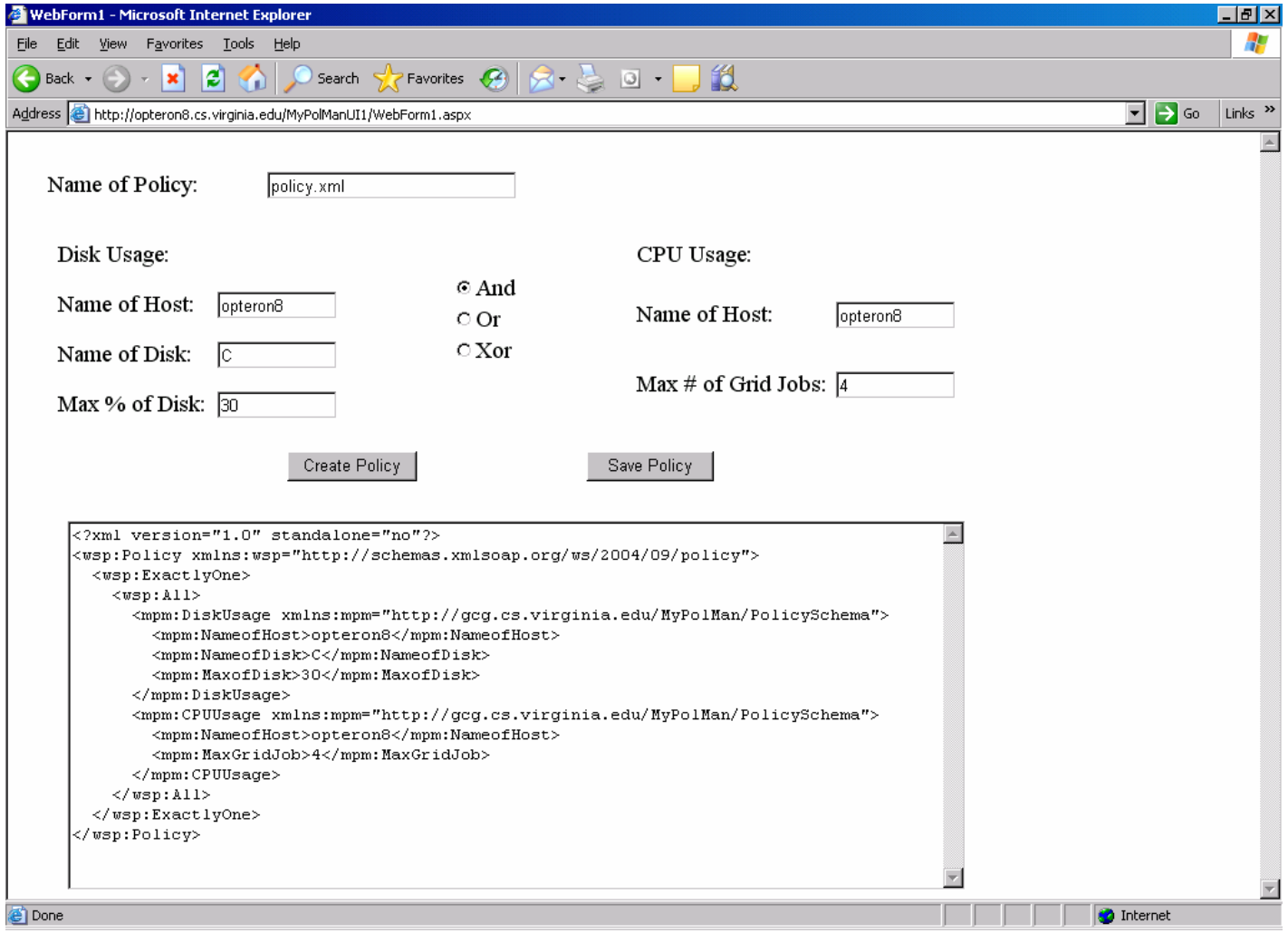
Resource Provider Data Policies

- **“Allow up to 30% of this disk for ‘Grid’ activities”**
  - “No one user can have more than 10G”
- **“Allow up to half of the network bandwidth to be used for ‘Grid’ activities”**
- **“Service ORNL requests before .edu requests”**
- **“All data requests must first be authenticated via GSI”**

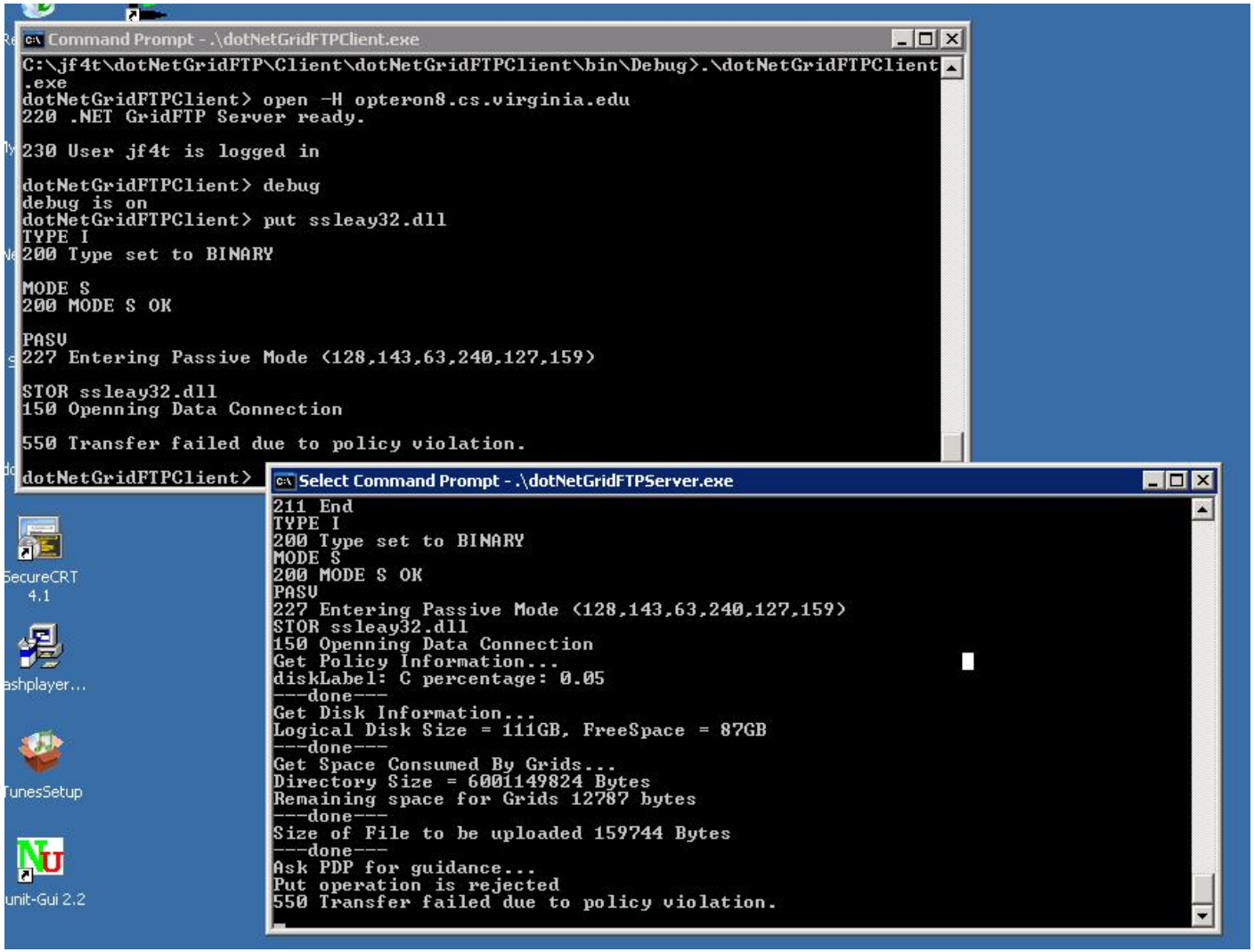
Consumer Data Policies

- **Bandwidth**
- **Response Time (Latency)**
- **Availability**
- **Access Control**
- **Authentication**
- **Persistence / “non-scrubability”**
- **Replication**
- **Backup**

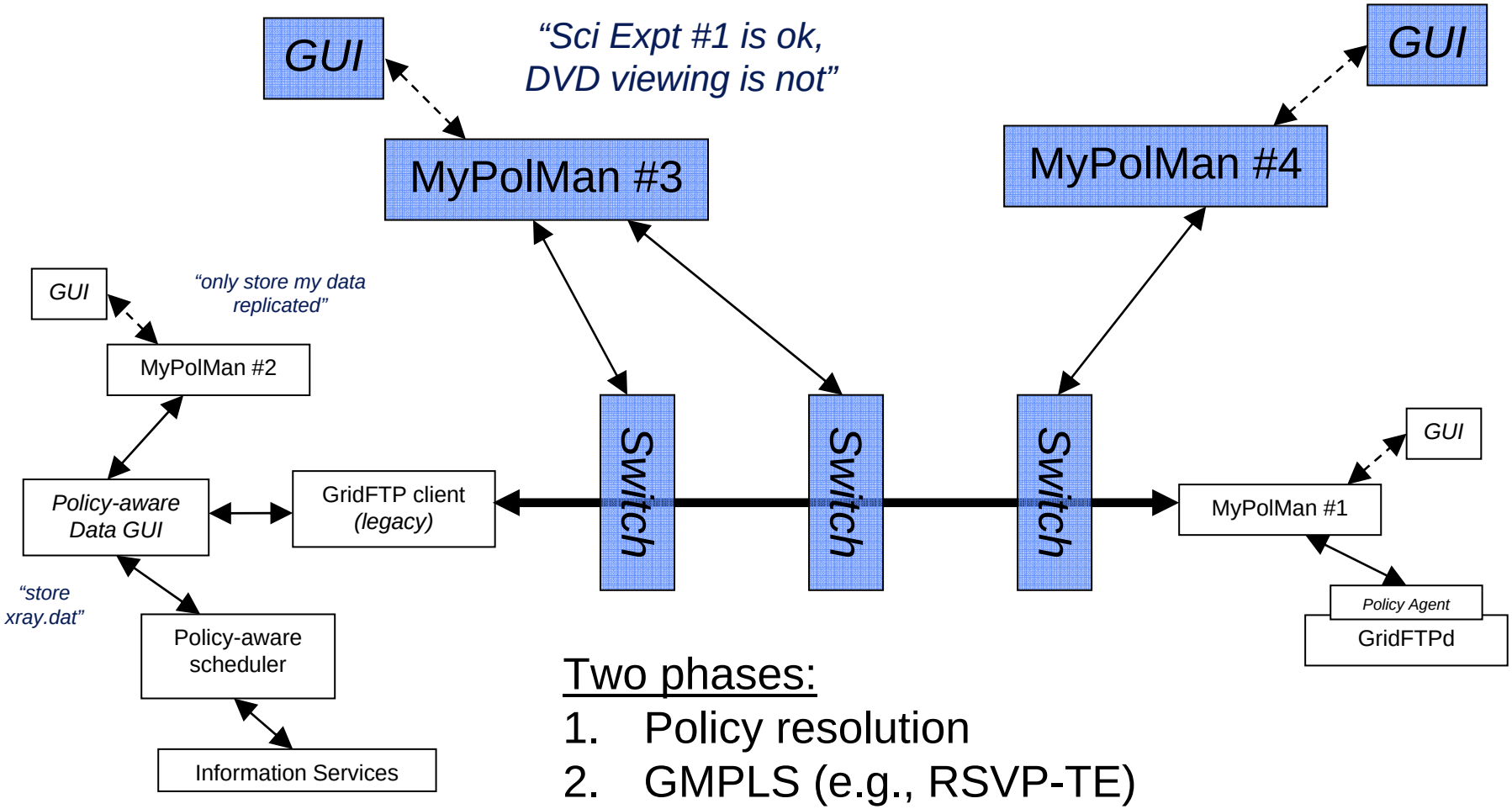
GUI


WebForm1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://opteron8.cs.virginia.edu/MyPolManUI1/WebForm1.aspx
Go Links
Name of Policy: policy.xml
Disk Usage:
Name of Host: opteron8
Name of Disk: C
Max % of Disk: 30
And
Or
Xor
CPU Usage:
Name of Host: opteron8
Max # of Grid Jobs: 4
Create Policy
Save Policy
<?xml version="1.0" standalone="no"?>
<wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
<wsp:ExactlyOne>
<wsp:All>
<mpm:DiskUsage xmlns:mpm="http://gcg.cs.virginia.edu/MyPolMan/PolicySchema">
<mpm:NameofHost>opteron8</mpm:NameofHost>
<mpm:NameofDisk>C</mpm:NameofDisk>
<mpm:MaxofDisk>30</mpm:MaxofDisk>
</mpm:DiskUsage>
<mpm:CPUUsage xmlns:mpm="http://gcg.cs.virginia.edu/MyPolMan/PolicySchema">
<mpm:NameofHost>opteron8</mpm:NameofHost>
<mpm:MaxGridJob>4</mpm:MaxGridJob>
</mpm:CPUUsage>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
Done
Internet

Runtime


Command Prompt - .\dotNetGridFTPClient.exe
C:\jf4t\dotNetGridFTP\Client\dotNetGridFTPClient\bin\Debug>.\dotNetGridFTPClient
.exe
dotNetGridFTPClient> open -H opteron8.cs.virginia.edu
220 .NET GridFTP Server ready.
230 User jf4t is logged in
dotNetGridFTPClient> debug
debug is on
dotNetGridFTPClient> put ssleay32.dll
TYPE I
200 Type set to BINARY
MODE S
200 MODE S OK
PASV
227 Entering Passive Mode (128,143,63,240,127,159)
STOR ssleay32.dll
150 Openning Data Connection
550 Transfer failed due to policy violation.
dotNetGridFTPClient>
Select Command Prompt - .\dotNetGridFTPServer.exe
211 End
TYPE I
200 Type set to BINARY
MODE S
200 MODE S OK
PASV
227 Entering Passive Mode (128,143,63,240,127,159)
STOR ssleay32.dll
150 Openning Data Connection
Get Policy Information...
diskLabel: C percentage: 0.05
---done---
Get Disk Information...
Logical Disk Size = 111GB, FreeSpace = 87GB
---done---
Get Space Consumed By Grids...
Directory Size = 6001149824 Bytes
Remaining space for Grids 12787 bytes
---done---
Size of File to be uploaded 159744 Bytes
---done---
Ask PDP for guidance...
Put operation is rejected
550 Transfer failed due to policy violation.
SecureCRT 4.1
unit-Gui 2.2

Better Policy-Aware Data Movement



Two phases:

1. Policy resolution
2. GMPLS (e.g., RSVP-TE)

Summary

- **Grids are not as usable as they can be**
  - Operations often fail because of (implicit) policy
- **We are designing/implementing a policy architecture**
  - Policy language, client-side GUI, Publish/Subscribe/Discovery, Policy evaluator, Auditing
- **Prototype policy-aware gridftp data movement**
  - Extend to network