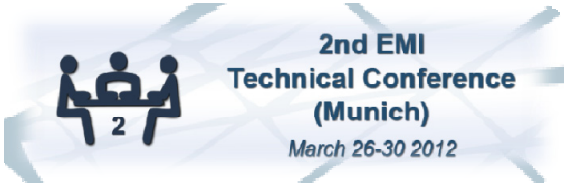
Software for Distributed Systems

The EMI Product Portfolio

Morris Riedel, Juelich Supercomputing Centre
EMI Strategic Director
2012-03-28

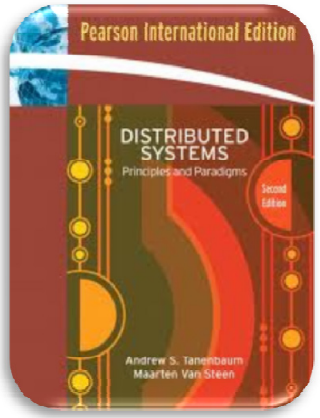


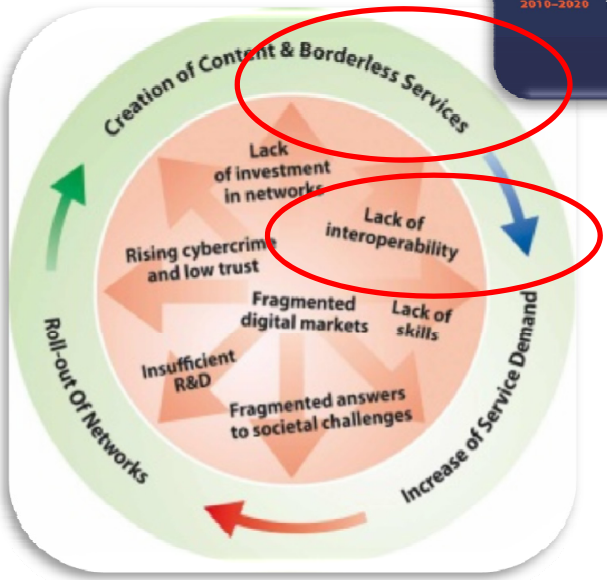
EMI is partially funded by the European Commission under Grant Agreement RI-261611

Greater Context of Talk

EUROPEAN MIDDLEWARE INITIATIVE

[3] Digital Agenda for Europe

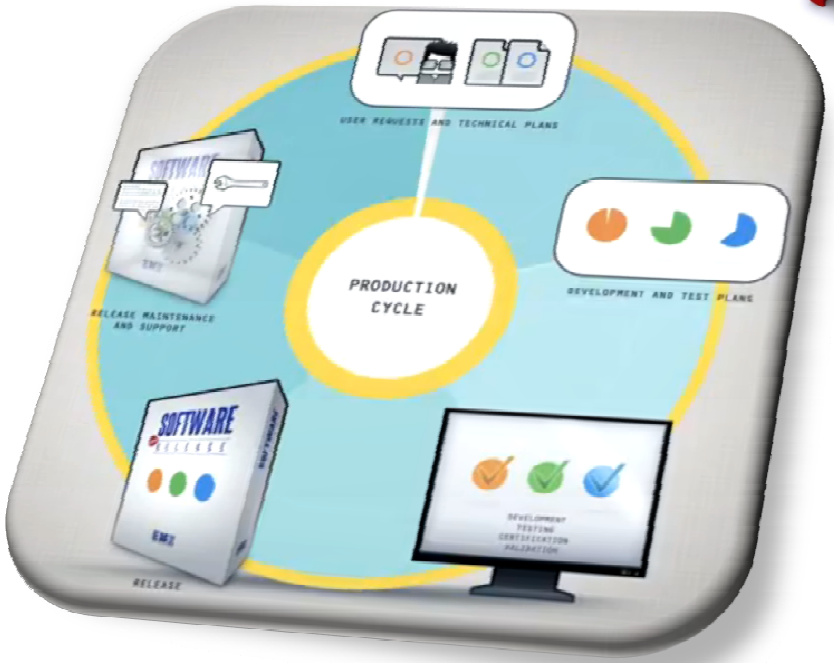




[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

Past & What is EMI?

10.000 ft Perspective

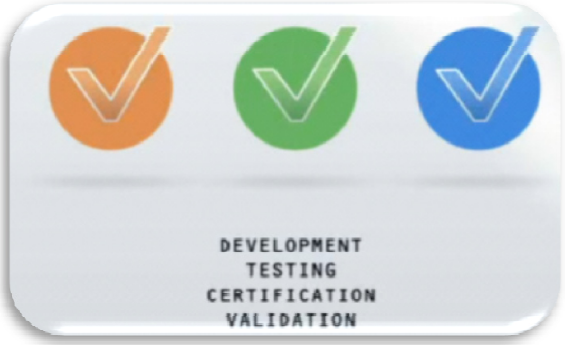


other scientific software tools

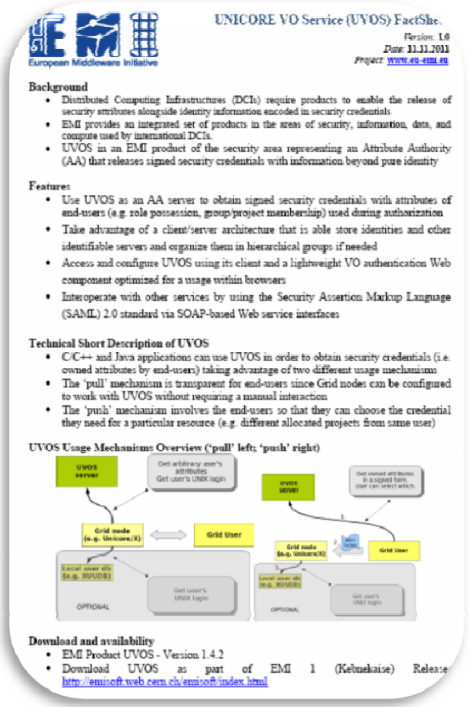
EMI INFSO-RI-261611

Present Achievements

- Middleware jointly developed & maintained
- Release process harmonized with policies
- Open Standards adoption increased & refined
- Explored several ways for sustainability



EMI FactSheets Available



UNICORE VO Service (UVOS) FactSht.

Version: 1.0
Date: 11.11.2011
Project: www.eu-emi.eu

Background

- Distributed Computing Infrastructures (DCIs) require products to enable the release of security attributes alongside identity information encoded in security credentials
- EMI provides an integrated set of products in the areas of security, information, data, and compute used by international DCIs.
- UVOS is an EMI product of the security area representing an Attribute Authority (AA) that releases signed security credentials with information beyond pure identity

Features

- Use UVOS as an AA server to obtain signed security credentials with attributes of end-users (e.g. role possession, group/project membership) used during authorization
- Take advantage of a client/server architecture that is able store identities and other identifiable servers and organize them in hierarchical groups if needed
- Access and configure UVOS using its client and a lightweight VO authentication Web component optimized for a usage within browsers
- Interoperate with other services by using the Security Assertion Markup Language (SAML) 2.0 standard via SOAP-based Web service interfaces

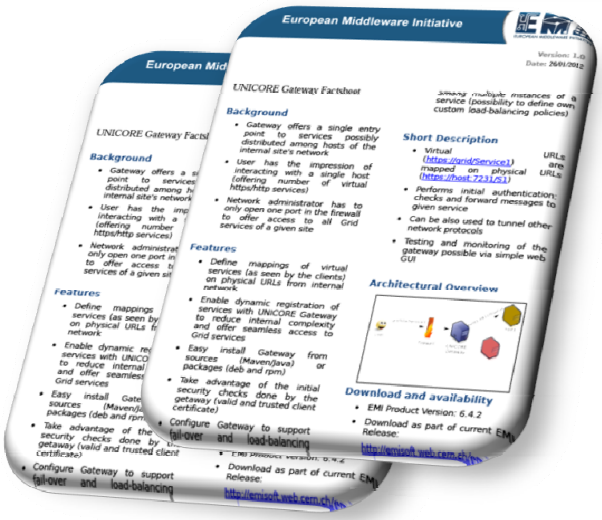
Technical Short Description of UVOS

- C/C++ and Java applications can use UVOS in order to obtain security credentials (i.e. owned attributes by end-users) taking advantage of two different usage mechanisms
- The 'pull' mechanism is transparent for end-users since Grid nodes can be configured to work with UVOS without requiring a manual interaction
- The 'push' mechanism involves the end-users so that they can choose the credential they need for a particular resource (e.g. different allocated projects from same user)

UVOS Usage Mechanisms Overview ('pull' left; 'push' right)

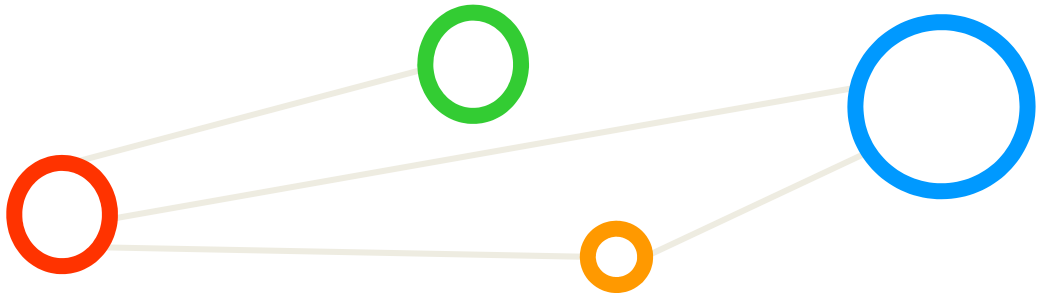
Download and availability

- EMI Product UVOS - Version 1.4.2
- Download UVOS as part of EMI 1 (Kebnekaise) Release http://emisoft.web.cern.ch/emisoft/index.html



[2] EMI Web Site - EMI Product Factsheets

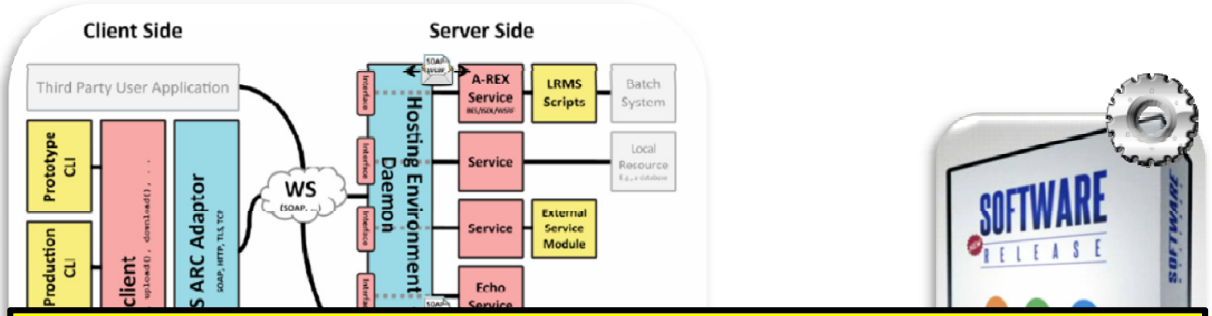
Distributed Systems Processing



EMI INFSO-RI-261611

ARC CE Added Value

- Used to submit and manage a wide range of applications running on computational resources of DCIs



Communication

'Where HTTP is the standard communication protocol for traditional Web-based distributed systems, the Simple Object Access Protocol (SOAP) forms the standard for communication with Web services…'

[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

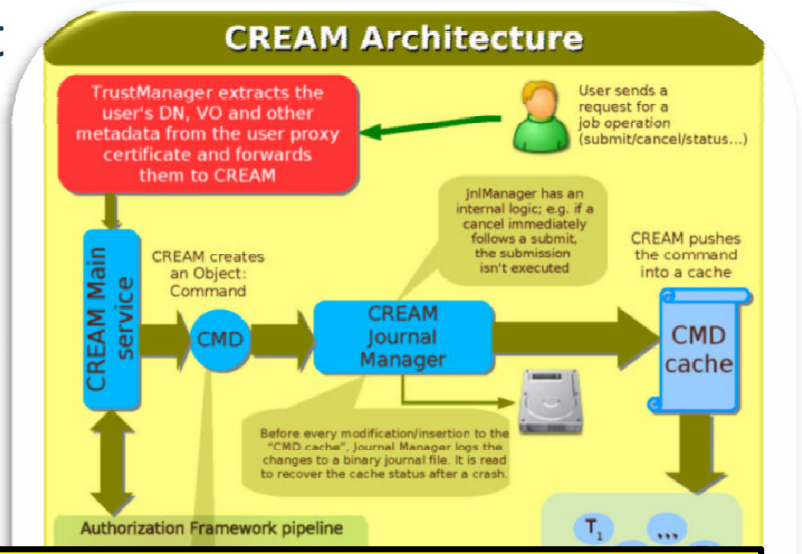
ARC CE Features

- Use the ARC CE as a light-weight system to execute applications across geographically distributed computing services and their underlying resources
- Take advantage of a client/server architecture that implements the functionality of a Computing Element (CE) accessing a wide variety of available batch systems
- Interoperate with other EMI services by using the EMI Execution Service via a SOAP-based Web service Interface

EMI INFSO-RI-261611

CREAM CE Added Value

- Used to submit and manage applications running on DCI resources



Servers – General Design Concurrent Server

'A concurrent server does not handle the request itself, but passes it to a separate thread or another process, after which it immediately waits for the next incoming request…'

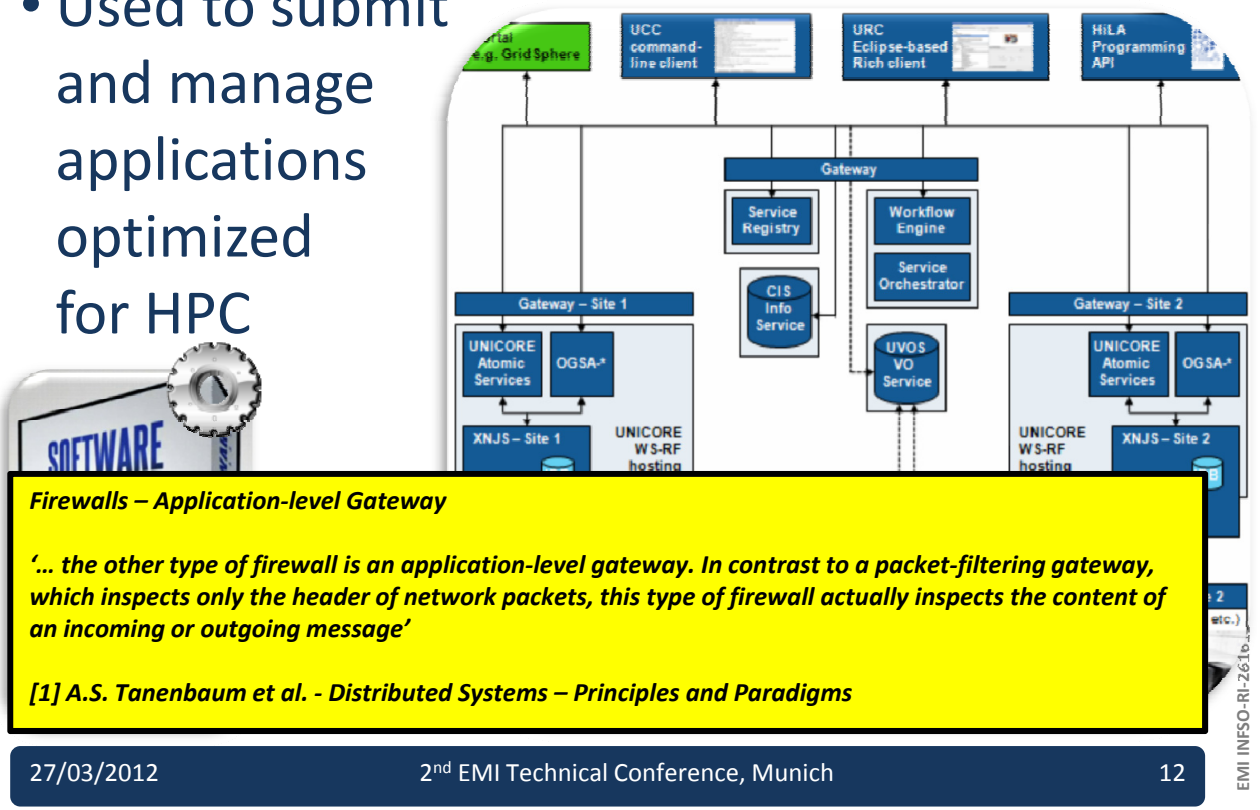
[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

CREAM CE Features

- Use the CREAM CE as a powerful system to execute applications across geographically distributed computing services and their underlying resources
- Take advantage of a client/server architecture that implements the functionality of a Computing Element (CE) accessing a wide variety of available batch systems
- Interoperate with other EMI services by using the EMI Execution Service via a SOAP-based Web service Interface
- A C++ based Command Line Interface (CLI) is available and other clients can be easily created
- CREAM provides hooks for accounting and offers data-staging functionality

UNICORE Added Value

- Used to submit and manage applications optimized for HPC



Firewalls – Application-level Gateway

'… the other type of firewall is an application-level gateway. In contrast to a packet-filtering gateway, which inspects only the header of network packets, this type of firewall actually inspects the content of an incoming or outgoing message'

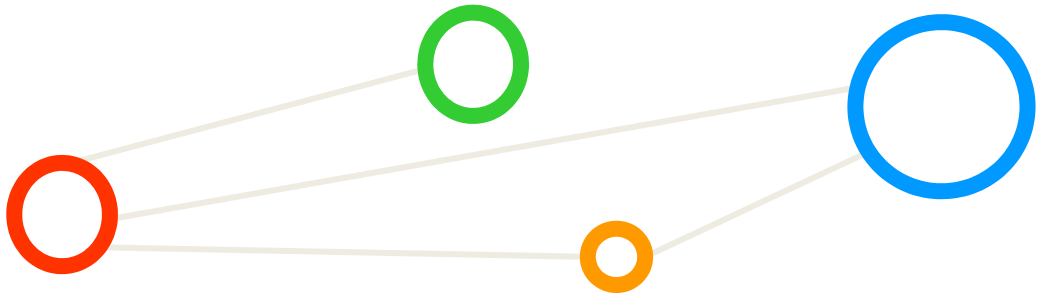
[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

UNICORE Features

- Use the UNICORE system as a powerful system to execute applications across geographically distributed computing services and their underlying resources
- Take advantage of a three-tier architecture that implements the functionality of a Computing Element (CE) accessing a wide variety (~13) of available batch systems
- Benefit from the maturity and reliability of accessing medium and large-scale HPC resources with key characteristics since ~15 years
- Deploy a solution that is specifically optimized for sensitive security environments that have less impact on site security policies

EMI INFSO-RI-261611

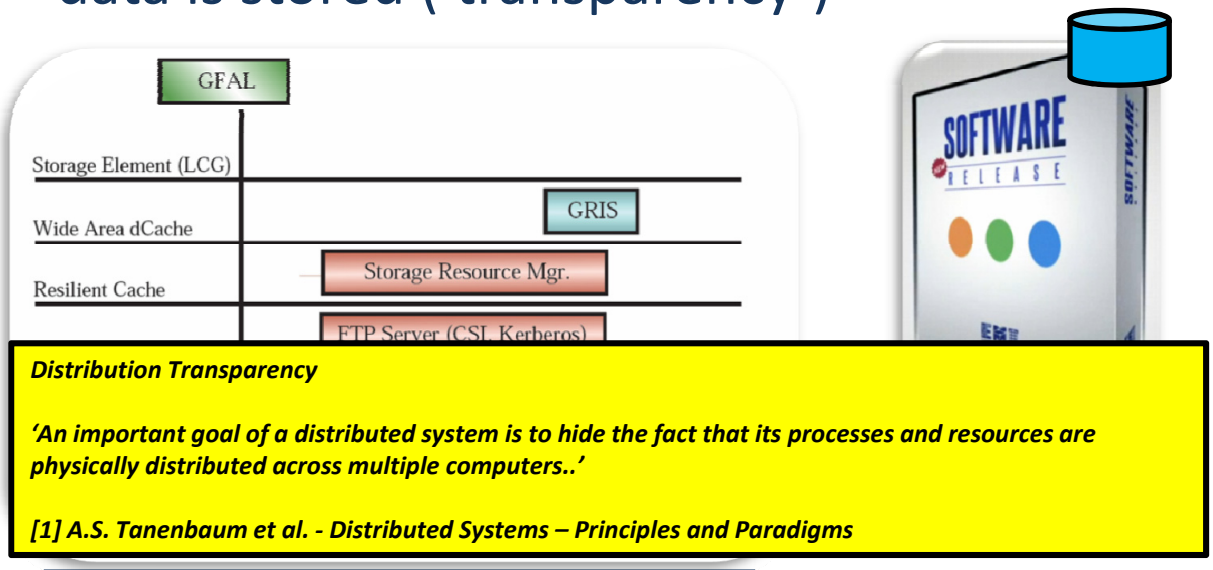
Data in Distributed Systems



EMI INFSO-RI-261611

dCache Added Value

- Used to store data in a distributed fashion without end-users being aware where their data is stored ('transparency')



Distribution Transparency

'An important goal of a distributed system is to hide the fact that its processes and resources are physically distributed across multiple computers..'

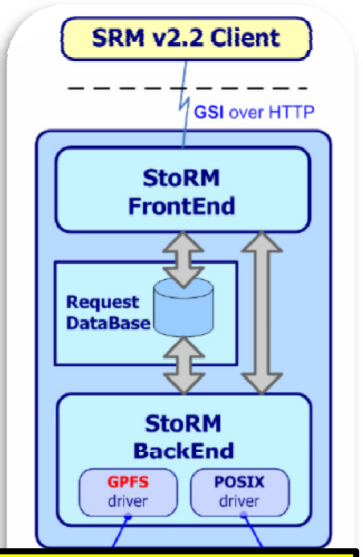
[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

dCache Features

- Use the dCache SE as a service in order to transparently provide access to disk-based
- Storage systems as well as tertiary storage (e.g. tapes) known for better cost-efficiency
- Take advantage of a strong client/server architecture that implements the functionality of a Storage Element (SE) offering a variety of access protocols (e.g. POSIX, etc.)
- Migrate data from one resource to another without affecting end-users
- Interoperate with other EMI storage services by using the Storage Resource Manager (SRM) 2.2 standard as Web service Interface or the HTTP-based WebDAV standard

StoRM Added Value

- Used to store data and information in different underlying disk-based storage systems
  - One standard interface: SRM



Open Distributed System

'An open distributed system is a system that offers services according to standard rules that describe the syntax and semantics of those services…'

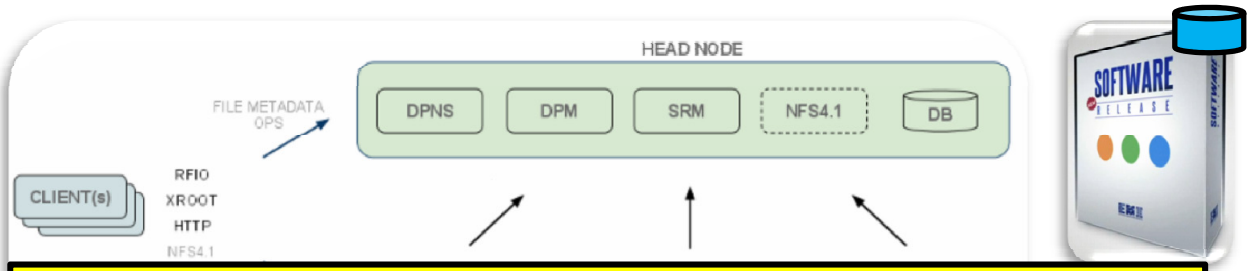
[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

StoRM Features

- Use the StoRM SE as a service that is specifically optimized for (parallel) disk-based storage systems such as the General Parallel File System (GPFS) or Lustre
- Take advantage of a strong client/server architecture that implements the functionality of a Storage Element (SE) offering a variety of access protocols (e.g. POSIX, etc.)
- Provide a stable storage interface with StoRM to end-users while the underlying file system and/or storage system might change over time
- Interoperate with other EMI storage services by using the Storage Resource Manager Open Grid Forum (SRM) 2.2 standard as Web service Interface
- The modular architecture decouples StoRM from the different underlying file systems

DPM Added Value

- Lightweight storage solution for DCI sites offering a simple way to create disk-based Grid storage elements and their management



Protocols

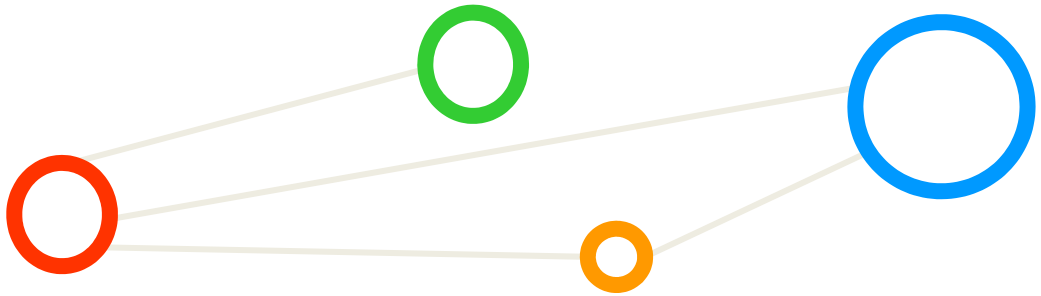
'The collection of protocols used in a particular system is called a protocol suite or protocol stack…'

[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

DPM Features

- Use the DPM SE as a lightweight service in order to transparently provide access to disk-based storage systems
- Install a client/server architecture that support many protocols for file access such as Remote File Input/Output (RFIO), XROOT, HTTP, GridFTP, and NSF4.1
- Interoperate with other EMI storage services by using the Storage Resource Manager (SRM) 2.2 standard
- Take advantage of a system focuses on manageability such as ease of installation and configuration as well as low effort of maintenance
- Leverage all the required functionality for your grid storage solution including support for multiple disk server nodes, different space types or multiple file replicas in disk pools

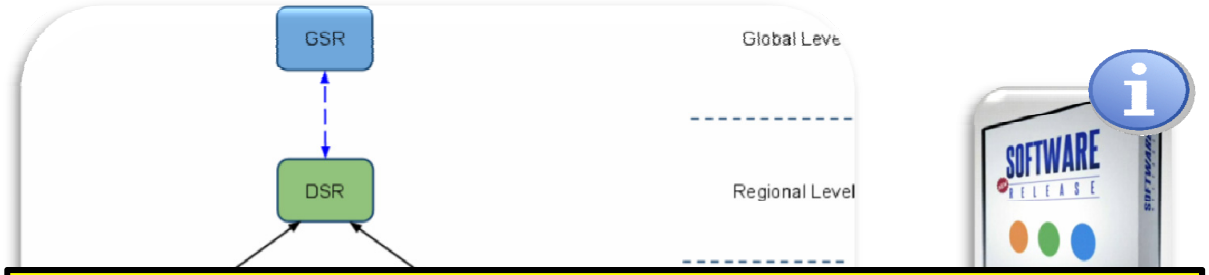
Distributed Systems Information



EMI INFSO-RI-261611

EMIR Added Value

- Provide high robustness, scalability and performance registry using a federated model (with no centralized, single entry point)



Scalability

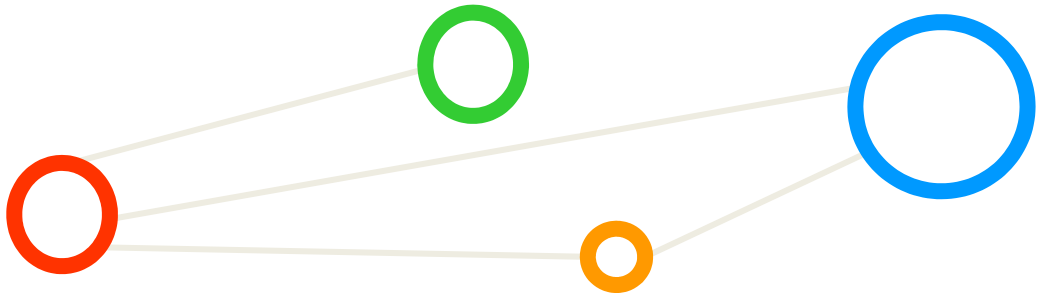
'… scalability is one of the most important design goals for developers of distributed systems…if more users or resources need to be supported, we are often confronted with the limitations of centralized services, data, and algorithms…'

[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

EMIR Features

- Use EMIR ReSTful interface to register and query the services
- Employ flexible, standardized and expressive information model to represent the services (GLUE2 information model)
- Setup authorization and access control with XACML policies or ACLs
- Write easy your own clients to interact with the service (WADL available)

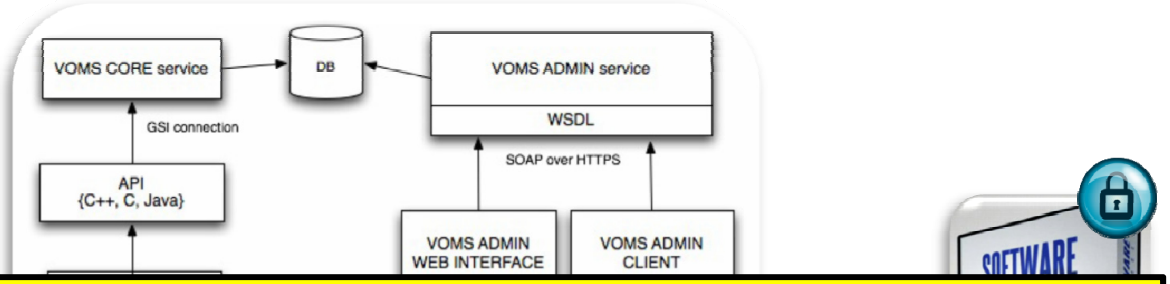
Distributed Systems Security



EMI INFSO-RI-261611

VOMS Added Value

- Attribute Authority (AA) releasing signed security credentials with information beyond pure identities (roles, groups, project, etc.)



Protection Domains - Authorization based on groups and roles of users

'One approach is to construct groups of users…related to having groups as protection domains, is also possible to implement protection domains as roles'

[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

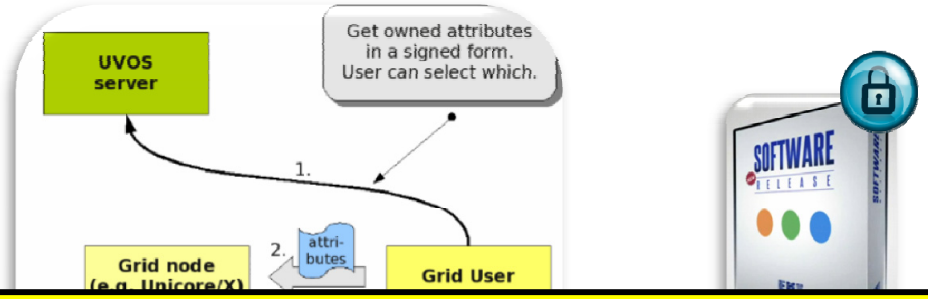
VOMS Features

- Use VOMS as an AA server to obtain signed security credentials with attributes of end-users (e.g. role possession, group/project membership) used during authorization
- Take advantage of a client/server architecture that is able to store identities and manage them in hierarchical groups
- Access and easily configure VOMS using its complementary voms-admin tool
- Interoperate by using the Security Assertion Markup Language (SAML) 2.0 standard via SOAP-based Web service interfaces or X.509 Attribute Certificates
- Engage in being among the first users that take advantage of the new Representational State Transfer (REST) VOMS interface

EMI INFSO-RI-261611

UVOS Added Value

- Attribute Authority (AA) releasing signed security credentials with information beyond pure identities (roles, groups, project, etc.)



Protection Domains - Authorization based on groups and roles of users

'One approach is to construct groups of users…related to having groups as protection domains, is also possible to implement protection domains as roles'

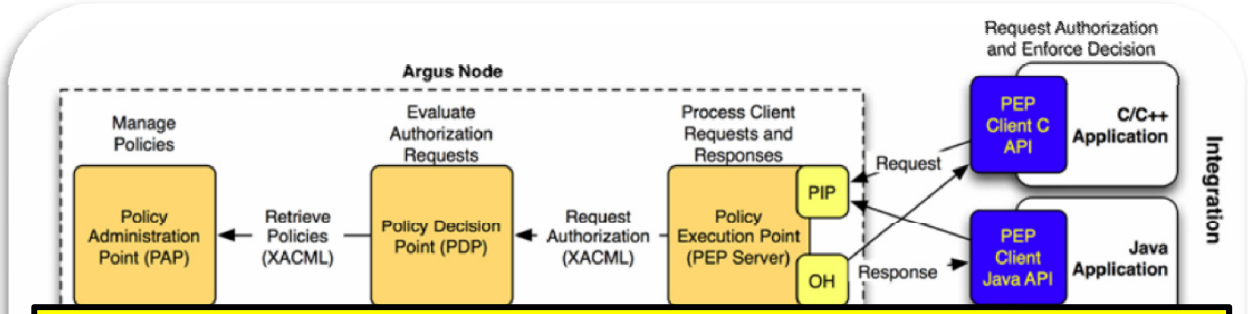
[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

UVOS Features

- Use UVOS as an AA server to obtain signed security credentials with attributes of end-users (e.g. role possession, group/project membership) used during authorization
- Take advantage of a client/server architecture that is able store identities and other identifiable servers and organize them in hierarchical groups if needed
- Access and configure UVOS using its client and a lightweight VO authentication Web component optimized for a usage within browsers
- Interoperate with other services by using the Security Assertion Markup Language (SAML) 2.0 standard via SOAP-based Web service interfaces

ARGUS Added Value

- Used to derive authorization decisions



Protection Domains - Authorization based on groups and roles of users

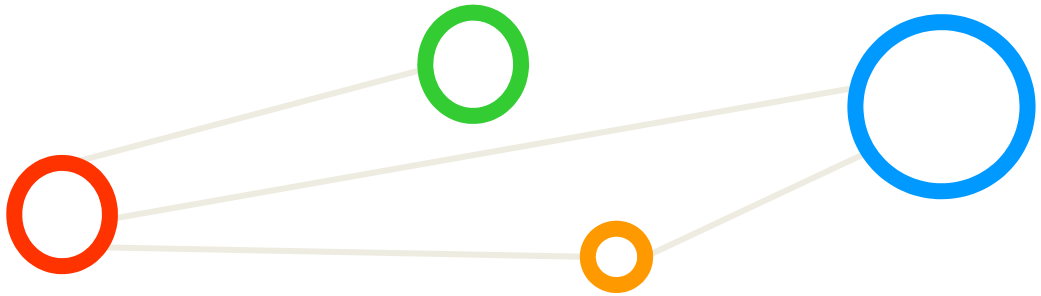
'One approach is to construct groups of users…related to having groups as protection domains, is also possible to implement protection domains as roles'

[1] A.S. Tanenbaum et al. - Distributed Systems – Principles and Paradigms

ARGUS Features

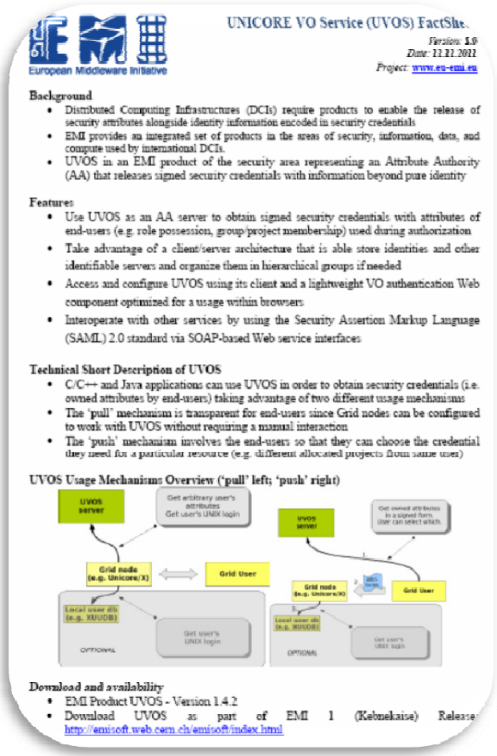
- Use ARGUS as a system to render consistent authorization decisions across geographically distributed services (computing, data, portals, etc.)
- Take advantage of a client/server architecture that implements the functionality of a Policy Enforcement Point (PEP)
- Manage policies through a Policy Administration Point (PAP) and its admin tool
- Interoperate with other services by using the Extensible Access Control Markup Language (XACML) standard via a SOAP-based Web service Interface

More Information



EMI INFSO-RI-261611

More Products are available!



UNICORE VO Service (UVOS) FactSht.

Version: 1.0
Date: 12.12.2011
Project: www.eu-emi.eu

Background

- Distributed Computing Infrastructures (DCIs) require products to enable the release of security attributes alongside identity information encoded in security credentials
- EMI provides an integrated set of products in the areas of security, information, data, and compute used by international DCIs.
- UVOS is an EMI product of the security area representing an Attribute Authority (AA) that releases signed security credentials with information beyond pure identity

Features

- Use UVOS as an AA server to obtain signed security credentials with attributes of end-users (e.g. role possession, group/project membership) used during authorization
- Take advantage of a client/server architecture that is able store identities and other identifiable servers and organize them in hierarchical groups if needed
- Access and configure UVOS using its client and a lightweight VO authentication Web component optimized for a usage within browsers
- Interoperate with other services by using the Security Assertion Markup Language (SAML) 2.0 standard via SOAP-based Web service interfaces

Technical Short Description of UVOS

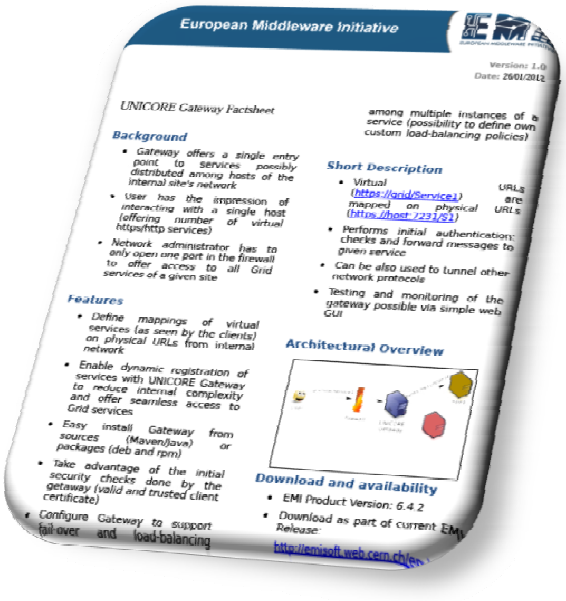
- C/C++ and Java applications can use UVOS in order to obtain security credentials (i.e. owned attributes by end-users) taking advantage of two different usage mechanisms
- The 'pull' mechanism is transparent for end-users since Grid nodes can be configured to work with UVOS without requiring a manual interaction
- The 'push' mechanism involves the end-users so that they can choose the credential they need for a particular resource (e.g. different allocated projects from same user)

UVOS Usage Mechanisms Overview ('pull' left; 'push' right)

Download and availability

- EMI Product UVOS - Version 1.4.2
- Download UVOS as part of EMI 1 (Kebnekaise) Release

http://emisoft.web.cern.ch/emisoft/index.html



European Middleware Initiative

Version: 1.0
Date: 26/01/2012

UNICORE Gateway Factsheet

among multiple instances of a service (possibility to define own custom load-balancing policies)

Background

- Gateway offers a single entry point to services possibly distributed among hosts of the internal site's network
- User has the impression of interacting with a single host (offering number of virtual https/http services)
- Network administrator has to only open one port in the firewall to offer access to all Grid services of a given site

Short Description

- Virtual URLs (https://grid/Service1) are mapped on physical URLs (https://host:7233/S1)
- Performs initial authentication; checks and forward messages to given service
- Can be also used to tunnel other network protocols
- Testing and monitoring of the gateway possible via simple web GUI

Features

- Define mappings of virtual services (as seen by the clients) on physical URLs from internal network
- Enable dynamic registration of services with UNICORE Gateway to reduce internal complexity and offer seamless access to Grid services
- Easy install Gateway from sources (Maven/Java) or packages (deb and rpm)
- Take advantage of the initial security checks done by the gateway (valid and trusted client certificate)
- Configure Gateway to support fail-over and load-balancing

Architectural Overview

Download and availability

- EMI Product Version: 6.4.2
- Download as part of current EMI Release

https://emisoft.web.cern.ch/(en

Future: Science Soft Activities

- Collaborate in a more open & flexible way
- Enhance ‘users choice’ via standard adoptions
- Join sustainability plans based on several pillars in Grid community
- Find new partners…

EMI INFSO-RI-261611

EMI References

- EMI Website
  http://www.eu-emi.eu/
- ‘ScienceSoft’ Web site (concept phase)
  http://www.sciencesoft.org

EMI INFSO-RI-261611

General References

[1] A.S. Tanenbaum et al. - Distributed Systems Principles and Paradigms, ISBN 013-613553-6

[2] EMI Product FactSheets
http://www.eu-emi.eu/product-factsheets

[3] Digital Agenda for Europe
http://ec.europa.eu/information_society/digital-agenda/index_en.htm