EGI-InSPIRE

UMD Quality Criteria
v4 DRAFT 2

Document identifier:	EGI-ALL-QC-V4.doc
Date:	**30/07/2012**
Document Link:	https://documents.egi.eu/document/1153

Abstract

This document describes the Quality Criteria that all software of the UMD distribution must meet.



Document Log

Issue	Date	Comment	Author/Partner
v0.1	02/11/2010	First draft	Enol Fernández
v1.0	03/11/2010	Changed Management, Traceability and Monitoring section	Enol Fernández
v1.1	03/11/2010	Added Probe description in GEN_MON_1	Enol Fernández
v1.2	11/11/2010	Some formatting update	Enol Fernández
v1.3	31/01/2011	Better test specification	Enol Fernández
1.4	09/02/2011	Review of criteria	Enol Fernández
2 DRAFT 1	24/06/2011	Preparation of new release	Enol Fernández
2	02/08/2011	Reorganisation, added new criteria.	Enol Fernández
3 DRAFT 1	13/10/2011	First draft of release 3	Enol Fernández
3 DRAFT 2	24/01/2012	Second draft of release 3	Enol Fernández
4 DRAFT 1	21/05/2012	First public draft of release 4	Enol Fernández
4 DRAFT 2	23/07/2012	Second public draft of release 4	Enol Fernández

TABLE OF CONTENTS

1 CRITERIA TEMPLATE

Criterion Name	
ID	**GENERIC_TEMPLATE**
Description	Provide a description of the criterion captured in this template.
Mandatory	YES/NO
Applicability	Specify which appliances/products must meet this criterion.

Input from Technology Provider	Describe here what is expected from the TP to fulfil the criterion	
Test Description	**Pre-condition**	Describe here the preconditions of the test
	Test	Describe in this field what the actions should the test perform
	Expected Outcome	Describe the expected outcome of the test execution, including any outputs.
Pass/Fail Criteria	Criteria that will determine whether if passes or not verification.	
Related Information	Resources found elsewhere (e.g. web pages, Wiki entries, publications and papers) which help to describe the requirement in further detail.	
Revision Log	Give the history of the changes in the criterion.	

2 DOCUMENTATION

Services in UMD must include a comprehensive documentation written in a uniform and clear style. All Quality Criteria described below may be met by a single document that contains all the requested sections.

Functional Description	
ID	**GENERIC_DOC_1**
Description	All products must provide a document with a brief functional description of the product.
Mandatory	NO
Applicability	All products

Input from Technology Provider	Document (or link) with a general description of the product that includes: • Purpose of the product • Capabilities meet by the product
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	V2: clarified the required documentation

Release Notes	
ID	**GENERIC_DOC_2**
Description	All products must provide a document with the release notes.
Mandatory	YES
Applicability	All products

Input from Technology Provider	Document (or link) with release notes of the product. They must include major the changes in the product: bug fixes, new features.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

User Documentation	
ID	**GENERIC_DOC_3**
Description	All products must provide a document describing how to use it.
Mandatory	NO
Applicability	All products with end-user tools and services.

Input from Technology Provider	Document (or link) with user guide describing the functionality of the software and how to use it.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

Online help (man pages)	
ID	**GENERIC_DOC_4**
Description	All products with end user command line tools must include man pages or online help.
Mandatory	NO
Applicability	All products with command line tools.

Input from Technology Provider	Man pages with information about the usage of commands. If man pages are not available, comprehensive help options must be included with the command with information about the usage (i.e. –h/--help option)
Pass/Fail Criteria	Online help should be available (man pages or command line help). Command line help should give meaningful cues (i.e., only a list of single-letter options is not sufficient) If both command line help (-h option) and man pages are provided they **must** be mutually consistent (describe the same set of options and their meaning).
Related Information	GGUS ticket # 73214
Revision Log	V3: Tighten wording to avoid situations as described in GGUS #73214

API Documentation	
ID	**GENERIC_DOC_5**
Description	Public API of product/appliances must be documented.
Mandatory	NO
Applicability	All products with public API.

Input from Technology Provider	Documentation (or link) of the API of the product. The documentation *should* cover all the existing public functionality of the API.
Pass/Fail Criteria	The document should exist and contain the API documentation. If the product implements a well-known or standard API, any missing functionality must be documented.
Related Information	
Revision Log	V2: review of the description

Administrator Documentation	
ID	**GENERIC_DOC_6**
Description	Products must provide an administrator guide describing installation, configuration and operation of the system.
Mandatory	NO
Applicability	All products managed by an administrator.

Input from Technology Provider	Documentation (or link) with requested documentation.
Pass/Fail Criteria	The document should exist and contain the requested information.
Related Information	
Revision Log	

<table>
<tr><th colspan="2">Service Reference Card</th></tr>
<tr><td>ID</td><td>GENERIC_DOC_7</td></tr>
<tr><td>Description</td><td>For each of the services that a product runs, document its characteristics with a reference card.</td></tr>
<tr><td>Mandatory</td><td>NO</td></tr>
<tr><td>Applicability</td><td>All products that need services for operation.</td></tr>
</table>

<table>
<tr><td>Input from Technology Provider</td><td>Documentation (or link) with requested documentation.</td></tr>
<tr><td>Pass/Fail Criteria</td><td>The document must exist and contain the following information for each service:
<table>
<tr><th colspan="2">ServiceName</th></tr>
<tr><td>Description</td><td>Description of the service</td></tr>
<tr><td>Init scripts</td><td>List of init scripts for the service, expected run levels</td></tr>
<tr><td>Daemons</td><td>List of daemons needed for the service</td></tr>
<tr><td>Configuration</td><td>List of configuration files used by the service</td></tr>
<tr><td>Logs</td><td>List of log files used by the service</td></tr>
<tr><td>Open ports</td><td>List of ports the service uses</td></tr>
<tr><td>Cron</td><td>List of crons used by the service</td></tr>
<tr><td>Other information</td><td>Any other relevant information about the service.</td></tr>
</table></td></tr>
<tr><td>Related Information</td><td></td></tr>
<tr><td>Revision Log</td><td></td></tr>
</table>

Software License	
ID	**GENERIC_DOC_8**
Description	Products must have a compatible license for using them in the EGI Infrastructure
Mandatory	YES
Applicability	All products.

Input from Technology Provider	Product License (link or document).
Pass/Fail Criteria	Pass: if the license is available and is compatible with the EGI infrastructure. For Open Source products, compatible licenses are those accepted by the Open Source Initiative and categorized as "Popular and widely used or with strong communities": - Apache License, 2.0 (Apache-2.0) - BSD 3-Clause "New" or "Revised" license (BSD-3-Clause) - BSD 3-Clause "Simplified" or "FreeBSD" license (BSD-2-Clause) - GNU General Public License (GPL) - GNU Library or "Lesser" General Public License (LGPL) - MIT license (MIT) - Mozilla Public License 1.1 (MPL-1.1) - Common Development and Distribution License (CDDL-1.0) - Eclipse Public License (EPL-1.0) Other licenses accepted by the Open Source Initiative and listed as "Special Purpose" are compatible with the infrastructure (when applicable): - Educational Community License - IPA Font License (IPA) - NASA Open Source Agreement 1.3 (NASA-1.3) - Open Font License 1.1 (OFL-1.1) Any other license, and non Open Source products will be evaluated by the verification team in coordination with the Operations Community.
Related Information	Open Source Initiative Licenses by Category: http://www.opensource.org/licenses/category
Revision Log	V2: Moved from Software Release to documentation.

Release changes testing	
ID	**GENERIC_DOC_9**
Description	Changes in a release of a product must be tested.
Mandatory	NO
Applicability	All Products.

Input from Technology Provider	Tests (or documentation for the test results) for relevant changes described in the product release notes, including bug fixes and any new features.
Pass/Fail Criteria	Pass if the TP provides documentation of the tests performed to certify the release quality. The documentation *should* describe tests (and tests results) for all the changes included, especially bug fixes. The granularity of the testing documentation will be determined per release basis. In the case of missing tests, the verifier will decide if the provided information is enough to trust quality of the changes introduced in the software.
Related Information	MS503: Software Provisioning Process
Revision Log	V2: Better specification of the pass/fail criteria. Moved to documentation criteria V3: improvement of the pass/fail criteria. V4: better wording after IGE review, turned into NOT mandatory.

Database Schema Documentation	
ID	**GENERIC_DOC_10**
Description	Database schemas changes must be documented.
Mandatory	YES
Applicability	All Products that make use of a database backends.

Input from Technology Provider	Documentation (or link) with description of the database schema used by the product. If there are schema changes between releases (minor or major upgradeable from previous major), also include documentation of those changes and scripts for migration to the new schema.
Pass/Fail Criteria	Pass if any database schema changes are documented and a migration path is provided via a script or with detailed instructions. The database schema documentation should be also available.
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

Policy changes	
ID	**GENERIC_DOC_11**
Description	Documentation of changes that may affect underlying policies.
Mandatory	YES
Applicability	All Products that implement EGI policies

Input from Technology Provider	Documentation (or link) of any changes introduced in the product that may affect any underlying policies (e.g. procedure for VOMS membership renewal) implemented by the service.
Pass/Fail Criteria	If a new release of a product introduces changes in its configuration options, management interfaces or any other feature that affects the implementation of underlying policies, those changes and their effects **must** be documented.
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

3 SOFTWARE DISTRIBUTION

Source Code Availability	
ID	**GENERIC_DIST_1**
Description	Open Source Products should provide their source code.
Mandatory	NO
Applicability	All Open Source Products.

Input from Technology Provider	Source code repository or source distribution of product with building documentation.
Pass/Fail Criteria	Open source products **must** publicly offer their source code and the license with the binaries. Build documentation (or link to it) should be available. Ideally, automatic or continuous build procedures exist.
Related Information	
Revision Log	V2: Changed ID (previously GENERIC_REL_2) V4: Merged GENERIC_DIST_1 and GENERIC_DIST_2 & Turned into not mandatory

Binary Distribution	
ID	**GENERIC_DIST_3**
Description	Products must be available in the native packaging format of the supported platform.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Binary distribution of product in the native packaging format of the supported platform (RPM, DEB, …)
Pass/Fail Criteria	- Binary packages using the standard packaging format of the OS (i.e. RPM, DEB...) must be provided for all the supported OS and/or architectures. - Packages **must** be signed by the TP - Packages *should* follow OS packaging policies (e.g. names of packages, use of filesystem hierarchy, init scripts). Any deviance from the policies must be documented. - Second level dependencies (i.e. software not provided by the TP in their repository) **must** be provided by the OS distribution or standard OS repositories (EPEL in SL5 & SL6). In the case of needing a different version for a specific package or packages from other repositories, the verifier will decide whether to accept or not the packages depending on the reason given for such dependencies on external packages.
Related Information	Verification reports from EMI release 1. #1357: Middleware use standard file locations GGUS #82417: https://ggus.eu/ws/ticket_info.php?ticket=82417
Revision Log	V2: Turn to mandatory, better description to avoid problems found in verification. Changed ID (previously GENERIC_REL_5) V4: Added requirement for signed packages.

4 SOFTWARE FEATURES

Backwards Compatibility	
ID	**GENERIC_SOFT_1**
Description	Minor/Revision releases of a product must be backwards compatible.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Products must maintain backwards compatibility between releases of the same major version. Ideally, TP provides tests to assure the backwards compatibility of the product.
Pass/Fail Criteria	All the changes in a minor or revision release *must* be backward compatible (test should be done with previous releases of clients within the same major version). Any new features should not introduce changes in the previous features.
Related Information	MS503: Software Provisioning Process IGE QC
Revision Log	

New features testing	
ID	**GENERIC_SOFT_2**
Description	Verification should cover testing of new features and bug fixes.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Release notes with changes in the software. The verifier will review each of the changes and check its correctness (whenever possible)
Pass/Fail Criteria	New features and bug fixes specified in the release notes work as documented. Some new features may not be tested if they are not relevant to the main capability of the product.
Related Information	MS503: Software Provisioning Process IGE QC
Revision Log	

5 SERVICE CRITERIA

5.1 Service Management

UMD products should have mechanisms for managing them, monitoring their status and tracing actions they perform on the system. Ideally, these should be also available remotely, allowing operators to react timely to problems in the infrastructure. This generic criteria for services is the minimum set of service related

Service control and status	
ID	**GENERIC_SERVICE_1**
Description	Services run by the product must provide a mechanism for starting, stopping and querying the status of the services.
Mandatory	YES
Applicability	All products that use services for operations.

Input from Technology Provider	Start/stop mechanism for each of the services following OS conventions. Ideally, provide a test suite for the mechanism as described below.	
Test Description	**Pre-condition**	Service is started
	Test	Start service
	Expected Outcome	No action taken, show a message stating the service is already started.
	Pre-condition	Service is stopped
	Test	Start service
	Expected Outcome	Service is started, show a message when it is started.
	Pre-condition	Service is started
	Test	Stop service
	Expected Outcome	Service is stopped, show a message stating the service is stopped.
	Pre-condition	Service is stopped
	Test	Stop service
	Expected Outcome	No action taken, show a message stating the service is already stopped.
	Pre-condition	Service is stopped
	Test	Check service status
	Expected Outcome	Show a message stating the service is stopped.

Test Description	**Pre-condition**	Service is started
	Test	Check service status
	Expected Outcome	Show a message stating the service is started.
Pass/Fail Criteria	Services run by the product must provide a mechanism for starting, stopping and querying the status of the services following the OS init scripts conventions (e.g. for Linux Distributions, check http://refspecs.freestandards.org/LSB_3.1.0/LSB-Core-generic/LSB-Core-generic/iniscrptact.html). They must work properly in **all** the cases described above. If the OS provides tools for configuring the services (chkconfig in RH based distros), these *should* work out of the box with the init scripts of the services	
Related Information	#2274: Service under RH following SystemV init system #1201: Homogeneity in service control.	
Revision Log	V3: Added related information, fix test conditions.	

5.2 Service logs

Log Files	
ID	**GENERIC_SERVICE_2**
Description	All services should create log files where the service administrator can trace most relevant actions taken.
Mandatory	YES
Applicability	All products that use services for operations.

Input from Technology Provider	List of logs generated by the service (the reference card of service should already include them)
Pass/Fail Criteria	List of logs is provided. They should follow the OS conventions for location and format so they can be treated with the standard tools of the OS (log rotation, collection with syslog, …)
Related Information	This criterion may be further specialized in the specific criteria for each product/capability determining which information must be logged or number/types of logs. #1357: Middleware use standard file locations
Revision Log	V2. Review of the criteria. V4: Added related information

5.3 Service Monitoring

All services in the EGI Infrastructure should provide monitoring probes that can be executed automatically by the EGI monitoring framework (based in Nagios). The probes should check the service responsiveness and correctness (good replies for typical requests).

Particular monitoring probes are defined at the Specific Quality Criteria document for Operations tools The probes that apply to all capabilities (generic probes) are identified as MON_PROBE_GENERIC_*xx*. For specific capabilities there might exist other probes that are described in the same document.

5.4 Service Accounting

All services in the EGI Infrastructure should provide ways of recording the use of resources within the infrastructure. The Accounting Capability described in the Operations Capabilities Criteria document specifies the criteria for the different appliances.

5.5 Availability, Reliability and Scalability.

The EGI Infrastructure depends on the uninterrupted performance of the installed software. All products should provide a reliable operation and should be able to handle growing amounts of work in a graceful manner. Specific criteria for the availability, reliability or scalability of appliances may be also defined in the criteria documents for each of the capabilities.

Service Reliability	
ID	**GENERIC_SERVICE_3**
Description	Services must maintain a good performance and reliability over long periods of time with normal operation.
Mandatory	NO
Applicability	All products that use services for operations.

Input from Technology Provider	Long running unattended operation test measuring performance of the product.	
Test Description	**Pre-condition**	Product is properly configured.
	Test	Start service and measure performance during operations.
	Expected Outcome	No significant performance degradation is observed in the system.
Pass/Fail Criteria	Service must not show performance degradation during a 3-day period. The most important parameters to check are: • stable memory usage • throughput and/or response times remain stable during the period of activity (they should be as good or better than at the beginning of the test for similar requests)	
Related Information		
Revision Log	V2: detailed pass/fail criteria	

Service Robustness	
ID	**GENERIC_SERVICE_4**
Description	Services should not produce unexpected results or become uncontrollable when taxed beyond normal capacity.
Mandatory	NO
Applicability	All products that use services for operations.

Input from Technology Provider	Assure that the services taxed beyond normal capacity do not produce unexpected results or become uncontrollable.
Pass/Fail Criteria	Services taxed beyond normal capacity: • should not become unresponsive to normal start/stop operations • must be able to start after a forceful stop • must not expose (potentially sensitive) memory contents to other processes • must not leave sensitive data in world-readable files • must not accept connections that would be refused under normal operating conditions
Related Information	TST_2 from IGE Quality Assurance.
Revision Log	

5.6 Service Configuration

Automatic Configuration	
ID	**GENERIC_SERVICE_5**
Description	Products that provide tools for configuration (yaim) that covers typical deployments must assure tools work as documented.
Mandatory	NO
Applicability	Products with automatic configuration tools

Input from Technology Provider	Tests of the automatic configuration tool (yaim) in typical deployment scenario.
Pass/Fail Criteria	Pass if the product can be configured as documented with the provided tool. Resulting configuration must prepare the product for operation without extra manual configuration steps (unless clearly documented).
Related Information	Yaim: https://twiki.cern.ch/twiki/bin/view/EGEE/YAIM UMD 1.0.0 Verification Reports.
Revision Log	V3: Removed the requirement for keeping manual configurations.

Default Password Configuration	
ID	**GENERIC_SERVICE_6**
Description	Products should not use default passwords. If the service needs a password, it must be generated randomly or force the admin to introduce one.
Mandatory	YES
Applicability	All products with passwords.

Input from Technology Provider	Configuration should never have default passwords. If there is an automated configuration generator (e.g. yaim) it must request the user to set one or generate a random one.
Pass/Fail Criteria	No default passwords are used for configuration of services.
Related Information	SVG Advisory 1414: https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414
Revision Log	

Default Configuration	
ID	**GENERIC_SERVICE_7**
Description	Default configuration of the service should be *usable*.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Documentation on the default values of any optional configuration parameters. Default values for those values reasonable for the normal operation of the service in a standard installation.
Pass/Fail Criteria	Pass if the documentation of the default values of the optional configuration parameters is available and the service runs with those default values (in a standard installation).
Related Information	VOMS mass user suspension (RT #3585)
Revision Log	

6 SECURITY

World Writable Files	
ID	**GENERIC_SEC_1**
Description	Products must not create world-writable files or directories.
Mandatory	YES
Applicability	All products.

Input from Technology Provider	World-writable files and directories are dangerous since they allows anyone to modify them, several vulnerabilities in recent years have been due to world writable files and directories being present when they should not be. Technology Provider must assure that they software do not produce world writable files in order to prevent new vulnerabilities being introduced in the future. Ideally a test that checks that those files do not exist should be provided.	
Test Description	**Pre-condition**	Service correctly configured and started
	Test	Check the existence of world writable or unowned files in the system.
	Expected Outcome	No world writable or unowned files exist.
Pass/Fail Criteria	The product should not create world-writable files or directories. If any world-writable files are needed for the normal operation of the service, these should be documented. Logs and config files **must** not be world-writable.	
Related Information	Proposed by the EGI SVG RAT to prevent new vulnerabilities in the future.	
Revision Log	V1.3 Changed test description. V4: improved pass/fail criteria.	

Directory Traversal Attacks testing	
ID	**GENERIC_SEC_2**
Description	Products should assure that directory traversal exploits are not possible using their interfaces. Special care must be taken to products exposing part of the file system (e.g. file access capabilities) and web services.
Mandatory	YES
Applicability	All products with previous known Directory Traversal exploits (See list at related information), any other product *should* also include this kind of testing.

Input from Technology Provider	A directory traversal (or path traversal) consists in exploiting insufficient security validation/sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The Technology Provider should test that directory traversal attacks are not possible using the product interface. Products that need to run as root user, must have special care in this case of attacks, since they may give access to whole file system.	
Test Description	**Pre-condition**	Service correctly configured and started
	Test	Try to exploit directory traversal in product
	Expected Outcome	No directory traversal succeeds.
Pass/Fail Criteria	Test for directory traversal exploiting do not successfully access the file system.	
Related Information	Advisory-SVG-2011-1569 (https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1569)	
Revision Log		

Passwords in world readable files	
ID	**GENERIC_SEC_3**
Description	Service password must not be stored in world readable files.
Mandatory	YES
Applicability	All products with passwords.

Input from Technology Provider	If the product uses passwords stored in files, those files must not be world readable.
Pass/Fail Criteria	No passwords are stored in world readable files.
Related Information	SVG Advisory 1414: https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1414
Revision Log	

7 MISCELLANEOUS

Bug Tracking System	
ID	**GENERIC_MISC_1**
Description	TP must enrol as 3rd level support in the EGI Helpdesk.
Mandatory	YES
Applicability	All Products.

Input from Technology Provider	Technology Providers must enrol in GGUS as 3rd level support for the products verified by the Quality Assurance team of EGI. Any further integration with TP-specific bug tracking software is entirely up to the Technology Provider.
Pass/Fail Criteria	Pass if Technology Provider enlisted as 3rd level support in GGUS.
Related Information	IGE QC
Revision Log	

8 AUTHENTICATION

An authentication token that is strongly bound to an individual must be applied consistently across the software used within the production infrastructure. The authentication system should be capable of supporting a delegation model.

8.1 Authentication Credentials

X.509 Certificate support	
ID	**AUTHN_CRED_1**
Description	Primary authentication token within the infrastructure is the X.509 certificate and its proxy derivatives.
Mandatory	YES
Applicability	Authentication Appliances.

Input from Technology Provider	Support for X.509 certificate (and proxy derivatives) as credential token for authentication.
Pass/Fail Criteria	Pass if the appliance is able to use X.509 certificates as authentication token. The appliance *should* also support proxy derivatives.
Related Information	UMD Roadmap [R 1]
Revision Log	

SHA-2 Certificate support	
ID	**AUTHN_CRED_2**
Description	SHA-2 certificates should be accepted by middleware.
Mandatory	NO
Applicability	Authentication Appliances.

Input from Technology Provider	Support for certificates and proxies with SHA-2 cryptographic hash functions.
Pass/Fail Criteria	Pass if the appliance is able to use SHA-2 certificates as authentication token. Information on how to get and test with SHA-2 certificates is available at [R 2]
Related Information	UMD Roadmap [R 1] Support for SHA2 proxies RT #3078
Revision Log	

RFC Proxy support	
ID	**AUTHN_CRED_3**
Description	RFC proxies should be accepted by middleware.
Mandatory	NO
Applicability	Authentication Appliances that

Input from Technology Provider	Support for RFC proxies as credential tokens for authentication.
Pass/Fail Criteria	Pass if the appliance is able to use RFC proxies as authentication token. Information on how to create RFC proxies is available at [R 2]
Related Information	UMD Roadmap [R 1]
Revision Log	

8.2 Authentication Protocols

TLS/SSLv3 Support	
ID	**AUTHN_PROTO_1**
Description	TLS/SSLv3/v2 with client-side authentication must be supported.
Mandatory	YES
Applicability	Authentication Appliances.

Input from Technology Provider	Support for accessing resources through protocols that are secured using SSL or TLS (e.g. plain socket, or https connections). If the component exposes a WebService that requires authentication, it should use the X.509 certificates/proxies with the https protocol.
Pass/Fail Criteria	Pass if the product uses SSL or TLS for accessing it. For the current releases of UMD, products still using GSI authentication (with httpg for WebServices) may be accepted, this exception may be dropped in future releases of the criterion.
Related Information	UMD Roadmap [R 1]
Revision Log	V2: Added GSI (httpg) exception for products that have not yet transitioned V4: changed from AUTH_IFACE_1 to AUTH_PROTO_1.

8.3 Delegation Interface

Delegation Interface	
ID	**AUTHN_DELEG_1**
Description	Delegation of credentials must be provided using one of the supported delegation interfaces: GridSite or Globus 4.
Mandatory	YES
Applicability	Authentication Appliances that provide (require) delegation.

Input from Technology Provider	Delegation implementation that includes all functionality of the GridSite or Globus 4 interfaces. Correct handling for erroneous input.
Pass/Fail Criteria	Pass if the delegation interface is tested and works as expected. Appliances must support at least **one** of the following interfaces: GridSite delegation or Globus 4 delegation.
Related Information	UMD Roadmap [R 1] GridSite Delegation [R 32] Globus Delegation [R 33]
Revision Log	V2: Merged AUTHN_DELEG_1 & 2.

8.4 CAs root certificates Distribution

These QC deal with the distribution of the EuGridPMA [R 34] root certificates.

CA Checksum	
ID	**AUTHN_CA_1**
Description	The CA distribution must assure that the distributed CA certificates are correct.
Mandatory	YES
Applicability	Trust Anchor Distribution

Input from Technology Provider	Checksum test of each of the root certificates distributed.	
Test Description	**Pre-condition**	None
	Test	Test checksum of the CA certificates.
	Expected Outcome	All checksums are correct.
Pass/Fail Criteria	All CA certificates have correct checksum.	
Related Information		
Revision Log		

CA valid dates	
ID	**AUTHN_CA_2**
Description	Dates of the distributed CA certificates are valid for the current date.
Mandatory	YES
Applicability	Trust Anchor Distribution

Input from Technology Provider	Data validity test of each of the root certificates distributed.	
Test Description	**Pre-condition**	None
	Test	Check the current date is in the range of the valid dates of the certificate.
	Expected Outcome	All dates are valid.
	Sample Test	`#!/bin/sh` `check_dates() {` `  certfile=$1` `  start=`openssl x509 -in $certfile -noout -startdate | cut -f2 -d"="` ` if [$? -ne 0] ; then` ` echo "Error while processing $certfile"` ` return 1` ` fi` ` now=`date +%s` `  start_sec=`date +%s -d"$start"` ` if [$now -lt $start_sec] ; then` ` echo "$start is before now in $certfile!"` ` return 1` ` fi` ` end=`openssl x509 -in $certfile -noout -enddate | cut -f2 -d"="` `  if [ $? -ne 0 ] ; then` `  echo "Error while processing $certfile"` `  return 1` `  fi` `  end_sec=`date +%s -d"$end"` ` if [$end_sec -lt $now] ; then` ` echo "$end is after now in $certfile!"` ` return 1` ` fi` ` return 0` `}`
Pass/Fail Criteria	All CA certificates have correct dates.	
Related Information		
Revision Log		

CA CRL check	
ID	**AUTHN_CA_3**
Description	The CRL of the CAs must be available for download and must be valid.
Mandatory	YES
Applicability	Trust Anchor Distribution

Input from Technology Provider	Test that the CRL of the CA is available for download and it's valid.	
Test Description	**Pre-condition**	List of URLs for each CRL is available.
	Test	Download CRL and load it.
	Expected Outcome	All CRLs can be downloaded and loaded correctly.
	Sample Test	

```
#!/bin/sh

check_crl() {
    url_file=$1
    url=`cat $url_file`
    crl=`mktemp`
    wget -q $url -O $crl
    if [ $? -ne 0 ] ; then
        echo "Unable to download crl from $url"
        rm  $crl
        return 1
    fi
    openssl crl -in $crl -noout &> /dev/null
    if [ $? -ne 0 ] ; then
        # try in other format
        openssl crl -inform der -in $crl -noout &> /dev/null
        if [ $? -ne 0 ] ; then
            echo "Unable to load crl"
            rm $crl
            return 1
        fi
    fi
    rm $crl
    return 0
}
```

Pass/Fail Criteria	All CRLs can be downloaded and loaded.
Related Information	
Revision Log	

9 ATTRIBUTE AUTHORITY

9.1 Attribute Authority Interface

Proxy Issue		
ID	**ATTAUTH_ IFACE_1**	
Description	Users must be able to get proxies with VO related information.	
Mandatory	YES	
Applicability	Attribute Authority Appliances	

Input from Technology Provider	Support for the creation of proxies for different users, roles and groups. Test for error situations (not registered user, unknown VO, non existing role/group, unreachable server)	
Test Description	**Pre-condition**	Valid user certificate, user registered in VO
	Test	Create proxy for user in the given VO.
	Expected Outcome	Valid proxy created.
	Pre-condition	Valid user certificate, user registered in VO, user in a given group/role
	Test	Create proxy for user in the given VO and group/role
	Expected Outcome	Valid proxy created with correct group/role information.
	Pre-condition	Valid user certificate, user not registered in VO
	Test	Create proxy for user in the given VO.
	Expected Outcome	Issue a error message stating that the user is unknown to the VO.
Pass/Fail Criteria	Tests for the creation of proxies work as expected. Groups/Roles/Attributes can be included in the created proxy.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

Proxy Information		
ID	**ATTAUTH_ IFACE_2**	
Description	Users must be able to get information about their proxies.	
Mandatory	YES	
Applicability	Attribute Authority Appliances	

Input from Technology Provider	Tools for getting proxy information.	
Test Description	**Pre-condition**	Valid user proxy
	Test	Get information from proxy.
	Expected Outcome	Return proxy information.
	Pre-condition	Non existent user proxy
	Test	Get information from proxy
	Expected Outcome	No information returned and error message issued.
Pass/Fail Criteria	Proxy information can be obtained. Complete Groups/Roles/Attributes is also shown.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

Proxy Destroy	
ID	**ATTAUTH_ IFACE_3**
Description	Users must be able to destroy a previously created proxy.
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for proxy destroy.	
Test Description	**Pre-condition**	Valid user proxy
	Test	Destroy user proxy.
	Expected Outcome	Proxy is destroyed.
Pass/Fail Criteria	Proxy is destroyed, no operations requiring a proxy can be done with it.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

SAML Assertion Support	
ID	**ATTAUTH_ IFACE_4**
Description	Users should be able to obtain SAML assertions with the VO information.
Mandatory	NO
Applicability	Attribute Authority Appliances with SAML support.

Input from Technology Provider	Support for generation of SAML assertions for different users, roles and groups. Correct handling of error situations (not registered user, unknown VO, non existing role/group, unreachable server)	
Test Description	**Pre-condition**	Valid user, user registered in VO/group/role.
	Test	SAML attribute query for user for the VO/group/role
	Expected Outcome	Valid SAML assertion returned with VO information
	Pre-condition	Valid user, user not registered in VO
	Test	SAML attribute query for user in the given VO.
	Expected Outcome	Issue a error message stating that the user is unknown to the VO.
Pass/Fail Criteria	Tests for the creation of SAML assertions work as expected. Groups/Roles/Attributes can be included in assertions.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

9.2 VO management

VO Creation	
ID	**ATTAUTH_ MGMT_1**
Description	The service administrator must be able to create new VOs in the service.
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for the creation of VOs, correct handling of incorrect input.	
Test Description	**Pre-condition**	Administrator privileges in VO service. Configured service.
	Test	Create a new VO
	Expected Outcome	New database is created and initialized.
	Pre-condition	Administrator privileges in VO service. Configured service. Existent VO name
	Test	Create a VO with already existent name.
	Expected Outcome	No action performed, warning message issued.
Pass/Fail Criteria	Pass if the administrator is able to create VOs for all the supported underlying databases.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

VO Administrators	
ID	**ATTAUTH_ MGMT_2**
Description	The service administrator must be able to define who has VO administrator privileges.
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for adding VO administrators, managing incorrect input.	
Test Description	**Pre-condition**	Administrator privileges in VO service. Configured service. User certificate of new admin.
	Test	Define VO administrator with user certificate.
	Expected Outcome	User is added as VO administrator.
	Pre-condition	Administrator privileges in VO service. Configured service. User certificate of already existent admin.
	Test	Define VO administrator with user certificate.
	Expected Outcome	No action performed, warning message is issued.
	Pre-condition	Administrator privileges in VO service. Configured service. User certificate of new admin.
	Test	Define VO administrator with user certificate for a nonexistent VO.
	Expected Outcome	Error message stating that the VO is not existent.
Pass/Fail Criteria	Pass if the administrator is able to assign administrator privileges to other users.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

VO Role/Group/Attribute Management	
ID	**ATTAUTH_ MGMT_3**
Description	Authorized users must be able to define roles, groups and attributes and manage the users with those assigned.
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for creation of roles, groups, attributes and the assignment and de-assignment of users to those.	
Test Description	**Pre-condition**	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.
	Test	Create a new role/group/attribute in the VO.
	Expected Outcome	New role/group/attribute is created in the VO
	Pre-condition	Authorized user to manage VO role/group/attribute. Already existent Role/Group/Attribute name.
	Test	Create role/group/attribute in the VO.
	Expected Outcome	No action performed; issue warning message about the role/group/attribute already existing.
	Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name.
	Test	Create a new role/group/attribute in the VO.
	Expected Outcome	No action performed, issue error message.
	Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add
	Test	Assign role/group/attribute to user.
	Expected Outcome	User has the role/group/attribute assigned.
	Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. VO User to add
	Test	Assign role/group/attribute to user.
	Expected Outcome	No action performed, issue error message.
	Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign
	Test	De-assign role/group/attribute to user.
	Expected	Role/Group/Attribute is de-assigned.

	Outcome	
	Pre-condition	Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign without assigned role/group/attribute
	Test	De-assign role/group/attribute to user.
	Expected Outcome	No action performed, warning message issued.
	Pre-condition	Non-Authorized user to manage VO role/group/attribute. Role/Group/Attribute name. User to de-assign
	Test	De-assign role/group/attribute to user.
	Expected Outcome	No action performed, issue error message.
Pass/Fail Criteria	Pass if authorized users are able to manage the role/groups/attributes for a given VO and the users that assigned to them.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

VO User Management	
ID	**ATTAUTH_ MGMT_4**
Description	Authorized users must be able to add and remove users to the VO
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for adding/removing users to the VO.	
Test Description	**Pre-condition**	Authorized user to manage VO users. User to add to VO.
	Test	Add user to VO
	Expected Outcome	User is correctly added to the VO.
	Pre-condition	Non-Authorized user to manage VO users. User to add to VO.
	Test	Add user to VO
	Expected Outcome	No action performed, issue error message.
	Pre-condition	Authorized user to manage VO users. User to add to VO that already belongs to the VO.
	Test	Add user to VO
	Expected Outcome	No action performed, issue a warning message.
Pass/Fail Criteria	Pass if authorized users are able to add/remove other users for a given VO.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

ACL Management	
ID	**ATTAUTH_ MGMT_5**
Description	Authorized users must be able to change the different ACLs of the VO.
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	Support for changing ACLs of users of the VO.	
Test Description	**Pre-condition**	Authorized user to manage ACLs.
	Test	Change ACL for a given user.
	Expected Outcome	ACL is correctly changed.
	Pre-condition	Non-Authorized user to manage ACLs.
	Test	Change ACL for a given user.
	Expected Outcome	No action performed, error message issued.
Pass/Fail Criteria	Pass if authorized users are able to manage the ACLs for other users for a given VO. The following list of ACLs is expected to be managed: • browse users of VO • management of groups • management of roles • management of attributes • management of ACL • add/remove users	
Related Information	UMD Roadmap [R 1]	
Revision Log		

User suspension notification	
ID	**ATTAUTH_ MGMT_6**
Description	Users must get a notification about the suspension of their membership prior to the suspension
Mandatory	YES
Applicability	Attribute Authority Appliances

Input from Technology Provider	The Attribute Authority appliance must send notifications to the users that are going to be suspended according to the EGI policies. This notification should be sent as an email warning about the membership expiration date and how to resign the VO AUP or any extra steps needed to successfully renew their membership. The notification must be sent in a configurable period before the expiration date (default value should be > 24h, e.g. 2 weeks)
Pass/Fail Criteria	Pass if •
Related Information	GGUS ticket #77913 RT ticket #3278
Revision Log	

9.3 VO Management Web Interface (VOMS-Admin)

VO List View	
ID	**ATTAUTH_ WEB_1**
Description	Users connecting to the web interface should be able to list the VOs handled by the server.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management

Input from Technology Provider	Provide a web view with the list of VOs in the server.	
Test Description	**Pre-condition**	VO Web server running, authorized user
	Test	Access VO list page.
	Expected Outcome	Web page with a list of all VOs in supported by the server and browsable by user.
Pass/Fail Criteria	VO list view is provided and shows only VOs that are viewable by user.	
Related Information		
Revision Log		

VO Membership Request	
ID	**ATTAUTH_ WEB_2**
Description	Users should be able to request membership to a VO from the web interface.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management

Input from Technology Provider	Provide a page for requesting VO membership and test its functionality. This page must ask for the following information: • Full name • Institution • Contact details (phone, e-mail, address) Once the information is entered, users receive an email to confirm the membership request. Once confirmed, VO Admins should receive a notification of the new request.	
Test Description	**Pre-condition**	VO Web server running, valid credentials of user.
	Test	User requests membership from VO.
	Expected Outcome	User gets an email to confirm the membership request.
	Pre-condition	VO Web server running, valid credentials of user, membership confirmation link.
	Test	User accesses the membership confirmation link.
	Expected Outcome	VO admin(s) receive a notification of the new request.
Pass/Fail Criteria	Pass if the VO membership request page provides the requested functionality.	
Related Information		
Revision Log		

VO Membership Authorisation	
ID	**ATTAUTH_ WEB_3**
Description	VO admins should be able to allow or deny pending membership request from the web interface.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management

Input from Technology Provider	Provide a web page for listing pending membership requests and allowing or denying them.	
Test Description	**Pre-condition**	VO Web server running, valid admin credentials, membership request.
	Test	Admin accepts the membership request.
	Expected Outcome	User is added to the VO. Notification email is sent to user.
	Pre-condition	VO Web server running, valid admin credentials, membership request.
	Test	Admin rejects the membership request.
	Expected Outcome	User is not added to the VO.
Pass/Fail Criteria	Pass if the admin can accept/reject VO membership requests from users.	
Related Information		

VO Administration	
ID	**ATTAUTH_ WEB_4**
Description	Authorized users should be able to manage VO groups, roles, attributes and ACLs from the web interface.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management

Input from Technology Provider	Provide pages for managing the groups, roles, attributes and ACLs of the VO. They must allow the creation of new items, assigning and removing users for those items, deleting items.	
Test Description	**Pre-condition**	VO Web server running, valid credentials.
	Test	Create new group/role/attribute using web interface.
	Expected Outcome	The new group/role/attribute is created.
	Pre-condition	VO Web server running, valid credentials.
	Test	Remove existing group/role/attribute using web interface.
	Expected Outcome	The group/role/attribute is deleted.
	Pre-condition	VO Web server running, valid credentials.
	Test	Assign group/role/attribute to user using web interface.
	Expected Outcome	The group/role/attribute is assigned to user.
	Pre-condition	VO Web server running, valid credentials.
	Test	Remove user from group/role/attribute using web interface.
	Expected Outcome	User no longer has group/role/attribute assigned.
Pass/Fail Criteria	Pass if the admin can accept/reject VO membership requests from users.	
Related Information		

VO Browse	
ID	**ATTAUTH_ WEB_5**
Description	Authorized used should be able to browse the VO members, groups, roles or attributes.
Mandatory	YES
Applicability	Web Portal for Attribute Authority Appliances management

Input from Technology Provider	Provide pages for listing the VO members, groups, roles and attributes for a given VO.	
Test Description	**Pre-condition**	VO Web server running, valid credentials.
	Test	Browse VO members by groups/roles/attributes.
	Expected Outcome	Web pages with list of users for groups/roles/attributes is delivered.
Pass/Fail Criteria	Pass if the VO browsing pages are provided and members can be listed by groups, roles and, or attributes.	
Related Information		
Revision Log		

10 AUTHORISATION

10.1 Policy Management

Policy Listing	
ID	**AUTHZ_ MGMT_1**
Description	Administrators must be able to list the policies stored in the service.
Mandatory	YES
Applicability	Authorisation Appliances with PAP

Input from Technology Provider	Support for policy listing	
Test Description	**Pre-condition**	Policy repository available.
	Test	List policies
	Expected Outcome	List of stored policies.
Pass/Fail Criteria	Pass if the test suite passes	
Related Information	UMD Roadmap [R 1] Argus [R 35]	
Revision Log		

Policy Repositories Management		
ID	**AUTHZ_ MGMT_2**	
Description	Administrators must be able to manage the remote Policy Repositories to be used by the service.	
Mandatory	YES	
Applicability	Authorisation Appliances with PAP	

Input from Technology Provider	Support for the management of Policy Repositories that will be used in the service.	
Test Description	**Pre-condition**	Remote policy repository available.
	Test	Add remote policy repository.
	Expected Outcome	Remote repository added; remote policies retrieved.
	Pre-condition	Configured Remote policy repository.
	Test	Remove remote policy repository.
	Expected Outcome	Remote repository removed, policies no longer available.
	Pre-condition	Configured Remote policy repository
	Test	Update remote policies.
	Expected Outcome	Remote policies retrieved.
	Pre-condition	Enabled policy repository.
	Test	Disable policy repository.
	Expected Outcome	Policies from repository no longer used.
	Pre-condition	Disabled policy repository.
	Test	Enable policy repository.
	Expected Outcome	Policies from repository used.
	Pre-condition	Several policies repositories configured.
	Test	Show policy repository order.
	Expected Outcome	Policy repository order shown.
	Pre-condition	Several policies repositories configured.
	Test	Set new policy repository order.
	Expected Outcome	New policy repository is set.

Pass/Fail Criteria	Pass if the administrator is able to configure the use of (remote) policy repositories: disabling, enabling and establishing an order for them.
Related Information	UMD Roadmap [R 1] Argus [R 35]
Revision Log	

10.2 Policy Definition

10.2.1 Central policy management (Argus)

(un) Banning Policies		
ID	**AUTHZ_ PCYDEF_1**	
Description	Administrators must be able to define policies that ban users or groups of users.	
Mandatory	YES	
Applicability	Authorisation Appliances with PAP	

Input from Technology Provider	Support for banning different users (defined by a DN) or group of users defined by certain attributes (e.g. role/group attributes, FQANs); also support re-establishing already existing banning.	
Test Description	**Pre-condition**	Policy repository available. Banning policy for user/group not defined
	Test	Define ban policy for user/group
	Expected Outcome	Ban policy for user/group stored in policy repository.
	Pre-condition	Policy repository available. Banning policy for user/group defined
	Test	Unban policy for user/group
	Expected Outcome	Ban policy for user/group no longer stored in policy repository.
Pass/Fail Criteria	Pass if the banning policies can be defined (and removed).	
Related Information	UMD Roadmap [R 1] Argus [R 35]	
Revision Log	V4: Removed explicit FQAN references.	

Policy Definition from file		
ID	**AUTHZ_ PCYDEF_2**	
Description	Administrators must be able to manage the policies in the service, loading them from a file. File syntax could be XACML or a simplified equivalent.	
Mandatory	YES	
Applicability	Authorisation Appliances with PAP	

Input from Technology Provider	Support for policy definitions with different users (usually defined by a DN) or group of users defined by certain attributes (e.g. role/group attributes, FQANs); both *allow* and *deny* policies for different resources and actions.	
Test Description	**Pre-condition**	Policy repository available. Policy file with policies.
	Test	Add policies from file.
	Expected Outcome	Policies from file now stored in repository.
	Pre-condition	Policy repository available with a policy to update. Update description in policy file.
	Test	Update policy from file.
	Expected Outcome	Update policy stored in repository.
	Pre-condition	Policy repository available with a policy to remove.
	Test	Remove policy.
	Expected Outcome	Policy no longer stored in repository.
Pass/Fail Criteria	Pass if the administrator cans add/update/remove policies for users and or groups of users.	
Related Information	UMD Roadmap [R 1] Argus [R 35]	
Revision Log	V4: Removed FQAN references.	

10.2.2 Service Based Authorisation (Not Using Argus)

Ban User/Group of users		
ID	**AUTHZ_ PCYDEF_3**	
Description	Administrators must be able to define policies that ban users (black list).	
Mandatory	NO	
Applicability	Authorisation Appliances without PAP (Argus)	

Input from Technology Provider	Support for banning of single user (defined by a DNs) or by a set of users (defined by role/group attributes or FQANs).	
Test Description	**Pre-condition**	Configured system.
	Test	Ban policy for user/group. Test access for user/group.
	Expected Outcome	Ban policy is correctly enforced.
	Pre-condition	Configured system. Banning policy for user/group defined
	Test	Unban user/group. Test access for user/group.
	Expected Outcome	User/group is allowed.
Pass/Fail Criteria	Pass if the banning policies can be defined and enforced at least for users, ideally support role/groups attributes for defining policies.	
Related Information		
Revision Log	V4: better wording, not mandatory since for some service only white list policies can be defined.	

Allowed users definition	
ID	**AUTHZ_ PCYDEF_4**
Description	Administrators must be determine which users/groups are allowed in the system
Mandatory	YES
Applicability	Authorisation Appliances without PAP

Input from Technology Provider	Support for allowing users/groups of users in the system. Support for defining allowed users (determined by DNs) or groups (defined by a set of role/group attributes or FQANs).	
Test Description	**Pre-condition**	Configured system.
	Test	Allow user/group access into system. Test access for user/group.
	Expected Outcome	User/group is allowed in the system.
Pass/Fail Criteria	Pass if the banning policies can be defined and enforced at least for individual users, ideally support role/groups attributes for defining policies.	
Related Information		
Revision Log	V2: Restricted policy definition to allowing access (full control of policy is expected in Argus like systems) V4: reviewed wording	

10.3 Policy Enforcement

User Mapping		
ID	**AUTHZ_ PEP_2**	
Description	The authorisation capability should provide mapping of authorized users to local accounts.	
Mandatory	YES	
Applicability	Authorisation Appliances	

Input from Technology Provider	Support for mapping of users to local accounts; with/without VOMS attributes (or any other role/group attributes schema agreed), and with/without pool accounts. The preferred mapping mechanism is the gridmap dir using gridmapfiles for defining the mappings.	
Test Description	**Pre-condition**	Configured system. No previous mapping for user.
	Test	Accepted authorisation.
	Expected Outcome	GID/UID of the mapping returned. Primary group determined by role/group attributes if available. For gridmap based mapping, new entry in grid map is created.
	Pre-condition	Configured system. Previous mapping for user existing.
	Test	Accepted authorisation.
	Expected Outcome	GID/UID of the previous mapping returned.
Pass/Fail Criteria	Pass if the mapping is performed as defined in the AuthZ appliance (e.g according to a gridmapfile). The use of pool accounts is desirable, although the criteria can pass if not supported. The verifier may accept other mapping mechanisms after discussion within the verification team.	
Related Information	UMD Roadmap [R 1] Argus [R 35]	
Revision Log	V4: removed FQAN references, relaxed pool account support.	

11 CREDENTIAL MANAGEMENT

11.1 Credential Management Interface

Credential Storage	
ID	**CREDMGMT_IFACE_1**
Description	Credential Management Appliances must provide an interface for storing user credentials.
Mandatory	YES
Applicability	Credential Management Appliances

Input from Technology Provider	Support for storing user credentials in the service (with and without VOMS extensions). The service must support storing proxies.	
Test Description	**Pre-condition**	Valid user credentials (X509 certificate/proxy), user allowed in the service.
	Test	Store user credential in the service
	Expected Outcome	Credential is stored in the system
	Pre-condition	Valid user credentials (X509 certificate/proxy), user not allowed in the service.
	Test	Store user credential in the service
	Expected Outcome	Error message is issued; no credentials are stored.
Pass/Fail Criteria	User can successfully store the credentials in the appliance with and without VOMS extensions.	
Related Information		
Revision Log	V4: added explicitly proxy testing.	

Credential Retrieval		
ID	**CREDMGMT_IFACE_2**	
Description	Credential Management Appliances must provide an interface for retrieving user credentials in the service.	
Mandatory	YES	
Applicability	Credential Management Appliances	

Input from Technology Provider	Support for retrieving user credentials in the service (with and without VOMS extensions).	
Test Description	**Pre-condition**	Valid user credentials stored in service, user allowed in the service.
	Test	Retrieve user credential
	Expected Outcome	User credentials returned.
	Pre-condition	No valid user credentials stored in the service.
	Test	Retrieve user credential
	Expected Outcome	Error message is issued; no credentials are returned.
Pass/Fail Criteria	User can successfully retrieve previously store credentials from the appliance with and without VOMS extensions.	
Related Information		
Revision Log		

Credential Renewal		
ID	**CREDMGMT_IFACE_3**	
Description	Credential Management Appliances must provide an interface for renewing user credentials in the service.	
Mandatory	YES	
Applicability	Credential Management Appliances	

Input from Technology Provider	Support for renewing user credentials in the service (with and without VOMS extensions).	
Test Description	**Pre-condition**	Valid user credentials stored in service, host allowed to renew credentials.
	Test	Renew user credential
	Expected Outcome	User credentials renewed.
	Pre-condition	Valid user credentials stored in service, host not allowed to renew credentials.
	Test	Renew user credential
	Expected Outcome	Error message is issued; no credentials are renewed.
	Pre-condition	No valid user credentials stored in the service.
	Test	Renew user credential
	Expected Outcome	Error message is issued; no credentials are renewed.
Pass/Fail Criteria	Services/Users can successfully renew previously retrieved credentials from the appliance with and without VOMS extensions.	
Related Information		
Revision Log		

11.2 Institutional Authentication Systems Linking

Institutional Authentication Linking	
ID	**CREDMGMT_ LINK _1**
Description	Users should be able to access grid resources using institutional authentication systems.
Mandatory	NO
Applicability	Credential Management Appliances

Input from Technology Provider	Support for linking institutional authentication system with the Credential Management implementation	
Test Description	**Pre-condition**	Valid institutional user credentials, user allowed in the service.
	Test	User requests grid credentials using his/her institutional credentials
	Expected Outcome	Short-lived X.509 credential for used created.
Pass/Fail Criteria	Short-lived X.509 credentials are created for authorized users. Test should be executed for each of the authentication systems supported (e.g. Kerberos or Shibboleth)	
Related Information		
Revision Log		

12 JOB EXECUTION

12.1 Job Execution Interface

Currently, there are different interfaces considered for the Job Execution Capability, although not interoperable several of them co-exist in the EGI Infrastructure. The implementations must support, at least, one of the interfaces listed.

Job Execution Interface	
ID	**JOBEXEC_IFACE_1**
Description	Job Execution Appliances must support (at least one of) the interfaces currently in production in the EGI Infrastructure or identified by the UMD Roadmap
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Implementation of one of the Job Execution Interface as defined in the UMD Roadmap. Ideally, a complete test suite of the Job Execution interfaces supported by the appliance. The test suite must include tests for all the documented functions, and for all functions, check both correct and invalid input and with valid and invalid credentials.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all interface functionality, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented. Errors/exceptions should be generated as documented.
Pass/Fail Criteria	The Job Execution Appliance that claims to support an interface must pass complete tests for that interface (provided by the TP or by the verification team). If the API is not completely supported, this **must** be documented. The test suite must be executed without errors. **At least one** of the following interfaces must be supported: • ARC-CE gridFTP [R 11] • CREAM [R 12] • EMI-ES [R 13] • Globus GRAM5 [R 14] • OGSA BES [R 16] • UNICORE UAS [R 17]	
Related Information	UMD Roadmap [R 1]	
Revision Log	V2: unification of several criteria regarding interfaces into this one. V3: removed DRMAA as possible interface.	

12.2 Job Submission tests

The following tests propose example job descriptions using the gLite JDL format for the specification of jobs. These examples are just used for illustrative purposes. Each appliance should execute the tests using their native format.

Simple Job	
ID	**JOBEXEC_JOB_1**
Description	Execute a simple job in the appliance.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Support for the submission of a job with no input or output files.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job submission of simple job:
		`Executable = /bin/sleep;`
		`Arguments = "120";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: merged JOBEXEC_*_JOB_1 into this criterion.	

Simple Job with input/output files	
ID	**JOBEXEC_JOB_2**
Description	Execute a simple job in the appliance that uses both input and output files.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Support for the submission of a job with input or output files.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system) Non-empty files "myfile"

	Test	Job submission for job with input and output files:
		`Executable = "/bin/ls";`
		`Arguments = "-l";`
		`StdOutput = "std.out";`
		`StdError = "std.err";`
		`InputSandbox = {"myfile"};`
		`OutputSandbox = {"std.out", "std.err"};`

	Expected Outcome	Job finishes correctly; output contains the listing of the directory including the input file with correct size. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: merged JOBEXEC_*_JOB_2 into this criterion.	

Cancel Job	
ID	**JOBEXEC_JOB_3**
Description	Cancel a previously submitted job.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Support for the cancellation of a job. Job cancelling must be possible for all different states that the job may be, e.g. cancel the job when it's running or cancel the job when it's already done.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job Submission and then cancellation.
		Possible description for job:
		`Executable = "/bin/sleep";`
		`Arguments = "20m";`

	Expected Outcome	Job is submitted and then cancelled correctly. Unique Identifier for the submitted jobs, status log of the job. The job must be removed from the execution manager.
Pass/Fail Criteria	Pass if the appliance is able to cancel jobs for any previous state of the job. If the job is in the execution manager system, it should be completely removed, especially if it's running.	
Related Information		
Revision Log	V2: merged JOBEXEC_*_JOB_3 into this criterion. Added clarification	

12.3 Execution Manager Support

These QC refer to the interaction of the Job Execution Capability with the underlying execution manager (usually a LRMS) for the work items submitted.

Not Invasive Deployment	
ID	**JOBEXEC_EXECMNGR_1**
Description	Job Execution Appliances should not introduce any modifications to the underlying execution manager or to the operations of the resources.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Description of all needed, if any, modifications on the local resources in order to deploy the Job Execution Appliance.
Pass/Fail Criteria	Any modifications must be documented, especially invasive ones. Modifications to consider are: • Installation of additional software at the WN is permitted as long as no extra services are run permanently at the WN. • Require the deployment of extra (shared) filesystems • Modification of the local submission mechanism of jobs (e.g. require the modification of prologue/epilogue scripts of the batch system) • Require the creation of extra user accounts or add special privileges to a specific account. • Require inbound or outbound connectivity
Related Information	
Revision Log	V2: added inbound, outbound connectivity. Relax Pass/Fail criteria

Job Management	
ID	**JOBEXEC_EXECMNGR_2**
Description	Job Execution Appliances must support the creation and management of work items to an execution manager.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Appliances must be able to: • create new jobs • retrieve the status of the jobs submitted by the appliance • cancel jobs • optionally, hold and resume jobs The Appliance may perform these operations for individual jobs or for set of jobs in order to improve its performance (e.g. for retrieving the status instead of querying each of the individual jobs, do a single query for all jobs submitted for the appliance)	
Test Description	**Pre-condition**	Configured system
	Test	Create new job(s) in execution manager
	Expected Outcome	New job(s) is created in the execution manager; id of job(s) returned
	Pre-condition	Previously submitted job(s)
	Test	Cancel job(s) in execution manager
	Expected Outcome	Job(s) is cancelled successfully.
	Pre-condition	Previously submitted job(s)
	Test	Query status of previously submitted job(s)
	Expected Outcome	Job (s) status is correctly fetched
Pass/Fail Criteria	Pass if the Appliance correctly manages jobs in the underlying execution manager. Tests must be executed (and pass) for each of the execution managers the appliance supports. All appliances should provide support for, **at least one**, of the following systems: • Torque/PBS • LSF • SGE/OGE • Slurm Optionally, the appliance may support a *fork* execution manager (spawning processes in the appliance host)	
Related Information		
Revision Log	V2: Major rewrite of criterion specification.	

Information Retrieval	
ID	**JOBEXEC_EXECMNGR_3**
Description	Job Execution Appliances must be able to collect information from the underlying execution manager.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Support for the information retrieval from execution manager. Information should be returned as a valid GlueSchema representation.	
Test Description	**Pre-condition**	Configured system
	Test	Get information from execution manager
	Expected Outcome	Representation of the current information from the execution manager is generated.
Pass/Fail Criteria	Pass if the Appliance produces information for each of the supported execution managers. The information must include all mandatory attributes of the Computing Element related entities in GlueSchema. All appliances should provide support for, **at least one**, of the following systems: • Torque/PBS • LSF • SGE/OGE • Slurm Optionally, the appliance may support a *fork* execution manager (spawning processes in the appliance host)	
Related Information	Information Capabilities QC	
Revision Log		



12.4 Availability/Scalability

Service Redundancy	
ID	**JOBEXEC_AVAIL_1**
Description	More than one Job Execution Capability implementation should be able to access a single execution manager concurrently.
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	Documentation on how to use more than one appliance instance accessing the same execution manager (if any special consideration must be taken into account) Test of concurrent access to same execution manager from at least two instances.	
Test Description	**Pre-condition**	More than one appliance instance configured to use the same execution manager
	Test	Submission of jobs to all configured appliances
	Expected Outcome	Jobs are executed without problems; they are not mixed up in any situation.
Pass/Fail Criteria	Pass if the documentation specifies the configuration steps for using more than one instance in the same execution manager. Tests passes correctly	
Related Information		
Revision Log	V2: Required documentation, changed ID	

Self Disabling Mechanism	
ID	**JOBEXEC_AVAIL_2**
Description	The Job Execution Capability should detect high load conditions and self-disable the job submission in order to maintain the quality of the service.
Mandatory	NO
Applicability	Job Execution Appliances

Input from Technology Provider	Self-disable mechanism under high-load scenarios. Ideally, stress test for the service that triggers a self-disabling mechanism.	
Test Description	**Pre-condition**	Correctly configured service.
	Test	Introduce high load into machine, submit job.
	Expected Outcome	High load situation is detected, job submission request is not allowed and message is sent to client.
Pass/Fail Criteria	Pass if the test executes as expected. The high load level should be configurable (e.g. CPU load > x, swap usage > y…)	
Related Information		
Revision Log	Changed ID	

Timely Job Status Updates	
ID	**JOBEXEC_AVAIL_4**
Description	Job Execution Appliances should be able to report the job status within a reasonable time frame since the events that originate those statuses even in situations of high load
Mandatory	NO
Applicability	Job Execution Appliances

Input from Technology Provider	Appliance must be able to report the status of the submitted jobs without big delays from the event that originates the status change (e.g. mark the job as running/done once the job enters the running/done status in the local batch system). Ideally TP provides a test for the service that asserts that the appliance is able to report immediately the job statuses under high load conditions (big number of concurrent jobs changing status)
Pass/Fail Criteria	Pass if the appliance reports the new status in a maximum of 10 minutes after the event that generated the status change.
Related Information	
Revision Log	V4: improved Pass/Fails Criteria

13 PARALLEL JOB

13.1 Submission of parallel jobs

The following tests propose example job descriptions using the gLite JDL format for the specification of jobs. These examples are just used for illustrative purposes. Each appliance should provide the tests using their native format.

Simple parallel job submission	
ID	**PARALLEL_JOB_1**
Description	Job Execution Appliances that also provide the Parallel Job Capability must allow users to submit a job requesting more than one execution slot.
Mandatory	YES
Applicability	Job Execution Appliances with Parallel Job Capability.

Input from Technology Provider	Support for the submission of parallel job, requesting more than 1 slot.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job submission:
		`Executable = "/bin/sleep";`
		`CPUNumber = 4;`
		`Arguments = "20";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job. Correct number of slots are allocated
Pass/Fail Criteria	Test is executed correctly. Mapping of slots to machines/cores not relevant for the test.	
Related Information	#1391: Support for parallel jobs in JDL.	
Revision Log	V2: Unified PARALLEL_JOB_1, 3 & 4 into this criterion.	

Single machine parallel job submission		
ID	**PARALLEL_JOB_2**	
Description	Job Execution Appliances that also provide the Parallel Job Capability should allow users to submit a job requesting more than one execution slot in a single machine.	
Mandatory	NO	
Applicability	Job Execution Appliances with Parallel Job Capability.	

Input from Technology Provider	Support for the submission of parallel job, requesting more than 1 slot in a single machine and for a complete machine.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job submission:
		`Executable = "/bin/sleep";`
		`NodeNumber = 1;`
		`SMPGranularity = 4;`
		`Arguments = "20";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job. Correct number of slots are allocated in a single machine
	Pre-condition	Valid user credentials (and delegation if needed in the system)

	Test	Job submission:
		`Executable = "/bin/sleep";`
		`NodeNumber = 1;`
		`SMPGranularity = 4;`
		`WholeNode = True;`
		`Arguments = "20";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job. Complete machine with the requested slots is allocated.
Pass/Fail Criteria	Test is executed correctly.	
Related Information		
Revision Log	V2: Unified PARALLEL_JOB_2 & 5.	

Fine grained mapping parallel job submission	
ID	**PARALLEL_JOB_3**
Description	Job Execution Appliances that also provide the Parallel Job Capability should allow users to submit a job requesting a combination of slots per physical machine.
Mandatory	NO
Applicability	Job Execution Appliances with Parallel Job Capability.

Input from Technology Provider	Support for the submission of parallel job requesting specific configurations of slots in several machines.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job submission:
		`Executable = "/bin/sleep";`
		`NodeNumber = 5;`
		`SMPGranularity = 2;`
		`Arguments = "20";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job. Correct number of slots is allocated.
Pass/Fail Criteria	Test is executed correctly for different combinations (e.g.: N processes in N different hosts, N processes in a single host, N processes per host in K hosts, K number of complete hosts with at least N slots)	
Related Information		
Revision Log	V2: Unified PARALLEL_JOB_2 & 5.	

13.2 MPI support

Precompiled MPI job Execution		
ID	**PARALLEL_MPI_1**	
Description	Parallel Job Appliances must support the execution of MPI jobs.	
Mandatory	YES	
Applicability	Parallel Job Appliances.	

Input from Technology Provider	Support for the submission of a MPI job with pre-existing binary.	
Test Description	**Pre-condition**	Valid User proxy and valid delegation in the service. MPI Binary
	Test	Submission of a MPI job requesting more than one execution slot with MPI Binary included in input sandbox of job or already installed in the system (description of job depending on Job Execution interface)
	Expected Outcome	Job is submitted and executed without errors; the requested slots are allocated. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test is provided and passes for all the MPI implementations supported. Support for Open MPI and MPICH2 should be included	
Related Information	User requirements: #672: MPI support	
Revision Log		

MPI job Execution from source.	
ID	**PARALLEL_MPI_2**
Description	Parallel Job Appliances must support the execution of MPI jobs that are compiled at submission time.
Mandatory	YES
Applicability	Parallel Job Appliances.

Input from Technology Provider	Support for the submission of a MPI job compiled from source during its execution.	
Test Description	**Pre-condition**	Valid User proxy and valid delegation in the service. Source code for MPI application.
	Test	Submission of a MPI job requesting more than one execution slot with MPI source code included in input sandbox of job (description of job depending on Job Execution interface). Prior to the execution of the application, the source must be compiled with the available compiler at the site.
	Expected Outcome	Job is submitted, compiled and executed without errors; the requested slots are allocated. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test is provided and passes for all the MPI implementations supported. Support for Open MPI and MPICH2 should be included	
Related Information	User requirements: #672: MPI support	
Revision Log		

13.3 OpenMP support

Precompiled OpenMP job Execution	
ID	**PARALLEL_OMP_1**
Description	Parallel Job Appliances must support the execution of OpenMP jobs.
Mandatory	YES
Applicability	Parallel Job Appliances.

Input from Technology Provider	Support for the submission of an OpenMP job with pre-existing binary.	
Test Description	**Pre-condition**	Valid User proxy and valid delegation in the service. OpenMP Binary
	Test	Submission of an OpenMP job requesting more than one execution slot with OpenMP Binary included in input sandbox of job (description of job depending on Job Execution interface)
	Expected Outcome	Job is submitted and executed without errors; the requested slots are allocated. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test is provided and passes for all the OpenMP implementations supported.	
Related Information		
Revision Log		

OpenMP job Execution from source		
ID	**PARALLEL_OMP_2**	
Description	Parallel Job Appliances must support the execution of OpenMP jobs that are compiled at submission time.	
Mandatory	YES	
Applicability	Parallel Job Appliances.	

Input from Technology Provider	Support for the submission of an OpenMP job that gets compiled at the remote site.	
Test Description	**Pre-condition**	Valid User proxy and valid delegation in the service. Source code for OpenMP application.
	Test	Submission of an OpenMP job requesting more than one execution slot with OpenMP source code included in input sandbox of job (description of job depending on Job Execution interface). Prior to the execution of the application, the source must be compiled with the available compiler at the site.
	Expected Outcome	Job is submitted, compiled and executed without errors; the requested slots are allocated. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test is provided and passes for all the OpenMP implementations supported.	
Related Information		
Revision Log		

14 INTERACTIVE JOB MANAGEMENT

Interactive login	
ID	**INTERACTIVE_JOB_1**
Description	Login interactively to a remote site using grid credentials
Mandatory	NO
Applicability	Interactive Job Management (Interactive Login)

Input from Technology Provider	Tool for providing interactive login to remote machine using any of the supported authn/authz in the UMD Roadmap.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)
	Test	Interactive login to remote site
	Expected Outcome	Login is performed and a shell is provided.
Pass/Fail Criteria	Pass if the tool is able to perform the remote logins correctly using the grid credentials	
Related Information	gsissh, glogin UMD Roadmap Interactive Job Management [R 1]	
Revision Log		

Interactive Job Perusal	
ID	**INTERACTIVE_JOB_2**
Description	Provide a mechanism for getting files produced by a job running in a remote site.
Mandatory	NO
Applicability	Interactive Job Management (Interactive Job Steering)

Input from Technology Provider	Mechanism that is able to retrieve the files produced by a job during its runtime. The provided service should be configurable to retrieve the files at periodic intervals of time. Files to retrieve *should* be configurable.
Pass/Fail Criteria	Pass if the provided service is able to retrieve at periodic intervals job output files during the job execution.
Related Information	WMS Job Perusal UMD Roadmap Interactive Job Management [R 1]
Revision Log	

Interactive Job Monitoring	
ID	**INTERACTIVE_JOB_3**
Description	Provide a mechanism for streaming files produced by a job running in a remote site.
Mandatory	NO
Applicability	Interactive Job Management (Interactive Job Steering)

Input from Technology Provider	Mechanism that is able to stream the files produced by a job during its runtime. Ideally, the files to stream should be configurable. By default the standard output and error of the job should be used.
Pass/Fail Criteria	Pass if the provided service is able to stream the job output files during the job execution.
Related Information	globus-job-get-output, i2glogin UMD Roadmap Interactive Job Management [R 1] #1385: Interactive jobs monitoring
Revision Log	

Interactive Job Steering	
ID	**INTERACTIVE_JOB_4**
Description	Provide a mechanism for steering a job running in a remote site.
Mandatory	NO
Applicability	Interactive Job Management (Interactive Job Steering)

Input from Technology Provider	Mechanism that is able to stream the files produced by a job during its runtime and to control the job execution (i.e. stream the job's standard input from the user location to the remote site).
Pass/Fail Criteria	Pass if the provided service is able to control the job execution by creating a communication channel that forwards output/error and input streams between the user and the remote job
Related Information	i2glogin UMD Roadmap Interactive Job Management [R 1]
Revision Log	

15 JOB SCHEDULING

15.1 Job Scheduling Interface

The Job Scheduling Capabilities does not have a standard interface. Any implementation of this capability can support on of the Job Execution interfaces proposed by the OGF (DRMAA, BES) or proprietary interfaces (gLite WMS)

Job Scheduling Interface	
ID	**JOBSCH_IFACE_1**
Description	Job Scheduling Appliances must support one of the interfaces currently in use or identified by the UMD Roadmap
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Implementation of one of the Job Scheduling Interfaces as defined in the UMD Roadmap. Ideally, a complete test suite of the Job Execution interfaces supported by the appliance. The test suite must include tests for all the documented functions, and for all functions, check both correct and invalid input and with valid and invalid credentials.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all interface functionality, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	The Job Scheduling Appliance that claims to support an interface must pass complete tests for that interface (provided by the TP or by the verification team). If the API is not completely supported, this **must** be documented. The test suite must be executed without errors. **At least one** of the following interfaces must be provided: • gLite WMS [R 18] • OGF DRMAA [R 15] • OGSA BES [R 16]	
Related Information	UMD Roadmap Job Scheduling Capability	
Revision Log	V2: Merged all the interface related criteria into this.	

15.2 Job Execution Capability Support

Remote Job Management	
ID	**JOBSCH_EXEC_1**
Description	Job Scheduling Appliances must support the creation and management of work items to an Job Execution Appliance
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Appliance must be able to: • create new jobs • retrieve the status of the jobs submitted by the appliance • cancel jobs • optionally, hold and resume jobs The Appliance may perform these operations for individually for each submitted job or for set of jobs in order to improve its performance (e.g. for retrieving the status instead of querying each of the individual jobs, do a single query for all jobs submitted at a given appliance)	
Test Description	**Pre-condition**	Configured system
	Test	Create new job(s) in job execution appliance
	Expected Outcome	New job(s) is created in the job execution appliance; id of job(s) returned
	Pre-condition	Previously submitted job(s)
	Test	Cancel job(s) in job execution appliance.
	Expected Outcome	Job(s) is cancelled successfully.
	Pre-condition	Previously submitted job(s)
	Test	Query status of previously submitted job(s)
	Expected Outcome	Job (s) status is correctly fetched
Pass/Fail Criteria	Pass if the Appliance correctly manages jobs in the job execution appliances. Tests must be executed (and pass) for each of the job execution appliances supported. **At least one** of the following interfaces must be supported: • ARC-CE gridFTP [R 11] • CREAM [R 12] • EMI-ES [R 13] • Globus GRAM5 [R 14] • OGF DRMAA [R 15] • OGSA BES [R 16] • UNICORE UAS [R 17]	

Related Information	UMD Roadmap Job Execution QC
Revision Log	V2: Major rewrite of criterion specification.

Remote Resource Information	
ID	**JOBSCH_EXEC_2**
Description	Job Scheduling Appliances must be able to use the resource descriptions using the current Information Model and Information Discovery interfaces.
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Appliances must handle resources described with the current Information Model (GlueSchema1.3 and optionally GlueSchema2) and Information Discovery (LDAPv3) interfaces.	
Test Description	**Pre-condition**	Configured system
	Test	Fetch information from Information Discovery Appliance.
	Expected Outcome	Information is fetched correctly; resources described are added to the list of possible resources to use.
Pass/Fail Criteria	Pass if the Appliance correctly fetches information from Information Discovery appliances and is able to use the resources described by GlueSchema v1.3 and/or GlueSchema v2.	
Related Information	Information Capabilities in the UMD Roadmap [R 1]	
Revision Log		

15.3 End-to-end job submission tests

The following tests propose example job descriptions using the gLite JDL format for the specification of jobs. These examples are just used for illustrative purposes. Each appliance should execute the tests using their native format.

Simple Job	
ID	**JOBSCH_JOB_1**
Description	Execute a simple job.
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Support for the submission of a job with no input or output files.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job submission of simple job:
		`Executable = /bin/sleep;`
		`Arguments = "120";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

Simple Job with input/output files	
ID	**JOBSCH_JOB_2**
Description	Execute a simple job that uses both input and output files.
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Support for the submission of a job with input or output files.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system) Non-empty file "myfile"

	Test	Job submission for job with input and output files:
		`Executable = "/bin/ls";`
		`Arguments = "-l";`
		`StdOutput = "std.out";`
		`StdError = "std.err";`
		`InputSandbox = {"myfile"};`
		`OutputSandbox = {"std.out", "std.err"};`

	Expected Outcome	Job finishes correctly; output contains the listing of the directory including the input file with correct size. Unique Identifier for the submitted jobs, status log of the job.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic.	

Cancel Job	
ID	**JOBSCH_JOB_3**
Description	Cancel a previously submitted job.
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Support for the cancellation of a job. Job cancelling must be supported for the different states that the job may be, e.g. cancel the job when it's running or cancel the job when it's already done.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job Submission and then cancellation.
		Possible description for job:
		`Executable = "/bin/sleep";`
		`Arguments = "20m";`

	Expected Outcome	Job is submitted and then cancelled correctly. Unique Identifier for the submitted jobs, status log of the job. Job is removed from remote Job Execution Appliance.
Pass/Fail Criteria	Pass if the appliance is able to cancel jobs for any previous state of the job. If the job is already submitted to a Job Execution Appliance, it should be completely removed from it, especially if it's running.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

Parallel Job	
ID	**JOBSCH_JOB_4**
Description	Execute a parallel job.
Mandatory	NO
Applicability	Job Scheduling Appliances with Parallel Job Support.

Input from Technology Provider	Support for the submission of a job with input or output files.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)

	Test	Job Submission or parallel job. Possible description for job:
		`Executable = "/bin/sleep";`
		`CPUNumber = 2;`
		`Arguments = "20";`

	Expected Outcome	Job finishes correctly. Unique Identifier for the submitted jobs, status log of the job. Correct number of slots is allocated at the remote site.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

Job List Match	
ID	**JOBSCH_JOB_5**
Description	List the available resources for a given job.
Mandatory	YES
Applicability	Job Scheduling Appliances

Input from Technology Provider	Support for the list match of a job.	
Test Description	**Pre-condition**	Valid user credentials and delegation in the service.

	Test	Job list match for job with requirements and rank expressions, for example:
		`Executable = "/bin/sleep";`
		`Requirements = other.GlueCEStateStatus = "Production";`
		`Rank = -other.GlueCEStateEstimatedResponseTime;`

	Expected Outcome	List of available resources for execution (with correct rank) is returned.
Pass/Fail Criteria	The Job Scheduling Appliance must return a list of available resources for the execution of any given job. Optionally, a *rank* defined by the user is returned by each of the resources.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

Parametric Job Submission		
ID	**JOBSCH_JOB_6**	
Description	Execute a parametric job.	
Mandatory	NO	
Applicability	Job Scheduling Appliances with support for parametric jobs.	

Input from Technology Provider	Support for the submission of parametric jobs.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)
	Test	Job submission of job with numeric parameters (e.g. `Parameters = 10000;ParameterStart = 1000; ParameterStep = 10;`).
	Expected Outcome	Job is executed correctly. List of JobIds for the parametric jobs and each of the subjobs is obtained; all states of the jobs must be logged correctly.
	Pre-condition	Valid user credentials (and delegation if needed in the system)
	Test	Job submission of job with a list of parameters (e.g. `Parameters={A, B, C,…}`).
	Expected Outcome	Job is executed correctly. List of JobIds for the parametric jobs and each of the subjobs is obtained; all states of the jobs must be logged correctly.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

Job Collection Submission	
ID	**JOBSCH_JOB_7**
Description	Execute a job collection
Mandatory	NO
Applicability	Job Scheduling Appliances with support for job collections.

Input from Technology Provider	Support for the submission of job collections.	
Test Description	**Pre-condition**	Valid user credentials (and delegation if needed in the system)
	Test	Job submission for job collection.
	Expected Outcome	Job is executed correctly. List of JobIds for the job collections and each of the subjobs is obtained; all states of the jobs must be logged correctly.
Pass/Fail Criteria	Pass if the test passes correctly.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

DAG Submission		
ID	**JOBSCH_JOB_8**	
Description	Execute a DAG job.	
Mandatory	NO	
Applicability	Job Scheduling Appliances with support for DAGs.	

Input from Technology Provider	Support for the submission of DAGs.	
Test Description	**Pre-condition**	Valid user credentials and delegation in the service.
	Test	Job submission for DAG.
	Expected Outcome	Job is executed correctly. List of JobIds for DAG and each of the subjobs is obtained; all states of the jobs must be logged correctly.
Pass/Fail Criteria	Pass if the test passes correctly. DAGs must be able to use any of the Job Execution Interfaces supported by the Job Scheduling Appliance. Explicit test this possibility.	
Related Information		
Revision Log	V2: moved specific WMS criteria to generic to all Job Scheduling	

15.4 gLite WMS

This section includes criteria applicable to the gLite WMS system.

Proxy Renewal		
ID	**JOBSCH_WMS_1**	
Description	The WMS must manage the user credentials and renew them if necessary.	
Mandatory	YES	
Applicability	gLite WMS Job Scheduling Appliances.	

Input from Technology Provider	Support for the proxy renewal mechanism for long running jobs.	
Test Description	**Pre-condition**	Valid user credentials with short duration (e.g. 30 min) and delegation in the service. Credentials Renewal service available.
	Test	Submit job that takes longer to complete that the credential lifetime (e.g. 1 hour)
	Expected Outcome	Job executes successfully. The scheduling services should perform a proxy renewal and state it in the log messages (if there is an error, log it also). Output of the job, and status messages stating the renewal of the user credentials.
	Pre-condition	Valid user credentials with short duration, e.g. 30 min, no renewal service.
	Test	Submit job that takes longer to complete that the credential lifetime (e.g. 1 hour)
	Expected Outcome	Job does not complete successfully. Log of operations and status of the job updated with information about the error (no renewal possible)
Pass/Fail Criteria	Will Pass if the proxy renewal is done, or if there is an error logged stating the problem. Will fail if there is no clear information about the process.	
Related Information		
Revision Log		

Job Resubmission		
ID	**JOBSCH_WMS_2**	
Description	Any job failures (due to resource malfunctioning or the job itself) must be resubmitted with a configurable amount of retrials.	
Mandatory	NO	
Applicability	gLite WMS Job Scheduling Appliances.	

Input from Technology Provider	Support for the resubmission mechanism of the WMS.	
Test Description	**Pre-condition**	Valid user credentials and delegation in the service.
	Test	Job submission that fails due to simulated remote resource malfunctioning.
	Expected Outcome	Job is resubmitted to other resource. Log of all failures and a complete trace of the job.
	Pre-condition	Valid user credentials and delegation in the service.
	Test	Job submission for job that always fails (e.g. exit code 1)
	Expected Outcome	Job is resubmitted until resubmission attempts reach the configured limit. Log of all failures and a complete trace of the job.
Pass/Fail Criteria	Job failures due to resource malfunctioning and not to the job itself must be resubmitted to other resources, with a configurable amount of repetitions. In the case of job failures due to the job itself must be resubmitted with a configurable amount of repetitions. In both situations, status must reflect clearly what is the cause of resubmission, new resource selected and attempt number	
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.	
Revision Log	V2: originally JOBEXEC_WMS_JOB_9	

JDL Acceptance Limits	
ID	**JOBSCH_WMS_3**
Description	The service should accept JDLs without size restrictions
Mandatory	NO
Applicability	gLite WMS Job Scheduling Appliances.

Input from Technology Provider	A test to submit a job and check if it is accepted or rejected, specially for big JDLs.	
Test Description	**Pre-condition**	Valid user credentials and delegation in the service.
	Test	Submission of job descriptions (specially large)
	Expected Outcome	Normal job submission if everything is correct; an error message if any problem arises.
Pass/Fail Criteria	Will Pass if JDL is correct, and submits the job or if there is a report on a known syntax error in the jdl. Will Fail if a wrong Jdl is accepted or if it crashes	
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.	
Revision Log	V2: originally JOBEXEC_WMS_JOB_10	

15.4.1 Security Advisories

Security Advisory 1502	
ID	**JOBSCH_WMS_SEC_1**
Description	Steal of proxies is possible without leaving trace.
Mandatory	YES
Applicability	gLite WMS Job Scheduling Appliances.

Input from Technology Provider	Test that assures the problem described in the SVG Advisory 1502 (proxy stealing) is fixed.
Pass/Fail Criteria	Fix for Advisory-SVG-2011-1502 is provided. A test that proves that the fix is provided should be also present.
Related Information	Advisory-SVG-2011-1502 (https://wiki.egi.eu/wiki/SVG:Advisory-SVG-2011-1502)
Revision Log	

15.4.2 Bugs

Long Proxy Chain Support	
ID	**JOBSCH_WMS_BUG_1**
Description	Long proxy chains should be supported without no issues.
Mandatory	YES
Applicability	gLite WMS Job Scheduling Appliances.

Input from Technology Provider	Support for long proxy chains such as the ones created when using myproxy (C=[…]/CN=proxy/CN=proxy/CN=proxy/CN=proxy)	
Test Description	**Pre-condition**	Valid authorized user credentials with long proxy chain.
	Test	Delegation of proxy into service.
	Expected Outcome	Delegation is performed without issues.
Pass/Fail Criteria	No authorization errors (for authorized users) given when using long proxy chains.	
Related Information	GGUS Ticket: #73035	
Revision Log		

Multiple Role/Group Proxy Support	
ID	**JOBSCH_WMS_BUG_2**
Description	Proxies of users belonging to multiple groups should be accepted.
Mandatory	YES
Applicability	gLite WMS Job Scheduling Appliances.

Input from Technology Provider	Support for renewal of proxies with multiple groups must be allowed.	
Test Description	**Pre-condition**	Valid user proxy with multiple groups.
	Test	Delegation of proxy into service, renewal of the delegation.
	Expected Outcome	Delegation and renewal are performed without issues.
Pass/Fail Criteria	Pass of the delegation and renewal are performed correctly for multiple group proxies.	
Related Information	GGUS Ticket: #78892	
Revision Log		

15.5 Service availability, monitoring and error handling.

Error Messages	
ID	**JOBSCH_SERVICE_1**
Description	Error messages provided by the service should be clear and facilitate the solution of those errors by users or service administrators
Mandatory	NO
Applicability	Job Scheduling Appliances.

Input from Technology Provider	Include in documentation, a list of possible errors and possible solution/cause for it. For errors that may reach the user, this list has to be exhaustive.
Pass/Fail Criteria	Will pass if the list of errors is documented and includes information about: • Error code • Error message (if applicable) • Error source (internal module or remote resource (specify it explicitly)) • Cause of error (syntax error, module malfunctioning, configuration problem, network error, other (specify it explicit)) • Type (critical, informative) • Possible solution
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.
Revision Log	

Service Information	
ID	**JOBSCH_SERVICE_2**
Description	Job Scheduling Appliances must be able to generate information about the provided service that can be used in a Information Discovery Appliance.
Mandatory	NO
Applicability	Job Scheduling Appliances.

Input from Technology Provider	Support for information generation about the service status.	
Test Description	**Pre-condition**	Configured system, Information Discovery appliance available.
	Test	Generate service information and publish to Information Discovery Appliance. Access Info Discovery Appliance.
	Expected Outcome	Information is produced and can be accessed through the Information Discovery Appliance.
Pass/Fail Criteria	Test is provided and executed as expected.	
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.	
Revision Log		

Self Disabling Mechanism	
ID	**JOBSCH_SERVICE_3**
Description	The Job Scheduling Capability should detect high load conditions and self-disable the job submission in order to maintain the quality of the service.
Mandatory	NO
Applicability	Job Scheduling Appliances

Input from Technology Provider	Support for self-disabling mechanism under high load conditions. Ideally, stress test for the service that triggers a self-disabling mechanism.	
Test Description	**Pre-condition**	Correctly configured service.
	Test	Introduce high load into machine, submit job.
	Expected Outcome	High load situation is detected, job submission request is not allowed and message is sent to client.
Pass/Fail Criteria	Pass if the test executes as expected. The high load level should be configurable (e.g. CPU load > x, swap usage > y…)	
Related Information	User requirements: #698: WMS stability and performance #702: Stability of UMD services and improvements	
Revision Log	V2: Changed ID (from JOBSCH_SERVICE_4 to JOBSCH_SERVICE_3)	

Job Submission Peaks	
ID	**JOBSCH_SERVICE_4**
Description	Job Scheduling Appliances should be able to handle high job submission rates of several hundreds jobs in short intervals.
Mandatory	NO
Applicability	Job Scheduling Appliances

Input from Technology Provider	Appliance should be able to handle a high number of jobs submitted in a short time interval (e.g. 500 jobs / minute). Ideally, test the service to assert that this is provided
Pass/Fail Criteria	Appliances should be able to handle job bursts of several hundreds of jobs in short intervals.
Related Information	User requirements: #698: WMS stability and performance
Revision Log	

Timely Job Status Updates	
ID	**JOBSCH_SERVICE_5**
Description	Job Scheduling Appliances should be able to report the job status within a reasonable time frame since the events that originate those statuses even in situations of high load
Mandatory	NO
Applicability	Job Execution Appliances

Input from Technology Provider	Appliance must be able to report the status of the submitted jobs without big delays from the event that originates the status change (e.g. mark the job as running/done once the job enters the running/done status in the local batch system). Ideally TP provides a test for the service that asserts that the appliance is able to report immediately the job statuses under high load conditions (big number of concurrent jobs changing status)
Pass/Fail Criteria	Appliances *should* be able to report the status immediately after the event that generated the status change.
Related Information	User requirements: #698: WMS stability and performance.
Revision Log	

16 INFORMATION MODEL

16.1 Information Model Schema

GlueSchema Support	
ID	**INFOMODEL_SCHEMA_1**
Description	Resource information exchanged in the EGI Infrastructure must conform to GlueSchema.
Mandatory	YES
Applicability	Information Model Appliances

Input from Technology Provider	Resource information published by Information Discovery Appliances must conform to the GlueSchema v2.0 and v1.3 (optionally).	
Test Description	**Pre-condition**	None.
	Test	Check that information published conforms to GlueSchema (v2.0 and 1.3). The suggested tool for testing the conformance is the GlueValidator [R 25]
	Expected Outcome	Information conforms to GlueSchema. NEEDS SPECIFICATION OF EXCEPTIONS
Pass/Fail Criteria	Information published must be available in GlueSchema v1.3 and/or GlueSchema v2. (it is expected that all products transition to GlueSchema v2) Ideally the Technology Provider should assure this by a test suite of the appliances.	
Related Information	UMD Roadmap [R 1] GlueSchema v1.3 [R 23] GlueSchema v2 [R 24] GlueValidator [R 25]	
Revision Log	V2: Merged INFOMODEL_SCHEMA_* into this criterion. Rephrasing. V4: Added reference to Glue Validator	

Middleware Version Information	
ID	**INFOMODEL_SCHEMA_2**
Description	The middleware version must be published in the resource information.
Mandatory	NO
Applicability	Information Model Appliances

Input from Technology Provider	Resource information published by Information Discovery Appliances must include the version of the middleware.
Pass/Fail Criteria	Middleware version of service is published correctly by the service.
Related Information	Requirement #1378
Revision Log	

17 INFORMATION DISCOVERY

17.1 Information Discovery Interface

Information Discovery Interface	
ID	**INFODISC_IFACE_1**
Description	Information published by the appliance must be available through LDAPv3 protocol
Mandatory	YES
Applicability	Information Discovery Appliances

Input from Technology Provider	LDAP interface for getting the available information.	
Test Description	**Pre-condition**	Information Discovery Appliance is running
	Test	Fetch information from Discovery Appliance using LDAPv3.
	Expected Outcome	Information is retrieved correctly from server.
Pass/Fail Criteria	Information published must be available through LDAPv3 protocol.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

17.2 Information Discovery Functionality

17.2.1 Information Aggregation

The Information Discovery services aggregate information from lower level sources of information in a hierarchical way. Appliances providing the Information Discovery Capability must be able to aggregate lower level sources of information and apply filter to that information

Information Filtering		
ID	**INFODISC_AGG_1**	
Description	The information discovery service must be able to filter some of the data coming from information sources (e.g. do not publish information of a compute capability for a given VO)	
Mandatory	NO	
Applicability	Information Discovery Appliances	

Input from Technology Provider	The Appliances must allow the definition of information filters (e.g. do not publish information of a CE for a given VO).	
Test Description	**Pre-condition**	Valid sources of information are available. Valid filter.
	Test	Filter sources according to filter.
	Expected Outcome	Output filtered information
	Pre-condition	Valid sources of information are available. Invalid filter.
	Test	Filter sources according to filter.
	Expected Outcome	Error message stating that the information cannot be filtered. Output unfiltered information.
Pass/Fail Criteria	The administrator must be able to define filters for the information that gets published by the appliance. The appliance defines the format and syntax for the filters.	
Related Information	UMD Roadmap [R 1]	
Revision Log	V2: Rephrase, turned to non-mandatory.	

Information Aggregation		
ID	**INFODISC_AGG_2**	
Description	The information discovery service must be able to collect data from different sources and aggregate them in a single source of information.	
Mandatory	YES	
Applicability	Information Discovery Appliances	

Input from Technology Provider	Support for the aggregation of different sources of information into the appliance (e.g. aggregation of several site-BDII in the top-BDII)	
Test Description	**Pre-condition**	Set of valid information service sources available and correct.
	Test	Aggregate information from sources
	Expected Outcome	Output aggregated information
	Pre-condition	Set of valid information service sources available, at least one incorrect (e.g. not GlueSchema compliant)
	Test	Aggregate information from sources
	Expected Outcome	Output aggregated information without incorrect source. Show a warning message.
	Pre-condition	Set of valid information service sources, at least one unreachable
	Test	Aggregate information from sources
	Expected Outcome	Output aggregated information without unreachable source. Show a warning message.
Pass/Fail Criteria	The appliance must aggregate several sources of information. When one of them presents errors or is unreachable, others still must be published. Update interval for sources must be configurable.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

Dynamic Information publication	
ID	**INFODISC_AGG_3**
Description	The information discovery service must be able to publish dynamic information at resource level.
Mandatory	YES
Applicability	Information Discovery Appliances

Input from Technology Provider	Support for the collection of dynamic information defined as mandatory in the GlueSchema. The update interval should be configurable.
Pass/Fail Criteria	The appliance must publish dynamic information defined in the GlueSchema (at least the mandatory attributes). The update interval must be configurable
Related Information	UMD Roadmap [R 1]
Revision Log	V4: general improvement of criterion.

17.2.2 Availability/Scalability

Top Information System Size	
ID	**INFODISC_AVAIL_1**
Description	Central Information Discovery appliances must be able to handle information about the whole EGI.eu infrastructure (which may contain several hundred sites)
Mandatory	YES
Applicability	Information Discovery Appliances

Input from Technology Provider	Limit of size of the data handled by the service should be enough to cover the whole EGI.eu Infrastructure. Documentation on how to tune the service in order support large data sizes.	
Test Description	**Pre-condition**	Correctly configured service.
	Test	Add information from all EGI.eu Infrastructure.
	Expected Outcome	Appliance is able to aggregate all the information and responds to clients.
Pass/Fail Criteria	Pass if the appliance is able to handle the global EGI.eu Infrastructure information.	
Related Information	UMD Roadmap [R 1]	
Revision Log	V2: major rephrasing V3: better wording	

18 MESSAGING

Messaging Interface	
ID	**MSG_IFACE_1**
Description	Messaging Appliances must support (at least one of) the interfaces currently in production in the EGI Infrastructure or identified by the UMD Roadmap
Mandatory	YES
Applicability	Messaging Appliances

Input from Technology Provider	Support for at least one of the EGI requested messaging interfaces. Ideally, provide a test suite that assured the support of those interfaces, that checks for all functions, both correct and invalid input. Any deviation from the messaging interface specification must be documented.	
Test Description	**Pre-condition**	Messaging Appliance configured
	Test	Test all interface functionality, with correct/incorrect input.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	The Messaging Appliance that claims to support an interface must have support of that interface. Any deviation from the interface specification must be documented. **At least one** of the following interfaces must be supported: • JMS 1.1 [R 26] • AMQP [R 27]	
Related Information	UMD Roadmap [R 1]	
Revision Log	V3: rephrasing not to require tests.	

19 DATA ACCESS

Criteria for the Data Access Capability are based on OGSA-DAI and WS-DAI interface as reference.

19.1 WS-DAI Interface

WS-DAIR API	
ID	**DATAACCESS_API_1**
Description	Data Access Appliances must implement (at least one of) the WS-DAI realizations and support all the functionality included in the interface.
Mandatory	YES
Applicability	Data Access Appliances

Input from Technology Provider	WS-DAI API support using the relational [R 3] or XML [R 4] realization. Ideally include a test-suite that covers all the documented functions in the WSDL.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all functionality of WS-DAI using the relational or XML realization, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the functions work as documented.
Pass/Fail Criteria	WS-DAI API is provided for the supported realizations. Check both correct and invalid input. Invalid output should throw an exception as documented. Test also with valid and invalid credentials. Invalid credentials should throw security related exceptions.	
Related Information	UMD Roadmap [R 1] WS-DAIR [R 3] WS-DAIX[R 4] #665: Data availability	
Revision Log	V2: Merged DATAACCESS_API_* V3: changed wording	

19.2 OGSA-DAI Criteria

Deployment of data resources		
ID	**DATAACCESS_OGSADAI_1**	
Description	The OGSA-DAI implementation should allow the deployment of data resources with SQL, XML or files sources.	
Mandatory	YES	
Applicability	OGSA-DAI Data Access Appliance.	

Input from Technology Provider	Support for deployment of SQL, XML and file data resources.	
Test Description	**Pre-condition**	Existing SQL data resource.
	Test	Deploy SQL data resource. Test queries against deployed resource.
	Expected Outcome	SQL data resources is available, queries are executed correctly.
	Pre-condition	Existing XMLDB data resource.
	Test	Deploy XMLDB data resource. Test queries against deployed resource.
	Expected Outcome	XMLDB data resource is available, queries are executed correctly.
	Pre-condition	Existing file data resource.
	Test	Deploy file data resource. Test queries against deployed resource.
	Expected Outcome	File data resource is available, queries are executed correctly.
	Pre-condition	Existing remote resource.
	Test	Deploy remote resource. Test queries against deployed resource.
	Expected Outcome	Remote resource is available, queries are executed correctly.
	Pre-condition	Deployed data resource.
	Test	Undeploy resource. Test queries against resource.
	Expected Outcome	Remote resource is no longer available; queries are not executed correctly.
Pass/Fail Criteria	Data resources can be deployed/undeployed and queries against the resources are executed correctly.	
Related Information	OGSA-DAI [R 5]	
Revision Log	V3: changed wording	

Management of data resources access	
ID	**DATAACCESS_OGSADAI_2**
Description	The OGSA-DAI implementation must allow the definition of which users are allowed to access the deployed resources
Mandatory	YES
Applicability	OGSA-DAI Data Access Appliance.

Input from Technology Provider	Support for user management of data resources.	
Test Description	**Pre-condition**	Existing data resource. Valid user credentials
	Test	Allow access to user. Test the access.
	Expected Outcome	User is allowed to access the data resource.
	Pre-condition	Existing data resource. Valid user credentials
	Test	Deny access to user. Test the access.
	Expected Outcome	User is not allowed to access the data resource.
Pass/Fail Criteria	Appliance must allow the admission/denial of users to data resources.	
Related Information	OGSA-DAI [R 5]	
Revision Log	V3: changed wording	

Deployment of activities at resource	
ID	**DATAACCESS_OGSADAI_3**
Description	The OGSA-DAI implementation should allow the deployment of activities in server.
Mandatory	YES
Applicability	OGSA-DAI Data Access Appliance.

Input from Technology Provider	Support for deployment of activities.	
Test Description	**Pre-condition**	OGSA-DAI server available; Activity classes available at server.
	Test	Deploy activity at server. Add activity to resource. Test execution of activity.
	Expected Outcome	Activity is available and executed correctly.
Pass/Fail Criteria	Appliance must allow the deployment of activities and their execution.	
Related Information	OGSA-DAI [R 5]	
Revision Log	V3: changed wording	

Workflow creation and execution		
ID	**DATAACCESS_OGSADAI_4**	
Description	The OGSA-DAI implementation should allow the creation of workflows with activities	
Mandatory	YES	
Applicability	OGSA-DAI Data Access Appliance.	

Input from Technology Provider	Support for the creation and execution of workflows.	
Test Description	**Pre-condition**	Existing OGSA-DAI server.
	Test	Create simple workflow, synchronous execution in server.
	Expected Outcome	Workflow is executed. Status and data results of workflow can be retrieved.
	Pre-condition	Existing OGSA-DAI server.
	Test	Create simple workflow, asynchronous execution in server.
	Expected Outcome	Workflow is executed. Status and data results of workflow can be retrieved.
Pass/Fail Criteria	Appliance must allow the creation of workflows and their execution in both synchronous and asynchronous mode.	
Related Information	OGSA-DAI [R 5]	
Revision Log	V3: changed wording	

20 METADATA CATALOGUE

Criteria for the Metadata Catalogue Capability are based on gLite LFC [R 6] and gLite AMGA [R 7]

20.1 LFC Implementation

20.1.1 LFC API

LFC API	
ID	**METADATA_LFC_API_1**
Description	LFC Metadata Catalogue Appliances must implement the LFC API.
Mandatory	YES
Applicability	LFC Metadata Catalogue Appliances

Input from Technology Provider	Support for the LFC API. Any deviation from the API should be documented. Ideally, provide a complete test suite that includes tests for all the documented functions.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all functionality of LFC API, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	Pass if the LFC API support is tested for all the available language bindings.	
Related Information	gLite LFC [R 6]	
Revision Log		

20.1.2 LFC Functionality

Directory Management		
ID	**METADATA_LFC_FUNC_1**	
Description	LFC Metadata Catalogue Appliances must allow users to organize the files in directories.	
Mandatory	YES	
Applicability	LFC Metadata Catalogue Appliances	
Input from Technology Provider	Support for directory management operations.	
Test Description	**Pre-condition**	Valid user credentials. Available Catalogue server.
	Test	Create new directory.
	Expected Outcome	New directory is created at server.
	Pre-condition	Valid user credentials. Available Catalogue server. Existing directory
	Test	List contents of directory.
	Expected Outcome	Contents of directory are returned.
	Pre-condition	Valid user credentials. Available Catalogue server. Existing empty directory
	Test	Remove directory.
	Expected Outcome	Directory is removed.
	Pre-condition	Valid user credentials. Available Catalogue server. Existing non-empty directory
	Test	Remove directory.
	Expected Outcome	Directory is not removed. Message is shown.
Pass/Fail Criteria	Pass if the Appliance provides support for managing directories.	
Related Information	gLite LFC [R 6]	
Revision Log		

ACL Operations		
ID	**METADATA_LFC_FUNC_2**	
Description	LFC Metadata Catalogue Appliances must allow users to set permissions on the entries.	
Mandatory	YES	
Applicability	LFC Metadata Catalogue Appliances	

Input from Technology Provider	Support for ACL management of LFC.	
Test Description	**Pre-condition**	Valid user credentials. Available LFC server. Existing entry
	Test	Show entry owner and permission
	Expected Outcome	Entry owner and permission are returned.
	Pre-condition	Valid user credentials with administrator privileges. Available LFC server. Existing entry.
	Test	Change owner of entry. Show entry owner.
	Expected Outcome	Owner of entry is changed and returned.
	Pre-condition	Valid user credentials with administrator privileges. Available LFC server. Existing entry.
	Test	Change group of entry. Show entry group.
	Expected Outcome	Group of entry is changed and returned.
	Pre-condition	Valid user credentials. Available LFC server. Existing entry.
	Test	Check the entry ACL is enforced.
	Expected Outcome	The permissions of entry are correctly enforced.
Pass/Fail Criteria	Pass if the Appliance provides support for managing ACL on catalogue entries.	
Related Information	gLite LFC [R 6]	
Revision Log		

Entry Comments	
ID	**METADATA_LFC_FUNC_3**
Description	LFC Metadata Catalogue Appliances must allow users to set comments on the catalogue entries.
Mandatory	YES
Applicability	LFC Metadata Catalogue Appliances

Input from Technology Provider	Support for the comment management of LFC	
Test Description	**Pre-condition**	Valid user credentials. Available LFC server. Existing entry
	Test	Set comment of an entry. Show comment to entry.
	Expected Outcome	The comment is correctly set and shown.
	Pre-condition	Valid user credentials. Available LFC server. Existing entry with comment.
	Test	Delete comment of an entry. Show comment to entry.
	Expected Outcome	The comment is correctly removed and nothing is shown.
Pass/Fail Criteria	Pass if the Appliance provides support for managing comments on catalogue entries.	
Related Information	gLite LFC [R 6]	
Revision Log		

User/Group Map Management		
ID	**METADATA_LFC_FUNC_4**	
Description	LFC Metadata Catalogue Appliances must allow the definition and management of user and group maps.	
Mandatory	YES	
Applicability	LFC Metadata Catalogue Appliances	

Input from Technology Provider	Support for the user/group management of LFC.	
Test Description	**Pre-condition**	Valid admin user credentials. Available LFC server.
	Test	List all user/group mappings
	Expected Outcome	List of all user/group mappings is shown.
	Pre-condition	Valid admin user credentials. Available LFC server.
	Test	List user mappings for specific user DN.
	Expected Outcome	List of user mappings is shown.
	Pre-condition	Valid admin user credentials. Available LFC server.
	Test	List group mappings for specific group name.
	Expected Outcome	List of group mapping is shown.
	Pre-condition	Valid admin user credentials. Available LFC server. Non existing user/group mapping.
	Test	Set new user/group mapping. List the user/group mapping.
	Expected Outcome	New mapping is set and shown accordingly.
	Pre-condition	Valid admin user credentials. Available LFC server. Existing user/group mapping.
	Test	Set new user/group mapping for a user/group. List the user/group mapping.
	Expected Outcome	New mapping is set and shown accordingly.
	Pre-condition	Valid admin user credentials. Available LFC server. Existing user/group mapping.
	Test	Remove user/group mapping for a user/group. List the user/group mapping.
	Expected Outcome	Mapping is removed and not shown.
Pass/Fail	Pass if the Appliance provides support for managing the mapping of users and	

Criteria	groups.
Related Information	gLite LFC [R 6]
Revision Log	

Entry Management		
ID	**METADATA_LFC_FUNC_5**	
Description	LFC Metadata Catalogue Appliances must allow users to create entries and to manage those entries.	
Mandatory	YES	
Applicability	LFC Metadata Catalogue Appliances	

Input from Technology Provider	Support for the entry management operations.	
Test Description	**Pre-condition**	Valid user credentials. Available Catalogue server. Available SE with file to register.
	Test	Create new entry (register file in server).
	Expected Outcome	New entry is created at server. GUID is returned
	Pre-condition	Valid user credentials. Available Catalogue server with existing entry. Available SE to register replica
	Test	Register new replica of the file in a new SE
	Expected Outcome	Entry is updated with the new replica
	Pre-condition	Valid user credentials. Available Catalogue server. Existing entry
	Test	List replicas of entry.
	Expected Outcome	Replica list is returned.
	Pre-condition	Valid user credentials. Available Catalogue server. Existing entry.
	Test	Remove one of the entry replicas
	Expected Outcome	Replica is removed. If it was the last one, remove also the entry.
	Pre-condition	Valid user credentials. Available Catalogue server. Existing entry.
	Test	Remove entry.
	Expected Outcome	Entry is removed (with all replicas)
Pass/Fail Criteria	Pass if the Appliance provides support for managing entries.	
Related Information	gLite LFC [R 6]	
Revision Log		

20.2 AMGA Implementation

20.2.1 AMGA Interface

AMGA Soap Interface	
ID	**METADATA_AMGA_API_1**
Description	AMGA Metadata Catalogue Appliances must implement the complete AMGA WSDL API [**¡Error! No se encuentra el origen de la referencia.**]
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the AMGA SOAP API. Any deviation from the API should be documented. Ideally, provide a complete test suite that includes tests for all the functionality.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all functionality of AMGA WSDL, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	Pass if the AMGA WSDL API is tested and works as documented.	
Related Information	gLite AMGA [R 7]	
Revision Log		

AMGA Streaming Interface	
ID	**METADATA_AMGA_API_2**
Description	AMGA Metadata Catalogue Appliances must implement the complete AMGA streaming API [**¡Error! No se encuentra el origen de la referencia.**]
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the AMGA Streaming API. Any deviation from the API should be documented. Ideally, provide a complete test suite that includes tests for all the functionality.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all functionality of AMGA Stream protocol, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	Pass if the API is tested and working as documented for all the available language bindings.	
Related Information	gLite AMGA [R 7]	
Revision Log		

20.2.2 AMGA Functionality

AMGA Streaming Interface	
ID	**METADATA_AMGA_FUNC_1**
Description	AMGA Metadata Catalogue Appliances must allow users to organize the files in directories.
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the directory management operations of AMGA.	
Test Description	**Pre-condition**	Valid user credentials. Available AMGA server.
	Test	Create new directory.
	Expected Outcome	New directory is created at AMGA server.
	Pre-condition	Valid user credentials. Available AMGA server. Existing directory
	Test	List contents of directory.
	Expected Outcome	Contents of directory are returned.
	Pre-condition	Valid user credentials. Available AMGA server. Existing empty directory
	Test	Remove directory.
	Expected Outcome	Directory is removed.
	Pre-condition	Valid user credentials. Available AMGA server. Existing non-empty directory
	Test	Remove directory.
	Expected Outcome	Directory is not removed. Message is shown.
	Pre-condition	Valid user credentials. Available AMGA server. Existing directory (different to current)
	Test	Change current directory to existing directory. Check current directory.
	Expected Outcome	Current directory has changed
Pass/Fail Criteria	Pass if users can manage directories in the server.	
Related Information	gLite AMGA [R 7]	

Revision Log	

Entry Management	
ID	**METADATA_AMGA_FUNC_2**
Description	AMGA Metadata Catalogue Appliances must allow users to manage the entries in the server.
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the entry management operations of AMGA.	
Test Description	**Pre-condition**	Valid user credentials. Available AMGA server.
	Test	Create a new entry. List entry's attributes
	Expected Outcome	Entry is created. The attributes are listed correctly.
	Pre-condition	Valid user credentials. Available AMGA server.
	Test	Create a new set of entries. List entries' attributes
	Expected Outcome	Entries are created. The attributes are listed correctly.
	Pre-condition	Valid user credentials. Available AMGA server. Existing entry.
	Test	Remove existing entry. List entry's attributes
	Expected Outcome	Entry is removed. The list command exits with an error.
Pass/Fail Criteria	Pass if users can manage entries in the server.	
Related Information	gLite AMGA [R 7]	
Revision Log		

Attribute Management	
ID	**METADATA_AMGA_FUNC_3**
Description	AMGA Metadata Catalogue Appliances must allow users to manage the attributes in the server.
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the attribute management operations of AMGA.	
Test Description	**Pre-condition**	Valid user credentials. Available AMGA server.
	Test	Add new attribute to directory. List directory attributes
	Expected Outcome	Attribute is added. List returns all attributes of directory.
	Pre-condition	Valid user credentials. Available AMGA server. Existing attributes for dir/entry
	Test	Remove attribute to from dir/entry. List dir/entry attributes
	Expected Outcome	Attribute is removed. List does not return removed attribute.
	Pre-condition	Valid user credentials. Available AMGA server. Existing attribute list for file
	Test	Clear attribute list for a file. Get file's attributes.
	Expected Outcome	All file's attributes are set to NULL. Attributes values are shown.
	Pre-condition	Valid user credentials. Available AMGA server. Entry with attribute list.
	Test	Clear attribute list for a file. List file's attributes
	Expected Outcome	Attribute list file. They are listed correctly.
Pass/Fail Criteria	Pass if users can manage the attributes for the entries in the server.	
Related Information	gLite AMGA [R 7]	
Revision Log		

Metadata Queries	
ID	**METADATA_AMGA_FUNC_4**
Description	AMGA Metadata Catalogue Appliances must allow users to find and update entries based on their metadata.
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for the metadata queries in AMGA.	
Test Description	**Pre-condition**	Valid user credentials. Available AMGA server.
	Test	Test the complete functionality (find, update, select) of the metadata queries in AMGA. Test available functions
	Expected Outcome	Queries work as expected.
Pass/Fail Criteria	Pass if the metadata queries are supported as documented.	
Related Information	gLite AMGA [R 7] AMGA Metadata Queries [R 10]	
Revision Log		

Attribute Management	
ID	**METADATA_AMGA_FUNC_5**
Description	AMGA Metadata Catalogue Appliances must allow users to set permissions on the entries.
Mandatory	YES
Applicability	AMGA Metadata Catalogue Appliances

Input from Technology Provider	Support for ACL related operations of AMGA.	
Test Description	**Pre-condition**	Valid user credentials. Available AMGA server.
	Test	Get current user.
	Expected Outcome	Current user is returned.
	Pre-condition	Valid user credentials. Available AMGA server. Existing entry/dir
	Test	Show entry/dir owner and permission
	Expected Outcome	Entry/dir owner and permission are returned.
	Pre-condition	Valid user credentials. Available AMGA server. Existing entry/dir
	Test	Change owner of entry/dir. Show entry/dir owner.
	Expected Outcome	Owner of entry/dir is changed and returned.
	Pre-condition	Valid user credentials. Available AMGA server. Existing entry/dir
	Test	Change entry/dir permissions. Check the permission is enforced.
	Expected Outcome	The permissions of entry/dir are changed and correctly enforced.
Pass/Fail Criteria	Pass if users can manage the ACLs of the entries in the server.	
Related Information	gLite AMGA [R 7]	
Revision Log		

21 FILE ENCRYPTION/DECRYPTION

Criteria for the File Encryption/Decryption Capability are based on gLite Hydra [R 37] as reference implementation. A key handling interface will be described in future versions of the roadmap following input from the EGI Community.

21.1 Key Management

Key Registration	
ID	**FILECRYPT_KEY_1**
Description	Hydra appliances must allow registering and unregistering keys.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.

Input from Technology Provider	Support for key registration/unregistration.	
Test Description	**Pre-condition**	Keystore running accepted user credentials.
	Test	Register key in server
	Expected Outcome	Key is successfully registered
	Pre-condition	Keystore running accepted user credentials.
	Test	Register key in server specifying cipher and key length.
	Expected Outcome	Key is successfully registered
	Pre-condition	Keystore running previously registered key, accepted user credentials.
	Test	Register key in server
	Expected Outcome	Warning issued, no action taken.
	Pre-condition	Keystore running previously registered key, accepted user credentials.
	Test	Unregister key in server
	Expected Outcome	Key is successfully unregistered
	Pre-condition	Keystore running, non-registered key, accepted user credentials.
	Test	Unregister key in server
	Expected Outcome	Warning message issued, no action taken.
Pass/Fail Criteria	Pass if the registration and unregistration of keys in the appliance work as expected.	

Related Information	Hydra [R 37]
Revision Log	V3: Improved wording.

Key and Password Splitting and Recombination		
ID	**FILECRYPT_KEY_2**	
Description	Hydra appliances must provide functionality for generating, splitting and recombine keys and passwords.	
Mandatory	YES	
Applicability	Hydra File Encryption/Decryption Appliances.	

Input from Technology Provider	Support for split and joining password and keys.	
Test Description	**Pre-condition**	Password/Key to split
	Test	Split password/key.
	Expected Outcome	Password is successfully splitted
	Pre-condition	Whole set of Password/key splits
	Test	Join splits
	Expected Outcome	Password/key successfully joined.
	Pre-condition	Minimum number of Password/key splits needed for joining.
	Test	Join splits
	Expected Outcome	Password/key successfully joined.
Pass/Fail Criteria	Pass if the split/join of password and keys functionality is provided. The tests should include different combination of number of parts and minimum number of parts needed for recombinations.	
Related Information	Hydra [R 37]	
Revision Log	V3: Improved wording.	

Key ACL management		
ID	**FILECRYPT_KEY_3**	
Description	Hydra appliances must allow the management of ACLs for a file/key.	
Mandatory	YES	
Applicability	Hydra File Encryption/Decryption Appliances.	

Input from Technology Provider	Support for ACL management of keys and keys set.	
Test Description	**Pre-condition**	Key registered in server, user allowed to list ACLs of key
	Test	List key ACLs
	Expected Outcome	ACLs of file correctly shown.
	Pre-condition	Key registered in server, user allowed to modify ACLs of key
	Test	Set new ACL for key.
	Expected Outcome	ACL changed correctly.
	Pre-condition	Key registered in server, ACL of key set.
	Test	Try allowed actions for ACL.
	Expected Outcome	Actions are performed correctly
	Pre-condition	Key registered in server, ACL of key set.
	Test	Try non-allowed actions for ACL.
	Expected Outcome	Actions are not allowed.
Pass/Fail Criteria	Pass if the ACLs can be listed and set. They are correctly enforced for actions.	
Related Information	Hydra [R 37]	
Revision Log	V3: Improved wording.	

21.2 File Encryption/Decryption

File Encryption/Decryption	
ID	**FILECRYPT_FILE_1**
Description	Hydra appliances must provide encryption and decryption of files functionality.
Mandatory	YES
Applicability	Hydra File Encryption/Decryption Appliances.

Input from Technology Provider	Support for file encryption and decryption.	
Test Description	**Pre-condition**	Existing file, key registered.
	Test	Encrypt and decrypt existing file.
	Expected Outcome	Result of the test is identical to original file.
Pass/Fail Criteria	Pass if the encryption/decryption of files functionality is provided.	
Related Information	Hydra [R 37]	
Revision Log	V3: Improved wording.	

File Encryption/Decryption into grid storage		
ID	**FILECRYPT_FILE_2**	
Description	Hydra appliances must allow storage of encrypted files into grid storage system and the retrieval and decryption of those files.	
Mandatory	YES	
Applicability	Hydra File Encryption/Decryption Appliances.	

Input from Technology Provider	Support for file encryption and decryption into grid storage (SRM).	
Test Description	**Pre-condition**	Existing file, available grid storage.
	Test	Encrypt and store file into grid storage, retrieval and decryption of file.
	Expected Outcome	Result of the test is identical to original file. Grid storage contains encrypted file.
	Pre-condition	Encrypted file stored in grid storage.
	Test	Retrieve file, decrypt file.
	Expected Outcome	File is correctly retrieved and decrypted.
Pass/Fail Criteria	Pass if the encryption/decryption of files into grid storage functionality is provided.	
Related Information	Hydra [R 37]	
Revision Log	V3: Improved wording.	

22 FILE ACCESS

Provides an abstraction that allows a file to be stored on or retrieved from a storage device (e.g. tape, disk, distributed file system, etc.) for use elsewhere in the infrastructure.

22.1 File Access Interface

POSIX Read file access	
ID	**FILEACC_API_1**
Description	Provide genuine POSIX read file access.
Mandatory	NO
Applicability	File Access Interface.

Input from Technology Provider	Support for the POSIX read file access: opening and reading files.	
Test Description	**Pre-condition**	POSIX access configured and available for user.
	Test	POSIX read file operations tests.
	Expected Outcome	POSIX file operations work as documented. Log of operations
Pass/Fail Criteria	Pass if POSIX access to files is provided.	
Related Information	UMD Roadmap [R 1] #1386: EMI Data clients should be able to offer the file:// protocol to SRM	
Revision Log	V2: changed to READ only access, and not mandatory.	

POSIX Write file access	
ID	**FILEACC_API_2**
Description	Provide genuine POSIX write file access.
Mandatory	NO
Applicability	File Access Interface.

Input from Technology Provider	Support for the POSIX file access: open (creating files), and write/append operations on files.	
Test Description	**Pre-condition**	POSIX access configured and available for user.
	Test	POSIX file write operations tests.
	Expected Outcome	POSIX file operations work as documented. Log of operations
Pass/Fail Criteria	Pass if POSIX write access to files is provided.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

23 FILE TRANSFER

23.1 File Transfer Interfaces

GridFTP File Access	
ID	**FILETRANS_API_1**
Description	Provide gridFTP access for reading data.
Mandatory	YES
Applicability	GridFTP File Transfer Appliances.

Input from Technology Provider	Support for reading and writing data from the Storage Resource using gridFTP.	
Test Description	**Pre-condition**	Valid credentials.
	Test	Transfer files via gridFTP protocol (both read and write operations)
	Expected Outcome	Files can be transferred. Log of operations
Pass/Fail Criteria	Pass if gridFTP access to files is provided.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

HTTPS File Access	
ID	**FILETRANS_API_2**
Description	Provide HTTP(S) access for reading data.
Mandatory	YES
Applicability	HTTPS File Transfer Appliances.

Input from Technology Provider	Support for reading data from the Storage Resource using http(s)	
Test Description	**Pre-condition**	Valid credentials.
	Test	Transfer files via HTTP(s) protocol.
	Expected Outcome	Files can be transferred. Log of operations
Pass/Fail Criteria	Pass if HTTP(s) read access to files is provided.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

WebDAV File Access	
ID	**FILETRANS_API_3**
Description	Provide WebDAV access for data.
Mandatory	YES
Applicability	WebDAV File Transfer Appliances.

Input from Technology Provider	Support for reading and writing data from the Storage Resource using WebDAV.	
Test Description	**Pre-condition**	Valid credentials.
	Test	Transfer files via WebDAV protocol (both read and write operations)
	Expected Outcome	Files can be transferred. Log of operations
Pass/Fail Criteria	Pass if WebDAV read access to files is provided.	
Related Information	UMD Roadmap [R 1]	
Revision Log		

24 FILE TRANSFER SCHEDULING

These criteria are defined taking gLite FTS [R 38] as reference implementation.

24.1 File Transfer Channel Management

Channel Management Operations	
ID	**FILETRANSFSCH_CHANNEL_1**
Description	FTS must allow administrators to add, drop and list channels for file transfers.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.

Input from Technology Provider	Support for channel management operations: add, drop and list channels for various sites. Support for setting the channel configuration.	
Test Description	**Pre-condition**	Valid administrator credentials. Valid Site A and B.
	Test	Add transfer channel from site A to site B
	Expected Outcome	New transfer channel created.
	Pre-condition	Valid administrator credentials. Existing channel
	Test	Drop channel.
	Expected Outcome	Channel is dropped.
	Pre-condition	Valid administrator credentials.
	Test	List available channels
	Expected Outcome	List of available channels is shown.
	Pre-condition	Valid administrator credentials. Existing channel.
	Test	Set channel configuration (bandwidth, transfer limit per VO, …)
	Expected Outcome	Channel configuration is effectively changed.
Pass/Fail Criteria	Pass if administrator can manage the channels correctly.	
Related Information	gLite FTS [R 38]	
Revision Log	V3: Improved wording.	

Channel Manager Control	
ID	**FILETRANSFSCH_CHANNEL_2**
Description	FTS must allow administrators to control who is allowed or not to manage a channel.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.

Input from Technology Provider	Support for channel manager control operations: add/remove channel managers and listing current channels.	
Test Description	**Pre-condition**	Valid administrator credentials. Existing channel. Credentials of user to add as manager
	Test	Add user as manager of channel. Test privilege operations on channel with user.
	Expected Outcome	Manager is added; privileged operations are performed correctly.
	Pre-condition	Valid administrator credentials. Existing channel.
	Test	List channel managers
	Expected Outcome	List of channel managers is returned
	Pre-condition	Valid administrator credentials. Existing channel. Existing manager of channel
	Test	Remove channel manager. Test privilege operations on channel with user
	Expected Outcome	Manager is removed; privileged operations are not performed.
Pass/Fail Criteria	Pass if administrator can list and change the channel managers. The manager access is correctly enforced.	
Related Information	gLite FTS [R 38]	
Revision Log	V3: Improved wording.	

24.2 File Transfer Management

File Transfer Operation Management		
ID	**FILETRANSFSCH_ MGMT _1**	
Description	FTS must allow users to create and manage file transfer operations.	
Mandatory	YES	
Applicability	FTS File Transfer Scheduling Appliances.	

Input from Technology Provider	Support for submission, query and cancelling file transfer operations.	
Test Description	**Pre-condition**	FTS Service available; source and destination available; list of files to transfer; valid user credentials
	Test	Create new file transfer job.
	Expected Outcome	New file transfer job created. ID of job returned.
	Pre-condition	Transfer job ID of a previously submitted job; valid user credentials.
	Test	Check status of job.
	Expected Outcome	Status of job returned.
	Pre-condition	Transfer job ID of a previously submitted job; valid user credentials.
	Test	Cancel job.
	Expected Outcome	Job is cancelled.
	Pre-condition	Transfer job ID of a previously submitted job; valid user credentials.
	Test	Cancel job.
	Expected Outcome	Job is cancelled.
Pass/Fail Criteria	Pass if users can create and manage transfer jobs.	
Related Information	gLite FTS [R 38]	
Revision Log	V3: Improved wording.	

End to end file transfer operation	
ID	**FILETRANSFSCH_ MGMT _2**
Description	FTS must execute correctly file transfer operations.
Mandatory	YES
Applicability	FTS File Transfer Scheduling Appliances.

Input from Technology Provider	End-to-end file transfer operation are performed correctly, if errors are found they are clearly indicated.	
Test Description	**Pre-condition**	FTS Service available; source and destination available; list of files to transfer; valid user credentials
	Test	Create new file transfer job.
	Expected Outcome	New file transfer job created and executed correctly.
Pass/Fail Criteria	Pass if users can create jobs and the jobs are executed correctly.	
Related Information	gLite FTS [R 38]	
Revision Log	V3: Improved wording.	

25 STORAGE MANAGEMENT

25.1 SRM Interface

SRM API Support	
ID	**STORAGE_API_1**
Description	Storage Management Appliances must provide support for SRM2.2 specification.
Mandatory	YES
Applicability	Storage Management Appliances

Input from Technology Provider	Valid SRM v2.2 API implementation, any deviations from the API implementation should be documented. Ideally, also provide a complete test suite and results for the API support	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test SRMv2.2 functionality, with correct/incorrect input and with valid and invalid credentials. Use S2 [R 40] test suite for reference.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	Pass if SRM v2.2 support is provided (as tested with S2 test suite). If the API is not completely supported, this should be documented.	
Related Information	UMD Roadmap [R 1] SRM v2.2 [R 39]	
Revision Log	V3: Improved wording	

LCG-UTILS test	
ID	**STORAGE_API_2**
Description	Test Storage Management Appliances with the lcg-utils commands.
Mandatory	YES
Applicability	Storage Management Appliances

Input from Technology Provider	Support for lcg-utils [R 42] commands, documentation of any possible incompatibilities with other Appliances.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test lcg-utils commands, with correct/incorrect input and with valid and invalid credentials. An example test suite is available at [R 43]
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	Pass if lcg-utils commands can be executed correctly against the Storage Management Appliance. In the case of incompatibilities or collateral effects they must be documented.	
Related Information	Although all Storage Management Appliances should use SRM [R 39] protocol, deficiencies in the protocol description had lead to different implementations and results. This tests intends to harmonize results at least when using lcg-utils, and until a complete and better description of SRM protocol and desired results is reached.	
Revision Log	V3: Added reference	

25.2 Storage Device Support

The Storage Management Capability provide an abstraction to a Storage Device, these QC refer to the interaction of the Storage Management Capability implementation with the underlying storage device. Storage Management Capabilities are expected to support the most common file systems and storage devices used in the current EGI infrastructure.

Information retrieval	
ID	**STORAGE_DEVICE_1**
Description	The Storage Management Capability must be able to provide information from the underlying storage and make it available to an Information Discovery Appliance.
Mandatory	YES
Applicability	Storage Management Appliances

Input from Technology Provider	Information retrieval mechanisms that generate the Storage Element related entities of the current UMD Information Model Capability (GlueSchema 1.3/GlueSchema 2) using the actual information of the underlying available storage.	
Test Description	**Pre-condition**	Configured system.
	Test	Retrieve current status from storage.
	Expected Outcome	All the mandatory Storage Element related entities of GlueSchema using the **actual** information are generated.
Pass/Fail Criteria	Pass if the information retrieval mechanisms are able to generate the requested information.	
Related Information		
Revision Log		

Fine grained authorization	
ID	**STORAGE_DEVICE_2**
Description	The Storage Management Capability must allow the implementation of a fine-grained authorization policy based on VO roles and enforce it (if defined).
Mandatory	NO
Applicability	Storage Management Appliances

Input from Technology Provider	Support for fine-grained authorization policy based on VO roles. Such authorization policy can be configured and applied to the full directory tree of the storage area or just to a fraction of the storage area directory tree.	
Test Description	**Pre-condition**	Configured system with a storage resource area directory tree with different authorization permissions along the directory tree for different VO roles.
	Test	Test I/O storage operations (write, copy, delete files) using SRM interface and LCG-UTILS in a storage space area directory using different VO roles in the FQAN.
	Expected Outcome	Log of the operation is performed. A user with a valid credential and invoking an authorized VO role should be able to write/delete or read/copy files from a given storage area, according to the defined policies.
Pass/Fail Criteria	Pass if a user can interact with the storage area tree in compliance with the defined fine-grained authorization policy based on the user VO roles.	
Related Information		
Revision Log		

Space reservations		
ID	**STORAGE_DEVICE_3**	
Description	The Storage Management Capability must allow the implementation of (virtual or real) reserved space areas as storage space tokens	
Mandatory	NO	
Applicability	Storage Management Appliances	

Input from Technology Provider	Support for (virtual or real) storage space reservations enabled as storage space tokens. Interactions with the storage areas represented by a given space token must be enforced to respect the defined fine-grained authorization policy. The storage resource information system must reflect the existence of storage space tokens (if configured).	
Test Description	**Pre-condition**	Configured system with (virtual or real) storage space reservations enabled as storage space tokens.
	Test	Retrieve current status from the storage space token area.
	Expected Outcome	All the mandatory Storage Element related entities of GlueSchema using the **actual** information for the storage space token area are generated.
	Pre-condition	Configured system with (virtual or real) storage space reservations enabled as storage space tokens.
	Test	Test I/O storage operations (write files, copy files, delete files) using SRM interface and LCG-UTILS in a storage space reservation area using a valid and invalid credential.
	Expected Outcome	Log of the operation is performed. A user with a valid credential should be able to copy and retrieve files from the storage space token area.
Pass/Fail Criteria	Pass if a user can interact with the storage space token area in compliance with the fine-grained authorization policies (STORAGE_DEVICE_2); if the storage space token area information is updated in the storage information system; and if all operations are properly logged.	
Related Information		
Revision Log		

Checksum	
ID	**STORAGE_DEVICE_4**
Description	The Storage Management Capability must support Adler32 checksum calculation and store the checksum value for a given file.
Mandatory	NO
Applicability	Storage Management Appliances

Input from Technology Provider	Support for storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.	
Test Description	**Pre-condition**	Configured system with checksum computation option enabled.
	Test	Test storing/retrieving/listing a file in a storage resource through the SRM interface or LCG-UTILS enabling the checksum computation.
	Expected Outcome	Files checksum values are computed while storing a file. The checksum values are computed and compared at source and destiny to detect file corruptions. The checksum value for a file is accessible via SRM interface or LCG-UTILS listing functions.
Pass/Fail Criteria	Pass if a user is able to store/retrieve/list a file in a storage resource through SRM interface or LCG-UTILS, and that the checksum value for the file was corrected computed and delivered.	
Related Information		
Revision Log		

26 REMOTE INSTRUMENTATION

There are no standardised interfaces known for the Remote Instrumentation Capability. The QC in this document is based in the Instrument Element [R 21] proprietary implementation from DORII [R 22] project.

Instrument Element API	
ID	**INSTRUMENT_IE_1**
Description	Instrument Element appliances must support the Instrument Element API
Mandatory	YES
Applicability	Instrument Element implementation of Remote Instrumentation Appliances

Input from Technology Provider	Support for the Instrument Element API as described in WSDL. Any missing functionality/deviation from the WSDL must be documented. Ideally, provide a test suite that covers all documented functions.	
Test Description	**Pre-condition**	Valid user credentials.
	Test	Test all interface functionality, with correct/incorrect input and with valid and invalid credentials.
	Expected Outcome	Log of all the operations performed. All the documented functions work as documented.
Pass/Fail Criteria	The Instrument Element Appliance passes complete tests of its SOAP interface. The test suite must be executed without errors. For all functions, check both correct and invalid input. Invalid output should throw an exception as documented. Test also with valid and invalid credentials. Invalid credentials should throw security related exceptions.	
Related Information	UMD Roadmap [R 1] Instrument Element [R 21]	
Revision Log	V3: Improved wording.	

Instrument Element File Access	
ID	**INSTRUMENT_IE_2**
Description	Instrument Element appliances should provide a file access transfer capability for moving data in and out of the instrument.
Mandatory	YES
Applicability	Instrument Element implementation of Remote Instrumentation Appliances

Input from Technology Provider	File access transfer capability for reading and writing data, preferably gridFTP.
Pass/Fail Criteria	The Instrument Appliance must provide a file access capability for transferring data from and to the product.
Related Information	UMD Roadmap [R 1] Instrument Element [R 21] File Access QC
Revision Log	

Instrument Element Messaging System	
ID	**INSTRUMENT_IE_3**
Description	Instrument Element appliances should provide a messaging system for asynchronous monitoring of instrument variables and signalling alarms and events to the users.
Mandatory	YES
Applicability	Instrument Element implementation of Remote Instrumentation Appliances

Input from Technology Provider	Messaging capability implementation for the asynchronous monitoring and notification of alarms and events to users, preferably JMS implementation.
Pass/Fail Criteria	The Instrument Appliance must provide a messaging capability for asynchronous monitorisation and notification of events.
Related Information	UMD Roadmap [R 1] Instrument Element [R 21] Messaging Capability QC
Revision Log	

Instrument Manager Support	
ID	**INSTRUMENT_IE_4**
Description	Instrument Element appliances must provide mechanisms for managing instruments.
Mandatory	YES
Applicability	Instrument Element implementation of Remote Instrumentation Appliances

Input from Technology Provider	Implementation of the Instrument Manager (IM) framework as described in the Instrument Element documentation (XML description of the instrument and abstract classes for the implementation).
Pass/Fail Criteria	The Instrument Appliance must completely support the Instrument Manager framework as described in the Instrument Element documentations. The framework must provide a way to define attributes read from the instrument, configuration parameters for the instrument, the different commands the instrument may receive and the states and transitions of the instrument.
Related Information	UMD Roadmap [R 1] Instrument Element [R 21]
Revision Log	

27 MONITORING CAPABILITY

This section documents the Specific Quality Criteria for the monitoring system (NAGIOS) and the web portal to check the results.

27.1 Nagios Configuration Generation

Generation of Nagios Configuration Files	
ID	**MON_NCG_1**
Description	The NCG must be able to generate a correct configuration for Nagios that includes all the hosts and services to be monitored.
Mandatory	YES
Applicability	Nagios Configuration Generator (NCG) component.

Input from Technology Provider	Support for the automatic generator of configuration files for Nagios: /etc/nagios and /etc/nagios/wlcg.d/* files must be generated based on the information gathered from the nformation gathered from GOCDB.	
Test Description	**Pre-condition**	Configured system.
	Test	Generate Nagios configuration files according to the information available in the databases.
	Expected Outcome	Working Nagios configuration files.
Pass/Fail Criteria	Pass if the automatic generation of configuration files works.	
Related Information	NCG [R 28]	
Revision Log		

Generation of Failover Nagios Configuration	
ID	**MON_NCG_2**
Description	The NCG must allow a redundant service configuration for Nagios that includes failover capability.
Mandatory	YES
Applicability	Nagios Configuration Generator (NCG) component.

Input from Technology Provider	Support for the automatic generation of configuration files for Nagios with redundant services: • Several WMS • Robot certificates • Several VOs and VOMSES	
Test Description	**Pre-condition**	Configured system.
	Test	Generate Nagios configuration files according to the information available in the databases.
	Expected Outcome	Working Nagios redundant configuration files using failover services.
Pass/Fail Criteria	Pass if the redundant services are configured and used correctly.	
Related Information	NCG [R 28]	
Revision Log		

27.2 Visualization Portal (MyEGI)

Resource Summary View	
ID	**MON_PORTAL_1**
Description	Provide a view of the summary status of resources.
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Summary view in visualization portal that provides the following basic information: • Site of the resource • Resource name • Type of service • Current status • Link to detailed and historical views • Use colors to display the status of the resource.
Test Description	**Pre-condition** Configured system. **Test** Browse the summary view of resources. **Expected Outcome** All requested information is provided
Pass/Fail Criteria	Pass if the resource summary view is provided for any selected resource with all the information specified above.
Related Information	MyEGI Portal [R 29]
Revision Log	

Resource Detail View	
ID	**MON_PORTAL_2**
Description	Provide a view of the detailed status of resources.
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Detailed view of the current status for resources that shows the results of the last execution of all the probes. Include all information requested in the summary view plus: • List of probes executed • Detailed results of probes • Last execution time for probe • Link to historical view
Test Description	**Pre-condition** Configured system. **Test** Browse the detailed view of resources. **Expected Outcome** All requested information is provided
Pass/Fail Criteria	Pass if the detailed view is provided for any selected resource with all the information specified above.
Related Information	MyEGI Portal [R 29]
Revision Log	

Resource Historical View	
ID	**MON_PORTAL_3**
Description	Provide a view of the historical status of resources.
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Historical view of the probes executed at resources. Show graphically in a timeline the results for the probes. For any given probe show the detailed view fields when selected.	
Test Description	**Pre-condition**	Configured system.
	Test	Browse the historical view of resources.
	Expected Outcome	All requested information is provided
Pass/Fail Criteria	Pass if the historical view is provided for any selected resource with all the information specified above.	
Related Information	MyEGI Portal [R 29]	
Revision Log		

Resource Filters	
ID	**MON_PORTAL_4**
Description	Provide ways to filter the information shown in the web interface for all the possible views of the portal.
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Provide ways to filter the information shown in the web interface for all the possible views of the portal. At least, the displayed resources should be filtered by the following constrains: • status of resource (select just one status or several) • type of service • supported VO • site which the resource belongs to • specific name of resource for historical view, range of dates which will be used for the information.	
Test Description	**Pre-condition**	Configured system.
	Test	Test the resource filters available.
	Expected Outcome	Resrouces are shown according to the filters tested.
Pass/Fail Criteria	Pass if the resource filters are provided and they work as expected.	
Related Information	MyEGI Portal [R 29]	
Revision Log		

Responsiveness	
ID	**MON_PORTAL_5**
Description	Visualization portal should provide fast response to user requests.
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Information should be displayed as soon as possible. If too much information is to be shown, the portal should use a paginated interface or dynamically load the content and provide as soon as possible a first set of results.	
Test Description	**Pre-condition**	Configured system.
	Test	Browse complex page (e.g. lots of resources)
	Expected Outcome	Page responsiveness is fast enough for navigation. Information is loaded dynamically or shown in a paged interface.
Pass/Fail Criteria	Pass if the complex pages are responsive for navigation (no more than 15 seconds for showing the first set of results)	
Related Information	MyEGI Portal [R 29]	
Revision Log		

Linkable Views	
ID	**MON_PORTAL_6**
Description	Views should have unique URLs that are independent to the user session
Mandatory	YES
Applicability	MyEGI monitoring visualization portal

Input from Technology Provider	Views should have unique URLs that are independent to the user session. These links should work for different users.	
Test Description	**Pre-condition**	Configured system.
	Test	Generate view link with user A, try it with user B
	Expected Outcome	Both users A and B get the same view results.
Pass/Fail Criteria	Views links must work for different users and/or sessions.	
Related Information	MyEGI Portal [R 29]	
Revision Log		

27.3 Database

Metric List Fetching	
ID	**MON_DB_1**
Description	The list of metrics to use in each of the services must be fetch at regular intervals from a given central location.
Mandatory	YES
Applicability	Metrics Database

Input from Technology Provider	Test of the metric fetch mechanism.	
Test Description	**Pre-condition**	Configured system.
	Test	Fetch metrics from central metric database. Generate list of updates for the current local metric database.
	Expected Outcome	Metrics are fetched correctly. A list of updates is generated.
Pass/Fail Criteria	Test must exist and execute correctly.	
Related Information		
Revision Log		

Resource List Fetching	
ID	**MON_DB_2**
Description	The list of resources to be tested should be dynamically discovered
Mandatory	YES
Applicability	Metrics Database

Input from Technology Provider	The list of resources to be tested should be dynamically discovered using the various information systems available. The list of sites to be tested meet the following requirements: • listed in the BDII • listed in the GOCDB • status in the GOCDB is Certified	
Test Description	**Pre-condition**	Configured system.
	Test	Fetch resources by quering BDII and GOCDB. List of updates to perform to the local resource DB.
	Expected Outcome	Resources are fetched correctly. A list of updates is generated.
Pass/Fail Criteria	Resource list is generates correctly according to the requirements.	
Related Information		
Revision Log		

28 MONITORING PROBES

The Monitoring Capability executes a set of probes defined by the operations community. These probes *should* be provided by the TP for each product.

Probe Template	
ID	**MON_PROBE_1**
Description	A template and documentation for the creation of new probes that can be integrated in the monitoring framework must exist.
Mandatory	YES
Applicability	Monitoring Capability

Input from Technology Provider	Template for probes and documentation for the creation and integration of probes into the framework (or link to those documents)
Pass/Fail Criteria	The QC will pass if the template and documentation is available for external developers and is usable for creating new probes.
Related Information	
Revision Log	

28.1 Service Probes

Certificate Lifetime Probe	
ID	**MON_PROBE_GENERIC_1**
Description	Provide a monitoring probe that assures that the host certificate lifetime for the service is valid.
Mandatory	NO
Applicability	All products that use host certificates

Input from Technology Provider	Certificate Validity Probe. The probe should only use the public interface of the service and run integrated in the monitoring infrastructure of EGI
Pass/Fail Criteria	The QC will pass if the TP provides with the service a probe for checking the certificate lifetime. This probe may be provided also indirectly as part of other probes.
Related Information	
Revision Log	V1.1 Added probe description. V2: Simplified description

Service Probe	
ID	**MON_PROBE_GENERIC_2**
Description	Provide monitoring probes that test the functionality of the service
Mandatory	NO
Applicability	All Services

Input from Technology Provider	Monitoring probe that tests that the service provides the expected functionality. The probe should only use the public interface of the service and run integrated in the monitoring infrastructure of EGI. The exact tests to perform for each service are determined by the operations community. For the current probes specification check the SAM documentation [R 30]
Pass/Fail Criteria	Probes must exist, they must be integrated with the EMI monitoring infrastructure and provide the expected functionality.
Related Information	SAM documentation [R 30]
Revision Log	

The criteria described in the next sections make reference to probes that are used by the EGI Operations community to monitor the Infrastructure. The specific appliances must support the execution of these probes.

28.1.1 Job Execution Capability Probes

Job Execution Probe	
ID	**MON_PROBE_JOBEXEC_1**
Description	Provide monitoring probes that test the functionality of Job Execution Capability
Mandatory	YES
Applicability	Job Execution Appliances

Input from Technology Provider	CE probes as described at: https://tomtools.cern.ch/confluence/display/SAM/CE
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

CREAM Job Execution Probe	
ID	**MON_PROBE_JOBEXEC_2**
Description	Provide monitoring probes that test the functionality of CREAM
Mandatory	YES
Applicability	CREAM Appliances

Input from Technology Provider	CREAM CE probes as described at: https://tomtools.cern.ch/confluence/display/SAM/CREAMCE-DJS
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

WN Probes	
ID	**MON_PROBE_JOBEXEC_3**
Description	Provide monitoring probes that test the correct function of Worker Nodes
Mandatory	YES
Applicability	Worker Node.

Input from Technology Provider	WN probes as described at: https://tomtools.cern.ch/confluence/display/SAM/WN.
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

28.1.2 Compute Job Scheduling Probes

WMS Probes	
ID	**MON_PROBE_JOBSCH_1**
Description	Provide monitoring probes that test the functionality of WMS.
Mandatory	YES
Applicability	WMS Job Scheduling Appliances.

Input from Technology Provider	WMS probes as described at: https://tomtools.cern.ch/confluence/display/SAM/WMS.
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

28.1.3 File Access Capability Probes

SRM Probes	
ID	**MON_PROBE_STORAGE_1**
Description	Provide monitoring probes that test the functionality of SRM.
Mandatory	YES
Applicability	Storage Management Appliances

Input from Technology Provider	SRM probes as described at: https://tomtools.cern.ch/confluence/display/SAM/SRM.
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

28.1.4 Metadata Catalogue Capability Probes

LFC Probes	
ID	**MON_PROBE_METADATA_1**
Description	Provide monitoring probes that test the functionality of LFC.
Mandatory	YES
Applicability	LFC Appliances

Input from Technology Provider	LFC probes as described at: https://tomtools.cern.ch/confluence/display/SAM/LFC.
Pass/Fail Criteria	Probes must exist and behave as expected in the probe documentation.
Related Information	SAM documentation [R 30]
Revision Log	

29 ACCOUNTING CAPABILITY

The use of resources within the e-Infrastructure must be recorded for understanding usage patterns by different user communities and by individuals within their communities.

29.1 Generation of Accounting Records

Job Execution Appliances Accounting	
ID	**ACC_JOBEXEC_1**
Description	Job Execution Appliances must generate accounting records for all the actions of the users into the local resources.
Mandatory	YES
Applicability	Accounting Appliances for Job Execution Capability (APEL)

Input from Technology Provider	The Job Execution Capability must generate accounting records for the actions of the users into the local resources (jobs submitted to the underlying execution manager). These records must include, at least, the following information for all the jobs submitted to the system: • User DN • VO • Job start execution time • Job end execution time • SPECint information • CPU & Wall Time • Number of slots/CPUs used by the job The generation of accounting records must be available for the execution managers supported by the Job Execution Capability implementations.
Test Description	**Pre-condition** Configured system. **Test** Creation of accounting records **Expected Outcome** Accounting records for the jobs submitted to the execution manager through the Capability.
Pass/Fail Criteria	Pass if the accounting records are generated correctly for all execution managers supported. The generation of the records should not compromise the availability and reliability of the system.
Related Information	
Revision Log	V4: Minor rephrasing

29.2 Accounting Store and Transmission for Job Execution Appliances.

The accounting information should be stored in a local database and transmitted in regular intervals to a central registry where information of the whole EGI infrastructure is stored.

Local Accounting Store	
ID	**ACC_STORE_1**
Description	APEL must be able to store the information collected from the execution manager in a site database.
Mandatory	YES
Applicability	Accounting Appliances

Input from Technology Provider	The accounting appliance must store the information collected from the execution manager in a site level database, where information about all the jobs executed at the site is stored. The appliance must include information for all the jobs submitted via the grid interface. The information collected for each job *should* contain the fields recommended by OGF: • ExecutingSite: Site name (example: RAL-LCG2) • LocalJobID: Local job name (example: 12311.lcgce02.gridpp.rl.ac.uk) • LCGJobID: *Optional* (default value: NULL) • LocalUserID: Local user name (example: alicesgm 001) • LCGUserID: User DN (example:/C=IT/O=INFN/OU=Personal Certificate ..) • LCGUserVO: Local user group (example: alice) • ElapsedTime: Job Wall duration (example: P8H24M47S) • BaseCpuTime: Job CPU duration (example: P8H21M34S) • ElapsedTimeSeconds: Job Wall duration in seconds (example: 3500) • BaseCpuTimeSeconds: Job CPU time duration in seconds (example: 3000) • StartTime: Job start time (example: 2010-03-14T11:06:08Z) • StopTime: Job stop time (example: 2010-03-14T19:30:55Z) • StartTimeUTC: Job start UTC time (example: 2010-03-14T11:06:08Z) • StopTimeUTC: Jobs stop UTC time (example: 2010-03-14T19:30:55Z) • StartTimeEpoch: Job start time epoch (example: 1079262368) • StopTimeEpoch: Job stop time epoch (example: 1079292655) • ExecutingCE: Submit Host (example: lcgce02.gridpp.rl.ac.uk) • MemoryReal: Used real memory (example: 769548) • MemoryVirtual: Used virtual memory (example: 1244948) • SpecInt2000: SpecInt2000 value (example: 40322) • SpecFloat2000: SpecFloat2000 value (example: 30234) • EventDate: Event record date (example: 2010-03-14) • EventTime: Event record time (example: 19:30:55)

Test Description	**Pre-condition**	Configured system. Accounting records are correctly generated.
	Test	Store accounting records into site registry.
	Expected Outcome	Accounting records are stored in the site registry. Log of operations is available.
Pass/Fail Criteria	Pass if the accounting records are stored correctly. The information contained in the records should cover the fields recommended by OGF. If any fields are missing, the verifier will decide if the information is enough or not to pass. Storage of the records should not compromise the availability and reliability of the system.	
Related Information		
Revision Log	V4: general review of criterion	

Accounting Records Transmission	
ID	**ACC_STORE_2**
Description	APEL must be able to send the records stored in the site registry to a central registry database by using a messaging system.
Mandatory	YES
Applicability	APEL Accounting Appliances.

Input from Technology Provider	Test for the transmission of records to the central registry using ActiveMQ.	
Test Description	**Pre-condition**	Configured system. Accounting records are correctly generated and stored in local registry.
	Test	Send new records to the central registry using ActiveMQ.
	Expected Outcome	Only new records are sent to central registry by default but site administrators are able also to republish accounting records in a specific interval using accounting configuration files. They are stored correctly there. Log of operations is generated.
Pass/Fail Criteria	Pass if the test is provided and passes. The transmission of the records should not compromise the availability and reliability of the system.	
Related Information		
Revision Log		

Periodic Local Registry Store	
ID	**ACC_CRON_1**
Description	The accounting appliance must periodically submit new accounting records to the local (site level) registry
Mandatory	YES
Applicability	APEL Accounting Appliances.

Input from Technology Provider	The accounting appliance must periodically submit new accounting records to the local registry. This action should be executed daily to check new executed jobs.	
Test Description	**Pre-condition**	Configured system.
	Test	Send new records to the local registry each day.
	Expected Outcome	Only new records are sent to local registry. They are stored correctly there. Accounting logs are generated locally.
Pass/Fail Criteria	Pass if the periodic update mechanism (e.g. cron) is provided and works as expected.	
Related Information		
Revision Log	V3: removed most cron references.	

Periodic Central Registry Update.	
ID	**ACC_CRON_2**
Description	The accounting appliance must periodically submit new accounting records to the global (central) registry
Mandatory	YES
Applicability	APEL Accounting Appliances.

Input from Technology Provider	Local registry must be able to submit new accounting records to global accounting registry using a message system. This action should be executed daily to check new executed jobs.	
Test Description	**Pre-condition**	Configured system.
	Test	Send new records to the global registry each day.
	Expected Outcome	Only new records are sent to global registry by default but site administrators are able also to republish accounting records in a specific interval using accounting configuration files. They are stored correctly there. Logs about the update are generated locally.
Pass/Fail Criteria	Pass if the periodic update mechanism (e.g. cron) is provided and works as expected.	
Related Information		
Revision Log	V3: removed most cron references.	

29.3 Visualization Portal

Accounting Portal Summary View	
ID	**ACC_PORTAL_1**
Description	Accounting portal must provide a front-end view of published CPU resources.
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Accounting portal provides a front-end view of published CPU resources that have been aggregated into summaries. These summaries may view per: • Site • Countries • VO • NGI • Tier1 / Tier2
Test Description	**Pre-condition** Configured accounting portal. **Test** Browse summaries. **Expected Outcome** Summary views are shown with correct data for all the possible levels.
Pass/Fail Criteria	Pass if the summary view is provided and is correctly generated for all possible levels
Related Information	EGI Accounting Portal [R 31]
Revision Log	

Accounting Portal Access Policy	
ID	**ACC_PORTAL_2**
Description	Sensitive information about VO usage and Users DNs must be encrypted and only accessible to their VO managers via X.509 certificate.
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Portal must include access policies for VO managers that restricts the information that can be accessed.	
Test Description	**Pre-condition**	Configured accounting portal. Valid VO manager certificate.
	Test	Browse VO view with VO usage and user DNs.
	Expected Outcome	Information is displayed correctly.
Pass/Fail Criteria	Pass if the access policy is applied correctly.	
Related Information	EGI Accounting Portal [R 31]	
Revision Log		

Accounting Portal Global View	
ID	**ACC_PORTAL_3**
Description	Accounting Portal views must include a production global view
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Accounting Portal views must include a production global view. This view must include a custom view where users can select how display desired accounting data, users can select these options: • Data to graph: Users can select Norm. Sum CPU in kSI2000-hours, or HEPSPEC-2006 number of jobs, Norm Sum elapsed time in kSI-2000 hours and HEPSPEC-2006 hours or CPU efficiency. • Data period to view. • Show data for Region, Date or VO and as function of Region, Date, VO or Country. • Group results by VO, Region or Date • Chart type: Accumulative bar, group bar or lines. • Scale: Linear or logarithmic. • A button to exclude operations VOs like dteam and ops. This general view must include also a list of certified sites which are not publishing accounting data since last 3 months. Accounting Portal views must include different charts and graphs for ease of use.
Test Description	**Pre-condition** Configured System. **Test** Visualize data with charts **Expected Outcome** Charts are correctly generated for the accounting data available based on users selection.
Pass/Fail Criteria	Pass if the charts are correctly generated for all the accounting data available and for all the chart models.
Related Information	EGI Accounting Portal [R 31]
Revision Log	

Accounting Portal VO Manager View	
ID	**ACC_PORTAL_4**
Description	Accounting Portal views must include a production VO manager view.
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Accounting Portal views must include a production VO manager view. This view must include a custom view where only VO managers can select and display desired accounting data, available options are: • VO to query including Group and Role. • NGI/Country to display. • Order by: Number of jobs, Norm. sum CPU, sum CPU, Norm sum time elapsed and sum. Time elapsed. • Data period to display This view generates a list with desired accounting information (including CPU efficiency for each VO group), a percentage pie chart and a bar chart for selected period of time.	
Test Description	**Pre-condition**	Configured System.
	Test	Visualize data with charts
	Expected Outcome	Charts are correctly generated for the accounting data available based on VO managers selection.
Pass/Fail Criteria	Pass if the charts are correctly generated for all the accounting data available and for all the chart models.	
Related Information	EGI Accounting Portal [R 31]	
Revision Log		

Accounting Portal VO Member View	
ID	**ACC_PORTAL_5**
Description	Accounting Portal views must include a production VO member view.
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Accounting Portal views must include a production VO member view. This view must include a custom view where only VO members can select and display desired accounting data: • VO including Group and Role. • Order by: Number of jobs, Norm. sum CPU, sum CPU, Norm sum time elapsed and sum. Time elapsed. • Data period to display. This view generates a list with desired accounting information (including CPU efficiency for each VO group), a percentage pie chart and a bar chart for selected period of time.
Test Description	**Pre-condition** Configured System. **Test** Visualize data with charts **Expected Outcome** Charts are correctly generated for the accounting data available based on VO members selection.
Pass/Fail Criteria	Pass if the charts are correctly generated for all the accounting data available and for all the chart models.
Related Information	EGI Accounting Portal [R 31]
Revision Log	

Accounting Portal Site Admin View	
ID	**ACC_PORTAL_6**
Description	Accounting Portal views must include a site admin view.
Mandatory	YES
Applicability	Accounting Portal Implementation

Input from Technology Provider	Accounting Portal views must include a production Site Admin view. This view must include a custom view where only site administrators can select and display desired accounting data for their sites, site administrator can select: • Site to display accounting data. • Order by: Number of jobs, Norm. sum CPU, sum CPU, Norm sum time elapsed and sum. Time elapsed. • Data period to display. This view generates a list with desired accounting information (including CPU efficiency for each VO group), a percentage pie chart and a bar chart for selected period of time.	
Test Description	**Pre-condition**	Configured System.
	Test	Visualize data with charts
	Expected Outcome	Charts are correctly generated for the accounting data available based on site administrators selection.
Pass/Fail Criteria	Pass if the charts are correctly generated for all the accounting data available and for all the chart models.	
Related Information	EGI Accounting Portal [R 31]	
Revision Log		

30 CLIENT TOOLS

30.1 Generic client tools criteria

Command line options coherency	
ID	**CLIENT_TOOLS_1**
Description	Client commands for the same product should have a coherent set of options.
Mandatory	NO
Applicability	Client Tools

Input from Technology Provider	Client command tools for a given product with coherent options between them (e.g. configuration file is always specified with –c option, vo with –vo option) Ideally, coherency with other product command line clients.
Pass/Fail Criteria	All the command tools for a given product must have a coherent command line options. Semantically common options for two commands must have the same syntax.
Related Information	Requirement #1780
Revision Log	

Error Messages	
ID	**CLIENT_TOOLS_2**
Description	Error messages provided by the service should be clear and facilitate the solution of those errors by users or service administrators
Mandatory	NO
Applicability	Client tools.

Input from Technology Provider	Any error in the client tools must produce a clear error message. A possible solution/cause for it should be given.
Pass/Fail Criteria	Pass if the errors provided by the client tools always produce a descriptive message. Errors without any message (unless a quiet option is specified) will make the criterion to fail. Ideally the following info is also documented/shown for all errors: • Error code • Error source (internal module or remote resource (specify it explicitly)) • Cause of error (syntax error, module malfunctioning, configuration problem, network error, other (specify it explicit)) • Type (critical, informative) • Possible solution
Related Information	Requirements gathered in MS305 related to resubmission of jobs, and information provided in error messages.
Revision Log	

31 CLIENT API

SAGA API Support	
ID	**CLIENT_API_1**
Description	Client Appliances should be “SAGA compliant” implementations of the SAGA API
Mandatory	YES
Applicability	Client API Appliances

Input from Technology Provider	A Client API Capability implementations that follows the SAGA API specification, and the language binding(s) for its respective programming language(s), both syntactically and semantically.
Pass/Fail Criteria	The Client API Appliance provides “SAGA compliant” implementations or “partially SAGA compliant” implementations as defined in the SAGA API specification.
Related Information	SAGA API [R 19][R 20]
Revision Log	

Middleware Bindings	
ID	**CLIENT_API_2**
Description	Technology Providers provide middleware bindings for accessing their products through SAGA
Mandatory	NO
Applicability	Client API Appliances

Input from Technology Provider	SAGA-adaptor for accessing the middleware products provided by the TP. A test-suite that assures that the SAGA-adaptor works as expected should be provided.
Pass/Fail Criteria	The SAGA-adaptor allows the access to the TP middleware through the SAGA API.
Related Information	SAGA API [R 19][R 20]
Revision Log	

31.1 Specific SAGA Bindings

31.1.1 BES

BES Bindings	
ID	**CLIENT_API_BES_1**
Description	SAGA bindings should provide remote execution using BES.
Mandatory	YES
Applicability	Client API Appliances with BES bindings

Input from Technology Provider	SAGA-adaptor for accessing BES resources (various URL schemes) that provides job abstraction, using
Pass/Fail Criteria	The SAGA-adaptor allows: - Running and managing jobs at remote resources (via BES) using
Related Information	SAGA API [R 19][R 20]
Revision Log	

31.1.2 Globus

Globus GRAM Bindings	
ID	**CLIENT_API_GLOBUS_1**
Description	Globus bindings should provide remote files access using Globus.
Mandatory	YES
Applicability	Client API Appliances with Globus bindings

Input from Technology Provider	SAGA-adaptor for accessing Globus resources via gram (URL scheme gram://) that provides job abstraction.
Pass/Fail Criteria	The SAGA-adaptor allows: - Use of X.509 context - Running and managing jobs at remote resources (via gram)
Related Information	SAGA API [R 19][R 20]
Revision Log	

Globus GridFTP Bindings	
ID	**CLIENT_API_GLOBUS_2**
Description	Globus bindings should provide remote file access using GridFTP
Mandatory	YES
Applicability	Client API Appliances with Globus bindings

Input from Technology Provider	SAGA-adaptor for accessing files resources via GridFTP (URL scheme gsiftp://, gsiscp://) that provides file abstraction.
Pass/Fail Criteria	The SAGA-adaptor allows: - Use of X.509 context - File operations: reading, writing, copying and modifying remote files and directories using GridFTP.
Related Information	SAGA API [R 19][R 20]
Revision Log	

31.1.3 SSH

SSH Bindings	
ID	**CLIENT_API_SSH_1**
Description	SSH bindings should provide remote execution and file access using SSH.
Mandatory	YES
Applicability	Client API Appliances with SSH bindings

Input from Technology Provider	SAGA-adaptor for accessing SSH resources (URL scheme ssh://) that provides job and file abstraction.
Pass/Fail Criteria	The SAGA-adaptor allows: - Running jobs at remote resources (via ssh) - File operations: reading, writing, copying and modifying remote files and directories using ssh.
Related Information	SAGA API [R 19][R 20]
Revision Log	

32 VIRTUAL MACHINE MANAGEMENT

32.1 Virtual Machine Management API

OCCI RESTful HTTP Rendering Support	
ID	**VIRT_MGMT_API_1**
Description	Virtual Machine Management Appliances should support the OCCI RESTful HTTP rendering.
Mandatory	NO
Applicability	Virtual Machine Management Appliances

Input from Technology Provider	Valid OCCI RESTful HTTP API implementation, any deviations from the API implementation should be documented. Ideally, also provide a complete test suite and results for the API support
Pass/Fail Criteria	Pass if OCCI RESTful HTTP support is provided. If the API is not completely supported, this should be documented.
Related Information	UMD Roadmap [R 1] OCCI API [R 44]
Revision Log	

32.2 Virtual Machine Management Operations

Management of images	
ID	**VIRT_MGMT_OPS_1**
Description	Virtual Machine Management Appliances must provide support for management of images.
Mandatory	YES
Applicability	Virtual Machine Management Appliances

Input from Technology Provider	Support for managing the images that can be instantiated: - Upload new image. - List available images - List/Update metadata of an image. - Create new image from running instance. - Delete image.
Pass/Fail Criteria	Pass if the volume management operations are supported.
Related Information	UMD Roadmap [R 1]
Revision Log	

Management of Virtual Machine Instances	
ID	**VIRT_MGMT_OPS_2**
Description	Virtual Machine Management Appliances must provide support for starting, stopping and listing instances.
Mandatory	YES
Applicability	Virtual Machine Management Appliances

Input from Technology Provider	Support for Virtual Machine Instance management operations: - Start an instance from a given image - Query the status of an instance - Pause and resume a given instance (optional) - List the current existing instances - Stop/Delete an instance. When starting the instance, an optional key may be specified with for ssh access. Support for additional instance metadata should be provided.
Pass/Fail Criteria	Pass if the management operations are supported. Ideally provide support for specifying image metadata.
Related Information	UMD Roadmap [R 1]
Revision Log	

Management of network addresses	
ID	**VIRT_MGMT_OPS_3**
Description	Virtual Machine Management Appliances must provide support for requesting and assigning network addresses to instances.
Mandatory	YES
Applicability	Virtual Machine Management Appliances

Input from Technology Provider	Support for managing the network addresses of instances: - List network addresses for a given instance. - Allocate a new network address for a given instance. - Remove network address for a given instance.
Pass/Fail Criteria	Pass if the network address management operations are supported.
Related Information	UMD Roadmap [R 1]
Revision Log	

Management of volumes	
ID	**VIRT_MGMT_OPS_4**
Description	Virtual Machine Management Appliances must provide support for creating, attaching, detaching and delete volumes (block level storage)
Mandatory	YES
Applicability	Virtual Machine Management Appliances

Input from Technology Provider	Support for managing the volumes: - Create new volumes. - Attach/Detach volume to running instance. - Delete existing volume.
Pass/Fail Criteria	Pass if the volume management operations are supported.
Related Information	UMD Roadmap [R 1]
Revision Log	

33 VIRTUAL MACHINE IMAGE FORMAT

OVF Image Format Support	
ID	**VIRT_IMG_1**
Description	OVF Image Format support.
Mandatory	NO
Applicability	Virtual Machine Image Format Appliances

Input from Technology Provider	Support for the OVF (Open Virtualisation Format) to deploy images on the virtualisation platforms.
Pass/Fail Criteria	Pass if OVF images can be deployed.
Related Information	UMD Roadmap [R 1] OVF [R 45]
Revision Log	

34 IMAGE DISTRIBUTION CAPABILITY

The Image Distribution Capability Criteria is based on the StratusLab MarketPlace [R 46].

34.1 StratusLab MarketPlace

The StratusLab MarketPlace is a server for virtual image metadata. It does not provide storage for the images, which must be supported by other services.

Image Metadata Registration	
ID	**VIRT_IMGDIST_1**
Description	Support for registration of virtual machine images metadata.
Mandatory	YES
Applicability	Image Distribution Appliances

Input from Technology Provider	Support for registration of new virtual machine metadata. The metadata must follow the schema of the StratusLab MarketPlace as described in the technical documentation and the compliance with that schema must be checked during the registration procedure. Metadata must be signed in order to avoid possible alterations of metadata. Any addition to the server must be confirmed by email.
Pass/Fail Criteria	Pass if metadata registration is possible.
Related Information	UMD Roadmap [R 1]
Revision Log	

Fetch Image Metadata	
ID	**VIRT_IMGDIST_2**
Description	Support for fetching image metadata.
Mandatory	YES
Applicability	Image Distribution Appliances

Input from Technology Provider	Support for fetching all metadata of an image by using its unique identifier
Pass/Fail Criteria	Pass if fetching image metadata is possible.
Related Information	UMD Roadmap [R 1]
Revision Log	

Image Metadata Query	
ID	**VIRT_IMGDIST_3**
Description	Support for queries of virtual machine images metadata.
Mandatory	YES
Applicability	Image Distribution Appliances

Input from Technology Provider	Support for querying the metadata stored in the server. The server must show a list of image identifiers and selected fields for all the images in the server. A paginated interface may be used.
Pass/Fail Criteria	Pass if metadata queries are possible in the server showing all the images registered.
Related Information	UMD Roadmap [R 1]
Revision Log	

Image Metadata Search	
ID	**VIRT_IMGDIST_4**
Description	Support for searches of virtual machine images metadata.
Mandatory	YES
Applicability	Image Distribution Appliances

Input from Technology Provider	Support for searching the metadata stored in the server by specifying constraints on the metadata values. Any metadata field may be used for searching. The query language is dependent on the server implementation.
Pass/Fail Criteria	Pass if searches can be performed on the metadata stored in the server.
Related Information	UMD Roadmap [R 1]
Revision Log	

35 REFERENCES

R 1	UMD roadmap: https://documents.egi.eu/public/ShowDocument?docid=100
R 2	QC Test Notes: https://wiki.egi.eu/w/index.php?title=EGI_Quality_Criteria_Testing
R 3	Web Services Data Access and Integration – The Relational Realisation (WS-DAIR) Specification, Version 1.0
R 4	Web Services Data Access and Integration – The XML Realization (WS-DAIX) Specification, Version 1.0
R 5	OGSA-DAI: http://www.ogsadai.org.uk/
R 6	gLite LFC: https://twiki.cern.ch/twiki/bin/view/EGEE/GliteLFC
R 7	AMGA: http://amga.web.cern.ch/amga/
R 8	AMGA WSDL: http://amga.web.cern.ch/amga/soap_wsdair.html
R 9	AMGA streaming API: http://amga.web.cern.ch/amga/protocol.html
R 10	AMGA Metadata Queries: http://amga.web.cern.ch/amga/queries.html
R 11	A. Konstantinov, ARC Computational Job Management Component – A-REX, NORDUGRID-TECH-14
R 12	CREAM: http://grid.pd.infn.it/cream/
R 13	EMI-ES: https://twiki.cern.ch/twiki/bin/view/EMI/EmiExecutionService
R 14	GRAM5: http://www.globus.org/toolkit/docs/latest-stable/execution/gram5/
R 15	OGF DRMAA: http://www.drmaa.org/
R 16	OGSA Basic Execution Service v1.0: http://www.ogf.org/documents/GFD.108.pdf
R 17	UNICORE UAS: http://www.unicore.eu/unicore/architecture/service-layer.php#anchor_uas
R 18	gLite WMS: http://web.infn.it/gLiteWMS/
R 19	SAGA-CORE-WG: A Simple API for Grid Applications (SAGA) v1.0 (GFD.90)
R 20	SAGA (A Simple API for Grid Applications): http://saga.cct.lsu.edu/
R 21	Instrument Element: http://www.dorii.eu/resources:adaptation:middleware:IE
R 22	DORII (Deployment of Remote Instrumentation Infrastructure) Project: http://www.dorii.eu/

R 23	GlueSchema Specification v1.3: http://glueschema.forge.cnaf.infn.it/Spec/V13
R 24	GlueSchema Specification v2.0: http://www.ogf.org/documents/GFD.147.pdf
R 25	Glue Validator: https://tomtools.cern.ch/confluence/display/IS/GLUEValidator
R 26	JMS (Java Message Service Specification) 1.1: http://www.oracle.com/technetwork/java/jms/index.html
R 27	AMQP (Advanced Message Queuing Protocol): http://www.amqp.org/confluence/display/AMQP/Advanced+Message+Queuing+Protocol
R 28	Nagios Config Generator: https://tomtools.cern.ch/confluence/display/SAM/NCG
R 29	My EGI portal: https://tomtools.cern.ch/confluence/display/SAM/MyEGI
R 30	SAM Probes Documentation: https://tomtools.cern.ch/confluence/display/SAM/Probes
R 31	Accounting Portal: http://accounting.egi.eu/
R 32	GridSite Delegation Protocol: http://www.gridsite.org/wiki/Delegation_protocol
R 33	Globus Delegation Service: http://www.globus.org/toolkit/docs/4.0/security/delegation/
R 34	European Policy Management Authority for Grid Authentication (EuGridPMA): http://www.eugridpma.org/
R 35	ARGUS Authorization Service: https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework
R 36	XACML: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
R 37	Hydra encrypted file storage: https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS
R 38	gLite FTS: https://twiki.cern.ch/twiki/bin/view/EGEE/GLiteFTS
R 39	SRM v2.2: http://www.ggf.org/documents/GFD.129.pdf
R 40	S2 Test: http://s-2.sourceforge.net/
R 41	SRM-Tester: https://sdm.lbl.gov/twiki/bin/view/Software/SRMTester/WebHome
R 42	Lcg-utils: http://grid-deployment.web.cern.ch/grid-deployment/documentation/LFC_DPM/lcg_util/
R 43	Lcg-utils test suite: http://glite.cvs.cern.ch/cgi-bin/glite.cgi/org.glite.testsuites.ctb/UI/tests/test-lcg-utils.sh?view=markup
R 44	Open Cloud Computing Interface WG, OGF, http://www.ggf.org/gf/group_info/view.php?group=occi-wg

R 45	Virtualization Management (VMAN), DMTF http://www.dmtf.org/standards/vman
R 46	StratusLab http://stratuslab.eu/
R 47	StratusLab MarketPlace Technical Note TN-Marketplace (V3.0)