# Table of Contents

**WLCG Baseline Versions**

OS and base dependencies......................................................................................................................1  
Middleware.............................................................................................................................................1  
Baseline versions of services and client tools for WLCG operations.....................................................1  
Tier-0 and Tier-1 Data Management Services........................................................................................1  
Issues Affecting the WLCG Infrastructure.............................................................................................1  
Globus GSSAPI Name compatibility change..........................................................................................2
WLCG Baseline Versions

OS and base dependencies

WLCG services and clients currently are released for RHEL-6 and/or -7 compatible distributions.

There is a constraint on the version of Java used by services due to security requirements imposed by openssl. The following minimum versions were observed to work OK:

- java-1.7.0-openjdk-1.7.0.131-2.6.9.0
- java-1.8.0-oracle-headless-1.8.0.121-2

Middleware

Note: OSG sites should follow guidelines from OSG Operations.

For EGI sites the default advice is to take MW products from the UMD repository:

- http://repository.egi.eu/download/

They are made available there after a successful Staged Rollout. The staged rollout process significantly increases the probability that components work well and that glitches have been caught.

For early access to newer versions ("caveat emptor") one may use the EGI Preview repository directly:

- https://wiki.egi.eu/wiki/Preview_Repository

For continued access to unsupported third-party products like Maui ("caveat emptor") one can use the EGI Community Third Party repository.

Baseline versions of services and client tools for WLCG operations

The WLCGBaselineTable lists the minimum recommended versions for WLCG production. It does not necessarily reflect the latest versions of packages available in the UMD / EPEL / ... repositories, but it contains the latest version fixing significant bugs or introducing important features. Versions newer than those indicated are assumed to be at least as good, unless otherwise indicated. In other words: if you have a version older than the baseline, you should upgrade at least to the baseline, while EGI or OSG may even recommend the latest version available in their releases.

Tier-0 and Tier-1 Data Management Services

Information about the Data Management service versions deployed at T0 and T1 sites is collected at WLCGT0T1GridServices.

Issues Affecting the WLCG Infrastructure

Last updated on 2018-02-24.

The following table serves to summarize the main MW issues affecting operations on the WLCG...
Globus GSSAPI Name compatibility change

Globus default hostname verification method has moved to 'STRICT_RFC2818' rather than 'HYBRID' by default with globus-gssapi-gsi-11.21

The differences between the 2 modes are explained in the configuration file /etc/grid-security/gsi.conf of the package globus-gssapi-gsi:

```
# GSSAPI Name compatibility mode when trying to determine
# if a host certificate is legitimate. GSI predates RFC2818,
# so there are some old, less-secure, practices by default.
# The different modes are:
# STRICT_GT2:
#    Strictly backward-compatible with GT 2.0 name matching.
#    X.509 subjectAltName values are ignored. Names with
#    hyphens are treated as wildcarded such that
#    host-ANYTHING.example.com will match a certificate named
#    host.example.com. The name matching will rely on canonical
#    host (as resolved via getnameinfo) name associated with
#    a connection's IP addresses.
# STRICT_RFC2818:
#    Support RFC 2818 server identity processing. Hyphen
#    characters are treated as normal part of a host name.
#    dnsName and ipAddress subjectAltName extensions are matched
#    against the host and port passed to GSSAPI. If subjectAltName
#    is present, X.509 SubjectName is ignored.
# HYBRID:
#    Support a hybrid of the two previous name matching algorithms,
#    liberally matching both hyphen wildcards, canonical names
#    associated with IP addresses, and subjectAltName extensions.
#    This has been the default since GT 4.2
```

The sites that are affected by this change are the ones running services whose clients may use globus-gssapi-gsi for authentication:

- CE
- FTS
- SRM
- GridFTP

Note: please let us know of other issues that should be listed here.

An archive for past issues already solved is available at WLCGMiddlewareIssuesArchive.

Globus GSSAPI Name compatibility change

Globus default hostname verification method has moved to 'STRICT_RFC2818' rather than 'HYBRID' by default with globus-gssapi-gsi-11.21

The differences between the 2 modes are explained in the configuration file /etc/grid-security/gsi.conf of the package globus-gssapi-gsi:

```
# GSSAPI Name compatibility mode when trying to determine
# if a host certificate is legitimate. GSI predates RFC2818,
# so there are some old, less-secure, practices by default.
# The different modes are:
# STRICT_GT2:
#    Strictly backward-compatible with GT 2.0 name matching.
#    X.509 subjectAltName values are ignored. Names with
#    hyphens are treated as wildcarded such that
#    host-ANYTHING.example.com will match a certificate named
#    host.example.com. The name matching will rely on canonical
#    host (as resolved via getnameinfo) name associated with
#    a connection's IP addresses.
# STRICT_RFC2818:
#    Support RFC 2818 server identity processing. Hyphen
#    characters are treated as normal part of a host name.
#    dnsName and ipAddress subjectAltName extensions are matched
#    against the host and port passed to GSSAPI. If subjectAltName
#    is present, X.509 SubjectName is ignored.
# HYBRID:
#    Support a hybrid of the two previous name matching algorithms,
#    liberally matching both hyphen wildcards, canonical names
#    associated with IP addresses, and subjectAltName extensions.
#    This has been the default since GT 4.2
```

The sites that are affected by this change are the ones running services whose clients may use globus-gssapi-gsi for authentication:

- CE
- FTS
- SRM
- GridFTP

Note: please let us know of other issues that should be listed here.

An archive for past issues already solved is available at WLCGMiddlewareIssuesArchive.
• MyProxy

and using DNS aliases which are not included within the SAN (Subject Alternative Name) field of the certificate (including the host name itself). Beware that "If subjectAltName is present in the certificate, X.509 SubjectName is ignored".

To avoid any issue with the security configuration of the services, we strongly advise site managers to make sure that all the hostnames and aliases used to connect to a service are included in its host certificate Subject Alternative Name field.