EGEE-III

FQAN PATTERN MATCHING

Update the file name and then use "update field" Word function, right mouse button

Use "update field" Word function, right mouse button

Document identifier:	EGEEIII
Date:	**10/09/2008**
Activity:	**JRA1**
Document status:	**DRAFT**
Document link:	https://edms.cern.ch/document/edmsId/version

Abstract: This document specifies the usage of wildcards in FQAN patterns. It defines the exact syntax and the semantics for wildcards in FQAN patterns. The target audience of the document are site and VO administrators, which use FQANs for authorization and identity mapping decisions, and developers that implement FQAN pattern matching libraries.

Document Log

Issue	Date	Comment	Author/Partner
	1.9.08	First Draft	Placi Flury

Document Change Record

Issue	Item	Reason for Change

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

1.1. PURPOSE

This document refines the "Use of wildcards in FQAN pattern matching" recommendation, which have been formulated in the attachment of the MJRA1.7 deliverable (https://edms.cern.ch/document/887174/1). The refinement eliminates existing ambiguities and provides the foundation for the implementation of libraries that process FQANs.

VO and site administrators can use the document as a reference for defining valid FQAN patterns that use wildcards.

1.2. DOCUMENT ORGANISATION

[Describe how the document is organized.]

1.3. APPLICATION AREA

This document applies to the implementation and support of the gLite middleware (3.1) within the scope of the EGEE project and the JRA1 activity mandate. It affects FQAN pattern matching as done by LCMAPS plugins, by the WMS, and by the security command line tools.

1.4. REFERENCES

[This subsection provides a complete list of all documents referenced elsewhere in the document.]

Table 1: Table of references

R 1	Overview of gLite authorization mechanisms. EGEE-II MJRA1.7 https://edms.cern.ch/document/887174/1
R2	FQAN Matching Rules https://edms.cern.ch/document/858263/1.
R 3	*VOMS Credential Format, Vincenzo Ciaschini, Akos Frohner: http://cern.ch/edg-wp2/security/voms/edg-voms-credential.pdf*

1.5. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGEE "Document Management Procedure" will be followed: http://egee-jra2.web.cern.ch/EGEE-JRA2/Procedures/DocManagmtProcedure/DocMngmt.htm.

1.6. TERMINOLOGY

This subsection provides the definitions of terms, acronyms, and abbreviations required to properly interpret this document. A complete project glossary is provided in the EGEE glossary http://egee-jra2.web.cern.ch/EGEE-JRA2/Glossary/Glossary.html.

Glossary

FQAN	Fully Qualified Attribute Name: A string containing VOMS group and (optionally) role information.
VO	Virtual Organization

2. FQAN SYNTAX

A Fully Qualified Attribute Name (FQAN) is a string compound consisting of the group, the subgroups, and the role a user chooses from, in order to access a grid resource. The resource, on the other hand, specifies FQAN *patterns* to denote the FQANs it accepts.

The syntax of FQANs and FQAN patterns have originally been defined in [R3] and [R2]. The new and simplified way of processing FQANs makes some of the content of these documents obsolete.

The following rules (taken from [R2], however, still apply:

FQANs are written in the following way:

- FQAN are composed by a group, potential subgroups, and an optional role part
    - Syntax is */group{/subgroup}[/Role=rolename]*
- By convention, the name of the first group is the name of the VO
- Subgroups are separated from the group name with a '/' (slash) delimiter
- The role is delimited by the "/Role=" tag.
- Membership in a subgroup implies membership in a group
    - E.g: if the FQAN '/atlas/prod' is in your credentials, then the FQAN '/atlas' is also in there
- The following characters are allowed in group and subgroup names: [0-9a-zA-Z-_.]
- The following characters are allowed in role names: [0-9a-zA-Z-_.]

The VO name should be unique for each VO. A way to guarantee that is to use as VO name a DNS name, which is owned by the VO.

3. USE OF WILDCARDS IN FQANS PATTERNS

The only supported wildcard is the asterisk character ("*"), and it can only be used

- in the group string after the trailing slash ("/") or
- the "/Role=" string to denote all possible roles:
- valid FQAN patterns must specify the VO. The "/*" pattern to denote any VO is not allowed.
- the "*" wildcard can substitute zero or more 'objects', where an object either is:
    - a subgroup
    - a role
- the wildcard is **not** allowed to substitute fractions of an 'object'.

Examples for valid FQAN patterns:

/vo/subgroup

/vo/subgroup/Role=role

/vo/subgroup/*/Role=role

/vo/*/Role=*

/vo/subgroup/Role=*

Examples for invalid FQAN patterns:

/*	VO not specified
/vo/*/subgroup	wildcard not after trailing slash ('/')
/vo/subgroup*	wildcard not after trailing slash ('/')
/vo/*ubgroup	wildcard substitutes fraction of an object
/vo/subgroup/**	invalid syntax
/vo/*/*	invalid syntax

3.1. INTERPRETATION OF THE WILDCARD

We stated that the "*" (asterisk) wildcard can substitute **zero or more** objects. Therefore following examples all do match:

Examples

FQAN pattern	FQAN	Match?
/dteam/*	/dteam	YES
/dteam/*	/dteam/atlas	YES
/dteam/*	/dteam/atlas/higgs	YES
/dteam/*/Role=production	/dteam/Role=production	YES
/dteam/Role=*	/dteam	YES
/dteam/*/Role=*	/dteam	YES

Obviously, the "/" and "/Role" tokens are only used as delimiter tags for the notation (the "/" tag delimits the group and subgroups and the "/Role=" tag delimits the role). For the interpretation whether a FQAN pattern matches or not, they are simply masked out.

3.2. NOTES FOR VO AND SITE ADMINISTRATORS

The new wildcard usage is not backwards compatible. That means, existing configurations (gridmap files) that used wildcards must be reviewed and most likely be changed. The differences are

- FQAN patterns that still contain a '/Capability=' segment will not be accepted anymore
- the "?" wildcard is not permissible anymore
- the "*" wildcard can not substitute parts of a group, subgroup or role, since only entire object substitution is allowed
- the "*" can only be at the trailing end of the group and/or role

3.3. NOTES FOR LIBRARY DEVELOPPERS

One should keep in mind, that the '*' wildcard may not be the only wildcard that will be used in future. Hence, keep in mind the extensibility of the implementation.

4. FURTHER EXAMPLES

The listed examples are the very same as in [R2]. Differences in the outcomes are marked in red.

Pattern	FQAN	Match ?
/atlas	/atlas	Yes
	/atlas/Role=NULL	Yes
	/atlas/prod	No
	/atlas/Role=sgm	No
	/atlas/prod/Role=sgm	No
	/atlassi	No
/atlas/Role=NULL	/atlas	Yes
	/atlas/Role=NULL	Yes
	/atlas/prod	No
	/atlas/Role=sgm	No
	/atlas/prod/Role=sgm	No
	/atlassi	No
/atlas/Role=*	/atlas	Yes
	/atlas/Role=NULL	Yes
	/atlas/prod	No
	/atlas/Role=sgm	Yes
	/atlas/prod/Role=sgm	No
	/atlassi	No
/atlas/prod/Role=*	/atlas	No
	/atlas/Role=NULL	No
	/atlas/prod	No
	/atlas/Role=sgm	No
	/atlas/prod/Role=sgm	Yes
	/atlas/prod/Role=NULL	Yes
	/atlassi	No
/atlas*	/atlas	INVALID FQAN Pattern
	/atlas/Role=NULL	INVALID FQAN Pattern
	/atlas/prod	INVALID FQAN Pattern
	/atlas/Role=sgm	INVALID FQAN Pattern
	/atlas/prod/Role=sgm	INVALID FQAN Pattern
	/atlassi	INVALID FQAN Pattern
	/atlas/prod/Role=NULL	INVALID FQAN Pattern
/atlas/*	/atlas	Yes
	/atlas/Role=NULL	Yes

	/atlas/prod	Yes
	/atlas/Role=sgm	No
	/atlas/prod/Role=sgm	No
	/atlassi	No
	/atlas/prod/Role=NULL	Yes
/atlas*/Role=sgm	/atlas	INVALID FQAN Pattern
	/atlas/Role=NULL	INVALID FQAN Pattern
	/atlas/prod	INVALID FQAN Pattern
	/atlas/Role=sgm	INVALID FQAN Pattern
	/atlas/prod/Role=NULL	INVALID FQAN Pattern
	/atlas/prod/Role=sgm	INVALID FQAN Pattern
	/atlassi/Role=sgm	INVALID FQAN Pattern
	/atlassi	INVALID FQAN Pattern
/atlas/*/Role=sgm	/atlas	Yes
	/atlas/Role=NULL	No
	/atlas/prod	No
	/atlas/Role=sgm	Yes
	/atlas/prod/Role=NULL	No
	/atlas/prod/Role=sgm	Yes
	/atlassi/Role=sgm	No
	/atlassi	No