Pattern Matching in gLite

C.Witzig, SWITCH
Security Architect EGEE
christoph.witzig@switch.ch

Why

- **Importance of pattern matching**
  - User's proxy certificate contains an attribute certificate, which contains a list of strings, called "fully qualified attribute names" FAQNs
  - User is authorized at the resource by matching these FQANs against a list of "allowed" FQAN patterns
  - Basis for authorization of users

- **VOMS contains two types of attributes:**
  - Group membership - they are always all present in the AC
  - Roles - they user must ask for them to be included at proxy creation time ("voms-proxy-init")

What's the big deal?

- **Quiz: Which FQANs match which patterns?**
  - FAQN patterns:
    - /vo1/analysis/*
    - /vo1/ana*
    - /vo1/analysis/role=*
  - FQANs:
    - /vo1/analysis
    - /vo1/analysis/higgs/role=production

Use of FAQNs and FQAN patterns

- **FQAN pattern matching rules are about to change**
  - Consequence of authorization study
    - done at the end of EGEE-II
  - Reason:
    - Many people had difficulty understanding/remembering the rules
    - Answer depended on the order of patterns in gridmapfile

- **Current use:**
  - https://edms.cern.ch/document/858263/1

- **Future use:**
  - To be uploaded (by tomorrow)

- **Exact transition date: TBA**

Current Rules

Syntax and Rules

- **FQAN patterns:**
  - May contain wildchars
  - Allowed wildchars: ? and *
  - Allowed characters: **: [0-9a-zA-Z-_.]**

- **/vo1/analysis/hi*/Role=production**
  1. If string Rule=NULL is present, eliminate it
  2. Separate subgroup and role substring and match them separately as substrings (“literal”)
     - /vo1/analysis/hi*
     - /Role=production

Pattern	FQAN	
/vo1/analysis/*/Role=pro	**/vo1/analysis/higgs/Role=pro**	**Yes**
	/vo1/analysis	**No**
	/vo1/analysis/Role=pro	**No**
/vo1/an*si?	**/vo1/analysis**	**Yes**
	/vo1/analysis/Role=pro	**No**

Note:

1. /vo1/* does not match /vo1
2. /vo1/Role=* does not match /vo1
3. In order to match an entire VO, you must use two patterns
   - /vo1
   - /vo1/*

New Rules

Syntax

- **FQAN patterns:**
  - Only * wildchar allowed and it must be at the end of the group/role substring after the trailing /
  - Allowed characters: **: [0-9a-zA-Z-_.]**

- **Allowed FQAN patterns**
  - /vo1/analysis
  - /vo1/analysis/*/Role=production
  - /vo1/*/Role=*

- **Not allowed FQAN patterns**
  - /vo1/*/higgs
  - /vo1/*/*
  - /vo1/ana*/higgs
  - /vo1/*/Role=pro*

Rules

- **Two possible interpretation of ***
  1. Object substitution
     - /vo1/* does not match /vo1
     - /vo1/Role=* does not match /vo
  2. Semantic substitution
     - /vo1/* matches /vo1
     - /vo1/Role=* matches /vo1

– **Semantic substitution chosen**

Pattern	FQAN	
/vo1/analysis/*/Role=pro	/vo1/analysis/higgs/Role=pro	Yes
	/vo1/analysis	No
	/vo1/analysis/Role=pro	Yes
/vo1/an*si?	Invalid pattern	
/vo1/*	/vo1	Yes
	/vo1/analysis	Yes
	/vo1/analysis/higgs	Yes
/vo1/*/Role=pro	/vo1/Role=pro	Yes
/vo1/Role=*	/vo1	Yes
/vo1/*/Role=*	/vo1	Yes

Note:

1. /vo1/* matches /vo1
2. /vo1/Role=* matches /vo1
3. In order to match all groups of an entire VO, you use one pattern
    1. /vo1/*
4. In order to match all groups and all roles of an entire VO, you use one pattern
    1. /vo1/*/Role=*

Matching Rule for LCMAPS

- **Current rule:**
  - LCMAPS takes first match
    - Consequence: Ordering in gridmapfile matters
      - *FQAN = /vo1/analysis*
      - */vo1/** *.user1* *<-- takes first one*
      - */vo1/analysis* *.user2*

- **New rule:**
  - LCMAPS takes most significant match
    - Consequence: Ordering in gridmapfile doesn't matter
      - *FQAN = /vo1/analysis*
      - */vo1/** *.user1*
      - */vo1/analysis* *.user2* *<-- takes first one*

Most significant match

- **Question:**
  - What is more significant:
    - /vo1/analysis/*/Role=production
    - /vo1/analysis/higgs/Role=*
  - Answer:
    - Group is more significant