Aresh's auth demo for CMS

Revision/update of the authentication system

- Task assigned by Julia (19 Sep 2017):
 - E-group cric-cmstest1 via SSO (both Stephan and Giuseppe belong to cric-cmstest1) mapped to Site Admin group able to edit CMS site model with instance-restrictions by country. The restriction should be on the country level and country is retrieved from VOMS (so unless the person has been logged in first time with VOMS, he/she can not edit site info, since the country is not resolved). => Stephan can edit US sites, Giuseppe Italian sites only after VOMS login.
 - E-group cric-cmstest2 via SSO (only Stephan belongs to cric-cmstest2) should be mapped to the CRIC group which is allowed to edit only T2_IT_Bari. => Stephan can edit T2_IT_Bari via SSO login
 - In short (see backup slides):
 - if Stephan logs in only via SSO, then Stephan can edit only T2_IT_Bari, but no other sites.
 - If Stephan logs in only via VOMS, then Stephan can edit all US sites, e.g. T1_US_FNAL, but not T2_IT_Bari.
 - If Stephan has done logins both via SSO and via VOMS, then Stephan can edit both T2_IT_Bari and US sites (e.g. T1_US_FNAL), but not other sites.

Revision/update of the authentication system

- ssl authentication implemented (for cric admins)
- modified implementation of 'Group' mapping for vomsauth
- modified implementation of 'Group' mapping for ssoauth
- modified cmsview ops_edit to enable restricted permissions
- Gitlab: https://gitlab.cern.ch/aresh/cric/commits/voms-auth

Plan

- Complete second task assigned by Julia:
 - Map **e-group cric-cmstest3** to the CRIC group which can edit any glidein entry info without any instance restriction, but not to edit CMS site (useful for glideins factory admins).
- Implement vomsauth cron to retrieve voms users' info

BACKUP

if I were Stephan and log in only via SSO, then I can edit only T2_IT_Bari, but not T1_US_FNAL, or any other sites.

Login only via SSO

		1					2	
Core - CMS - Documentation - Admin - Home / Core - Help -	aresh.vedaee@cern.ch -		Core - CMS -	Documentation - Adn	nin 👻	0 Help -	aresh.vedaee@cern.ch -	() Exit
CRIC WebUI Portal for Core Resources	Aresh Vedaee		Basic relations	ι	Jpdate CMS Site object	: T2_IT_Bari	Aresh Vedaee	
Welcome to the CRIC Web Portal for the Core Resources. This service will hopefully give an answer to your needs for accessing information a service has been built on top of new technologies. See below for a list of available features.	Aresh.Vedaee@cern.ch Groups: CRIC-CMS-SITE- ADMIN-T2_IT_Bari (sso)	ces. The	Experiment Site: Tier level:	? T2_IT_Bari ? 2		•	Aresh.Vedaee@cern.ch Groups: CRIC-CMS-SITE- ADMIN-T2_IT_Bari (sso)	
For Operators For Experts			Country:	? Italy		•		
RC Site list Create new RC site Create new RC site Create new Regional Center			RC site (GOCDB/OIM):	INFN-BARI		•		
• Downtimes			VO name:	CMS		•		
CAN NOT EDIT T1_US_FNAL !!!		2					<u>A</u>	
The Core - CMS - Documentation - Admin - O Help -	aresh.vedaee@cern.ch -	Exit	Core - CMS -	Documentation - Adr	min 🔻	1 Help -	aresh.vedaee@cern.ch 💭 ୯	D Exit
Permission denied	Aresh Vedaee				Permission	denied	Aresh Vedaee	
We're sorry but access to this page is restricted	Aresh.Vedaee@cern.ch		We're sorry but acces	ss to this page is restrict	ed		Aresh.Vedaee@cern.ch	
You are not allowed to edit object T1_US_FNAL: no appropriate instance-specific permissions granted for given object (however you are a required_permissions=['cms.change_cmssite']			You are not allowed to edi	Groups: CRIC-CMS-SITE-				
	ADMIN-T2_IT_Bari (sso)		required_permissions=[ch	ns.change_cmssite']			ADMIN-T2_IT_Bari (sso)	

if I were Stephan and log in only via VOMS, then I can edit only T1_US_FNAL, but not T2_IT_Bari, or any other non-US sites.

Login only via VOMS

Core - CMS -	Documentation -	Admin 🗸	Home	Core 🚯 Help 🗸	aresh.vedaee@cern.ch
6	CF	RIC WebUI Por	tal for Core Re	esources	Aresh Vedaee
		urces. This service will hopefully See below for a list of available fe		for accessing information a	Aresh.Vedaee@cern.ch Groups: CRIC-CMS- REGIONAL-ADMIN-US (voms) 38
For Op	perators		For Experts		() Exit
RC S Crea	Site list te new RC site te new Regional Center		Regional CenterRC pledges	ers	
• Dow					
Core - CMS	- Documentation	 Admin 		Help +	aresh.vedaee@cern.ch
Core - CMS Basic relations	- Documentation		Site object: T1_US		aresh.vedaee@cern.ch Aresh Vedaee
		Update CMS S	Site object: T1_US		
Basic relations	: I T1_US_FN	Update CMS S	Site object: T1_US		Aresh Vedaee Aresh.Vedaee@cern.ch Groups: CRIC-CMS- REGIONAL-ADMIN-US (voms)
Basic relations Experiment Site	: 71_US_FN : 71_US_FN	Update CMS S	Site object: T1_US		Aresh Vedaee Aresh.Vedaee@cern.ch Groups: CRIC-CMS-
Basic relations Experiment Site	: ? T1_US_FN : ? 1 : ? USA	Update CMS S	Site object: T1_US		Aresh Vedaee Aresh.Vedaee@cern.ch Groups: CRIC-CMS- REGIONAL-ADMIN-US (voms)

Can not EDIT T2_IT_BARI !!!

Core < CMS < Documentation < Admin < Help < aresh.vedaee@cern.ch < C Exit</td>

Permission denied

We're sorry but access to this page is restricted

Vou are not allowed to edit object T2_IT_Bari: no appropriate instance-specific permissions granted for given object (however you are able required_permissions=['cms.change_cmssite']

Please relogin with other credentials or request required permissions.

Core - CMS - Documentation - Admin - O Help -	aresh.vedaee@cern.ch -	() Exit
Permission denied	Aresh Vedaee	
e're sorry but access to this page is restricted	Aresh.Vedaee@cern.ch	
You are not allowed to edit object T1_UK_RAL: no appropriate instance-specific permissions granted for given object (however you are able required_permissions=['cms.change_cmssite']	Groups: CRIC-CMS- REGIONAL-ADMIN-US (voms)	
ease relogin with other credentials or request required permissions.	© Exit	

If I were Stephan and have done VOMS/SSO logins, then I can edit both T2_IT_Bari and T1_US_FNAL but no other sites

5

Logins via VOMS/SSO

	0				CAN EDI	12_11_Bari !!!			
A Core - CMS -	i Documentation - Admin - Home / Core Help -	aresh.vedaee@cern.ch -	C Exit	Core - CMS -	Documentation - Admin -	(🚯 Help 👻 🤷	aresh.vedaee@cern.ch +	O Exit
CRIC WebUI Portal for Core Resources		Aresh Vedaee		Basic relations	Update CMS	Site object: T2_IT_Bari	,	Aresh Vedaee	
	I for the Core Resources. This service will hopefully give an answer to your needs for accessing information new technologies. See below for a list of available features.	Aresh Vedaee@cern.ch Groups: CRIC-CMS- a REGIONAL-ADMIN-US (voms),CRIC-CMS-SITE- ADMIN-T2_IT_Bari (sso)	ces. The	Experiment Site: Tier level:	 72_IT_Bari 2 	•	F	Aresh.Vedaee@cern.ch Groups: CRIC-CMS- REGIONAL-ADMIN-US voms),CRIC-CMS-SITE-	
For Opera	For Operators For Experts			Country:	2 Italy	•	A	ADMIN-T2_IT_Bari (sso)	
 RC Site list Create new RC site RC pledges 				RC site (GOCDB/OIM):	INFN-BARI	•			
	/ Regional Center			VO name:	CMS	•			
Core → CMS →	CAN EDIT T1_US_FNAL !!!	✓ aresh.vedaee@cern.ch ✓	Sector	Core - CMS -	Documentation - Admin -	0	🖲 Help 🗸 🔒 ar	aresh.vedaee@cern.ch +	() Exit
Basic relations	Update CMS Site object: T1_US_FNAL	Aresh Vedaee			Perm	nission denied	A	resh Vedaee	
Experiment Site:	71_US_FNAL	Aresh.Vedaee@cern.ch Groups: CRIC-CMS- REGIONAL-ADMIN-US (voms),CRIC-CMS-SITE- ADMIN-T2_IT_Bari (sso)		We're sorry but access	to this page is restricted	Δ.	resh.Vedaee@cern.ch		
Tier level: Country:	Image: USA			You are not allowed to edit of required_permissions=['cms.	permissions granted for given object (however yo	you are able G	Groups: CRIC-CMS- IEGIONAL-ADMIN-US poms),CRIC-CMS-SITE-		
RC site (GOCDB/OIM):				Please relogin with other creder	AD	DMIN-T2_IT_Bari (sso)			
VO name:	CMS ·							8	