fuss-manager - Segnalazione #863

Aggiungere permission checking a operation e API

06/28/2019 01:48 PM - Elena Grandi

Status:	Chiuso	**Start date:**	06/28/2019
Priority:	Normale	**Due date:**	
Assignee:	Enrico Zini	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.7 Autenticazione e autorizzazione		
Resolution:	fixed		

Description

Related issues:

Related to fuss-manager - Segnalazione #862: form/view di login	**Chiuso**	**06/28/2019**
Blocked by fuss-manager - Segnalazione #856: interfaccia con LDAP asincrona ...	**Chiuso**	**06/28/2019**

Associated revisions

Revision a908b879 - 10/02/2019 10:41 AM - Elena Grandi

Pass user informations to operations. refs: #863

Revision 5728ad26 - 10/03/2019 02:51 PM - Elena Grandi

Start checking permissions for operations. refs: #863

Revision 8002fce0 - 10/04/2019 11:01 AM - Elena Grandi

Fix some tests and code errors. refs: #863

Revision 5374e745 - 10/07/2019 10:12 AM - Elena Grandi

Start testing permissions. refs: #863

Revision 8469c804 - 10/07/2019 10:36 AM - Elena Grandi

Further permission tests. refs: #863

Revision ce151ab6 - 10/07/2019 10:38 AM - Elena Grandi

Permissions on remaining ops. refs: #863

Revision 02ee4927 - 10/08/2019 12:40 PM - Elena Grandi

Permission checking on sync and async methods. refs: #863

Revision 3a0e70f6 - 10/09/2019 01:06 PM - Elena Grandi

Further webapi permissions. refs: #863

Revision 124717db - 10/10/2019 12:17 PM - Elena Grandi

Override the user if passed by js in decoded. refs: #863

Revision 3f870563 - 10/10/2019 12:21 PM - Elena Grandi

Use @wraps on decorators. refs: #863

Revision 65d962e3 - 10/10/2019 12:55 PM - Elena Grandi

Move checking for permissions to a common place. refs: #863

Revision a1aa0926 - 10/10/2019 01:47 PM - Enrico Zini

Merging t863 into master. Refs: #863

History

#1 - 06/28/2019 01:48 PM - Elena Grandi

- Blocked by Segnalazione #856: interfaccia con LDAP asincrona per tornado added

#2 - 07/11/2019 12:03 PM - Elena Grandi

- Blocked by Segnalazione #862: form/view di login added

#3 - 09/30/2019 12:12 PM - Elena Grandi

- Blocked by deleted (Segnalazione #862: form/view di login)

#4 - 09/30/2019 12:12 PM - Elena Grandi

- Related to Segnalazione #862: form/view di login added

#5 - 10/09/2019 02:30 PM - Elena Grandi

- Status changed from Nuovo to Commenti

- Assignee changed from Elena Grandi to Enrico Zini

Ripasso il ticket per review e merge.

Mi pare ci sia quasi tutto, solo non sono sicura se aggiungere in tests/test_webserver.py un test in più per le operations che testi un'operation che richieda permessi, perché non son sicura che funzioni correttamente (sospetto che al momento non dia un forbidden, ma un 500 o simili).

#6 - 10/10/2019 12:10 PM - Enrico Zini

- Assignee changed from Enrico Zini to Elena Grandi

Bel branch, mi piace molto!

Alcuni commenti piú o meno estetici.

In manager/ops.py:58, suggerisco un decoded.pop("user", None) per buttar via 'user' se viene passato per sbaglio da javascipt, altrimenti il costruttore di Op lanca un'eccezione per un parametro passato due volte.

In alternativa, forse meglio, un override pari pari: decoded["user"] = user.

Nel decoratore permission_required, in caso user sia None, possiamo dare per scontato che il permesso non ci sia, e quindi semplificare i vari getattr successivi, o c'è la possibilità che vengano assegnati permessi all'utente None?

Nei decoratori, aggiungi un functools.wraps, cosí vengono preservati gli attributi della funzione originale nella funzione wrappata: https://docs.python.org/3.5/library/functools.html#functools.wraps

Visto che il controllo dei permessi è replicato nei due decoratori di ops e di webapi, propongo di spostarlo in una funzione unica in perms.py, cosí quella parte, abbastanza security sensitive, rimane in un posto solo per testarla, fare code review, e sistemare bug.

#7 - 10/10/2019 01:03 PM - Elena Grandi

Enrico Zini wrote:

> In manager/ops.py:58, suggerisco un decoded.pop("user", None) per buttar via 'user' se viene passato per sbaglio da javascipt, altrimenti il costruttore di Op lanca un'eccezione per un parametro passato due volte.
>
> In alternativa, forse meglio, un override pari pari: decoded["user"] = user.

fatto con l'alternativa override

> Nel decoratore permission_required, in caso user sia None, possiamo dare per scontato che il permesso non ci sia, e quindi semplificare i vari getattr successivi, o c'è la possibilità che vengano assegnati permessi all'utente None?

Mi pare realistico che l'utente None possa avere ReadonlyBaseAccess.

> Nei decoratori, aggiungi un functools.wraps, cosí vengono preservati gli attributi della funzione originale nella funzione wrappata: https://docs.python.org/3.5/library/functools.html#functools.wraps

fatto

> Visto che il controllo dei permessi è replicato nei due decoratori di ops e di webapi, propongo di spostarlo in una funzione unica in perms.py, cosí quella parte, abbastanza security sensitive, rimane in un posto solo per testarla, fare code review, e sistemare bug.

fatto, anche questo.

#8 - 10/10/2019 01:07 PM - Elena Grandi

- Assignee changed from Elena Grandi to Enrico Zini

#9 - 10/10/2019 01:48 PM - Enrico Zini

- Status changed from Commenti to Chiuso

- Resolution set to fixed

Perfetto, mergiato in master, chiudo.