Gestion des accès

La gestion des accès dans authentic a deux objectifs:

- gérer les accès aux service soit directement soit indirectement en leur transmettant des attributs,
- gérer les accès à la partie administrative d'authentic lui même, en permettant une utilisation multi-tenant i.e. pouvoir gérer plusieurs organisation ayant éventuellement des relations hiérarchiques entre elles.

L'idée est de partir du modèle RBAC et d'en garder l'essentiel pour couvrir ces deux besoins.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

`Modèle RBAC avec héritage`

Nous n'avons pas besoin de la partie sur les permissions qui rend le modèle complexe à gérer; on confondra toujours un rôle avec une permission sur un objet, i.e. pour chaque paire permission, objet dont nous aurions besoin, il y aura un rôle équivalent qui pourra se combiner avec d'autres rôle en utilisant l'héritage permettant ainsi exactement les mêmes possibilités que le modèle RBAC complet.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

`Modèle RBAC simplifié pour Authentic`

Notion d'héritage

L'héritage entre rôle n'a rien à voir avec l'héritage en programmation. Si un rôle R1 hérite d'un rôle R2, cela veut dire que le rôle R1 possède en plus des siennes toutes les permissions associées au rôle R2, soit directement soit via héritage. C'est une relation transitive, si R2 hérite de R3 alors R1 hérite indirectement aussi de R3.

Cela revient aussi à dire que tous les membres de R1 sont aussi indirectement des membres de R2.

Les rôles

Les rôles seront séparés en deux:

- les rôles fonctionnels créés et gérés par les utilisateurs, ils ne sont lié directement à aucune permission sur aucun objet, ils peuvent seulement hériter d'autres rôles,
- les rôles techniques gérés par leur système, ils sont créés, gérés et supprimés par le système selon le besoin, pour chaque et chaque action pour laquelle il faudrait gérer une autorisation un tel rôle sera créé.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

`Modèle RBAC simplifié pour Authentic`

Rôles techniques d'administration

Pour permettre un découpage à gros grain de l'administration on ajoute le concept d'organisation, chaque objet (y compris les utilisateurs et les rôles) appartiennent à une organisation. Un rôle technique d'administration général est associé à chaque organisation, c'est l'équivalent du rôle super-utilisateur classique mais contraint à une organisation donnée. Les organisations sont structurées en arbre, une organisation peut contenir d'autres organisations et ses administrateurs ont tout pouvoir sur ces sous-unités administratives.

Pour chaque type d'objet on ajoute dans chaque organisation des rôles techniques d'administration de ces objets, le rôle technique d'administration général en hérite.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

`Vue des rôles techniques d'administration avec une unique unité administrative`

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

`Vue sur les rôles techniques d'administration avec plusieurs unités administratives hiérarchisées`

Rôle technique d'administration des rôles

Pour chaque rôle R (technique ou pas) un rôle technique d'administration Ra est crée. Il désigne les utilisateurs ayant le droit d'ajouter ou d'enlever des membres à ce rôle ainsi que de faire hériter un autre rôle de ce même rôle. Cette dernière opération revenant à affecter tous les membres de l'autre rôle au rôle administré, il est logique de le rendre possible.

Les rôles d'administration des rôles sont particuliers en ce qu'ils contrôlent leur propre administration, i.e. l'administrateur d'un rôle pourra toujours déléguer son pouvoir à un autre, i.e. il est aussi administrateur du rôle d'administration. Ceci pour éviter une récursion infinie au niveau des rôles d'administration des rôles qui aurait eu besoin d'un rôle d'administration à leur tour. On dit que ces rôles sont 'auto-administrés'.

Pour rendre n'importe quel rôle 'auto-administré' il suffit de lui faire hériter de son rôle d'administration.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

Rôles techniques de gestion des accès

TODO Pour chaque object ayant besoin d'un accès on crée un rôle technique par exemple pour un service SAML w.c.s. on créera un rôle accès w.c.s, il donne accès ce service, sans lui l'IdP ne répondra pas.

À supposer que l'IdP propose de modéliser les rôles applicatifs, ils seront reproduits du coté d'authentic par des objets spécifiques, pour chacun de ces objets authentic créera un rôle d'accès du même nom. Ce rôle héritera du rôle d'accès de base.

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" *

"/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

Visibilité

Il peut se poser la question de savoir si un administrateur d'un rôle dans organisation fille doit pouvoir voir les utilisateurs ou les rôles de l'organisation parente ou d'une organisation sœur quand il administre son rôle. Pour l'instant nous écartons ce problème et le déclarons hors-scope. Dans toutes les situations où un utilisateur est amené à choisir un utilisateur, ajouter un membre à un rôle, ou un rôle sans nécessité d'une permission particulière[1] tous les utilisateurs ou rôles seront visibles.

[1] par exemple pour hériter d'un rôle il faut être administrateur de celui-ci, il ne sera donc pas possible de voir dans la liste les rôles qu'on administre pas

IHM

Le graphes des rôles est un graphe dirigé complexe qu'on essayera pas de représenter. On aura comme actuellement avec les groupes une vue alphabétique de la liste de tous les rôles, et pour chaque rôle la liste de ses membres (directs et indirects via l'héritage). On y ajoutera deux nouveaux onglets: la liste des rôles dont il hérite et la liste des rôles qui héritent de lui. Tout au plus les services pourront indiquer des relations hiérarchiques de représentation pour certains rôles techniques, ceux-ci ayant généralement des relations d'héritage simples entre eux. Ainsi il sera intéressant dans l'exemple plus haut de présenter le rôle d'accès w.c.s. comme racine d'un arbre dont les catégories en sont les branches.

Chaque organisation disposera d'une vue d'accueil présentant l'accès aux 2 objets gérés principaux les utilisateurs et les rôles. Il y sera aussi présents un bouton d'accès pour chaque sous-organisation. Les [xxx] sont des liens. [-] est un bouton de suppression, [/] un bouton de suppression grisé.

```
Agglo

   [Agglo           ]    [Ville1          ]   [Ville2] | [Ville3] | [Ville 4]
   | → utilisateurs |    | → utilisateurs |   ...
   | → (à réfléchir)|
   |                |
```

> Benj m'a dit qu'on laissait tomber cet affichage des utilisateurs par organisation (ville), c'est pas gérable quand il y a beaucoup de ville (+ de 1000 au CDG59 actuellement et beaucoup aussi dans l'AO en cours). Du coup on ne verra que les utilisateurs pour lesquels on a les droits nécessaires. Affichage sous forme de liste paginée avec une colonne indiquant l'organisation à laquelle appartient l'utilisateur.
> Idem pour les rôles.

`Accueil du manager d'authentic`

```
[Agglo] > Ville1

   [Utilisateurs] | [Rôles] | [Services SAML]

-----

   [Service enfance] [Service état civil]
```

`Accueil du manager d'authentic pour la sous-organisation ville1`

```
[Agglo] > [Ville1] > Utilisateurs

 Recherche: _________________ [Créer un nouvel utilisateur]

    Nom | Prénom | Email
1 [xxx | xxx    | xxx@xxx ]
2 [yyy | yyy    | yyy@yyy ]

   [1] [2] .. [5] [6]
```

> Dans le cadre de Publik, on s'est mis d'accord sur le fait que l'accueil du /manage d'Authentic était superflu : il ne contient rien qui ne soit déjà exposé sur le portail agent (hobo/combo). Benj est ok en dépit de ce qu'il écrivait ici #7088

`Administration des utilisateurs de ville 1`

```
 [Agglo] > [Ville1] > [Utilisateurs] > Utilisateur 1

  Informations | [ Rôles ]

  Nom:     xxxx_____       [Renvoyer un mot de passe]
  Prénom:  xxxx_____
  Email:   xx@xx____       [Forcer le changement du |
                           |au prochain login       ]
   [1] [2] .. [5] [6]
```

`Administration des informations personnelles de l'utilisateur 1 de ville 1`

```
 [Agglo] > [Ville1] > [Utilisateurs] > Utilisateur 1

  [Informations] | Rôles

  |   | Nom
  -------------------------
  | 1 | Administrateur Ville 1 [-]
  | 2 | Administrateur de service enfance de ville 1 (rôle hérité) [/]
  | 3 | W.C.S (rôle hérité) [/]
  | 4 | W.C.S :: Service enfance [-]
  |

  Ajouter un rôle: _____ [Ok]
  `Vous devez être administrateur d'un rôle pour pouvoir l'ajouter`
```

(possibilité de clic sur "rôle hérité" pour avoir des infos du comment)

`Administration des rôles de l'utilisateur 1 de ville 1`

```
 [Agglo] > [Ville1] > Rôles

  Recherche: _____ [Créer un nouveau rôle]

 |   | Nom                                          | Technique
 -------------------------------------------------
 | 1 | Administrateur de ville 1                    |   Oui
 | 2 | +-- Gestion des utilisateurs                 |   Oui
 | 3 | +-- Gestion des rôles                        |   Oui
 | 4 | +-- Gestion des services SAML                |   Oui
 | 5 | +-- Administration du service enfance        |   Oui <- à voir si on fait aussi apparaître les
rôles d'administration du niveau n au niveau n+1
 | 6 | +-- Administration du service état civil     |   Oui
 | A | +-- Administration "élu"                     |   Oui
 | 7 | Accès à W.C.S.                               |   Oui
 | 8 | +--- Service Enfance                         |   Oui
 | 9 | +--- Service état civil                      |   Oui
 | B | +--- Élu                                     |   Oui
 |10 | Élus                                         |   Non
```

(suggestion : mettre dans un onglet différent les rôles d'administration des rôles (5, 6, A))

(injonction : retirer la colonne technique)

`Administration des rôles de ville 1`

```
 [Agglo] > [Ville1] > [Rôles] > Élus

  Membres | [Rôles hérités] | [Rôles héritants]

  |   | Nom | Prénom | Email    | Membre direct
  ---------------------------------------------
  | 1 | xxx | xxx    | xxx@xxx  | Oui  [-]
```

```
  | 2 | yyy | yyy    | yyy@yyy  | Non  [/]
  | 3 | zzz | zzz    | zzz@zzz  | Oui  [-]
  ....

  [1] [2] .. [3] [4]

  Ajouter un membre: _____________ [Ok]
```

(rôles hérités → rôles dont on est membre) (rôles héritants → rôles "membres de")

`Administration des membres du rôle Élus`

```
 [Agglo] > [Ville1] > [Rôles] > Élus

  [Membres ] | _Rôles hérités_ | [Rôles héritants]

  |   | Nom du rôle
  ---------------------------------------------
  | 1 | W.C.S :: Élu

  Ajouter un rôle hérité: _____________ [Ok]
  `Pour pouvoir ajouter un rôle hérité vous devez être administrateur de ce rôle`
```

`Administration des rôles hérités du rôle Élus`

```
 [Agglo] > [Ville1] > [Rôles] > Élus

  [Membres ] | [Rôles hérités] | _Rôles héritants_

  |   | Nom du rôle                          |
  ---------------------------------------------
  | Aucun rôle héritant                      |

  Ajouter un rôle héritant: _____________ [Ok]
```

`Administration des rôles hérités du rôle Élus`