Quarantaine et remédiation : communiquer pour ne plus bloquer

Sébastien Beaudlot
Direction Opérationnelle des Systèmes d'Information
Avignon Université
74 Rue Louis Pasteur
84029 AVIGNON CEDEX

Jade Tavernier
Direction Opérationnelle des Systèmes d'Information
Avignon Université
74 Rue Louis Pasteur
84029 AVIGNON CEDEX

Maxime Charpenne
Direction Opérationnelle des Systèmes d'Information
Avignon Université
74 Rue Louis Pasteur
84029 AVIGNON CEDEX

Résumé

Les raisons d'interagir hors processus formalisés avec nos utilisateurs sont variées : validité de leurs identifiants, signature de la charte d'usage des services numériques, comptes bloqués pour envoi de spam, etc. De par la criticité de ces événements ou la nécessité d'interagir avec les usagers, les procédures associées sont souvent manuelles et les identités numériques sont parfois impactées (blocage ou suspension).

Les agents intervenant sur les identités numériques et ceux étant en contact avec leurs propriétaires ne sont pas les mêmes. La communication est alors laborieuse et les conséquences parfois préjudiciables. Le processus d'authentification étant un passage obligé pour tous les usagers, c'est le moment idéal pour leur présenter de l'information et leur permettre de se débloquer en toute autonomie.

En associant des procédés de mise en quarantaine et de remédiation, nous tentons d'adresser des problèmes communs à toutes les populations par la communication :

- *La quarantaine capte l'attention au moment de la saisie des identifiants ;*
- *L'application d'information-remédiation permet le suivi des blocages et de leur résolution.*

Autour des services communs et éprouvés que sont CAS et LDAP, nous avons construit une application et une API pour répondre à ces deux besoins : mise en quarantaine et remédiation autonome.

Mots-clefs

Quarantaine, remédiation, blocage, identité numérique, CAS, LDAP, API

1 Introduction

En pratique, les raisons nécessitant d'attirer l'attention d'un usager sur un événement lié à son identité numérique sont hétéroclites. Cet événement peut conduire à bloquer l'utilisation de l'identité numérique et on ne peut plus interagir avec l'utilisateur. On devient donc dépendant d'un échange (présentiel, téléphone) avec l'usager pour débloquer la situation.

Par exemple, à Avignon Université, on remarque une recrudescence des campagnes de vols de mot de passe par hameçonnage qui nécessitent, pour chaque vol, des interventions manuelles :

- à réception du message de RENATER avertissant du blocage de la messagerie pour compromission, le compte de l'usager est bloqué afin d'empêcher son utilisation à des fins délictueuses.
- un membre du service informatique explique à l'usager ce qui s'est produit et comment renforcer sa vigilance pour éviter de communiquer à nouveau ses identifiants.

D'autres motifs peuvent justifier le blocage total d'un compte : détection d'activité réseau malveillante, fin de période de grâce après la fin d'un contrat, ou tout autre motif adapté aux usages de l'établissement.

Avant la mise en place du projet faisant l'objet de cet article, la méthode employée consistait en une réinitialisation aléatoire du mot de passe du compte concerné. Si cette action a le mérite d'être très efficace pour empêcher l'utilisation de l'identité numérique, elle fait cependant preuve d'une grosse lacune en termes de communication auprès de l'usager. Ce dernier n'a aucun moyen de savoir qu'il a été bloqué (les services affichant alors une erreur dans la saisie des identifiants) et cet état peut lui être préjudiciable (exemple d'un étudiant devant utiliser la plateforme d'enseignement numérique pour un examen). Par ailleurs, il ne connaît pas les raisons du blocage de son compte. D'autre part, l'absence de formalisation du blocage engendrait des difficultés au sein du service informatique : ce statut n'étant pas associé au compte, le partage de l'information entre collègues était chronophage et ne permettait pas de gérer l'assistance aux utilisateurs de manière cohérente.

Devant ce constat, nous avons souhaité mettre en place des outils permettant :

- d'empêcher l'authentification sans modifier le mot de passe ;
- de communiquer lors de la tentative d'authentification d'un compte bloqué le motif du blocage et les démarches que peut entreprendre son propriétaire afin de le débloquer.

Comme le motif du blocage est concrétisé par un état formel associé à l'identité numérique, il est très facilement partagé au sein du service informatique sans devoir mettre en place un processus particulier.

Dans cet article, nous allons détailler la solution que nous avons mise en œuvre, basée sur trois briques :

- La majorité de nos services utilisant le protocole CAS, nous avons choisi de nous appuyer sur la fonctionnalité *Authentication Interrupt* de CAS et d'agir au niveau du système d'authentification *Single Sign On* (SSO).
- L'annuaire LDAP, point central de notre système d'information, est utilisé pour stocker les motifs de quarantaines et l'état de quarantaine de chaque compte.
- Enfin, une application développée par nos soins fournit une interface à ce nouveau flux de communication en présentant les motifs de blocages et en redirigeant l'usager bloqué vers les services de remédiation idoines.

Le projet, pensé pour être à terme mis à disposition de la communauté, propose une architecture permettant d'intégrer des motifs de quarantaines divers, à la discrétion de chaque établissement souhaitant implémenter ce principe. Les technologies employées (Apereo CAS, LDAP) ont été choisies dans ce but, car elles sont largement répandues au sein de la communauté université / recherche.

2 Principe de fonctionnement

Notre solution repose sur la possibilité d'interrompre une authentification CAS en laissant le soin à une source externe de décider si cette authentification doit être poursuivie ou refusée. Nous appelons « quarantaine » la raison particulière d'empêcher l'usage normal d'un compte.

Une quarantaine est définie par un identifiant, un nom et une description (présentés aux utilisateurs), le nombre de fois où elle peut être reportée par l'utilisateur, la durée de chaque report et, le cas échéant, un moyen de remédiation. Certaines quarantaines peuvent interdire la remédiation autonome et obliger l'usager à se présenter auprès d'un intervenant pour résoudre le problème.

La quarantaine est appliquée à un compte par une API. Dans ce contexte, le projet ne fournit que l'API : il appartient au responsable de la quarantaine de prévoir les outils, manuels ou automatique, permettant de l'appliquer lorsque l'événement lié survient. Par exemple : pour une quarantaine forçant le remplacement d'un mot de passe expiré, il faut éxécuter un script quotidien vérifiant l'âge de tous les mots de passe qui appellera l'API pour poser la quarantaine idoine sur chaque compte dont le mot de passe est trop ancien.

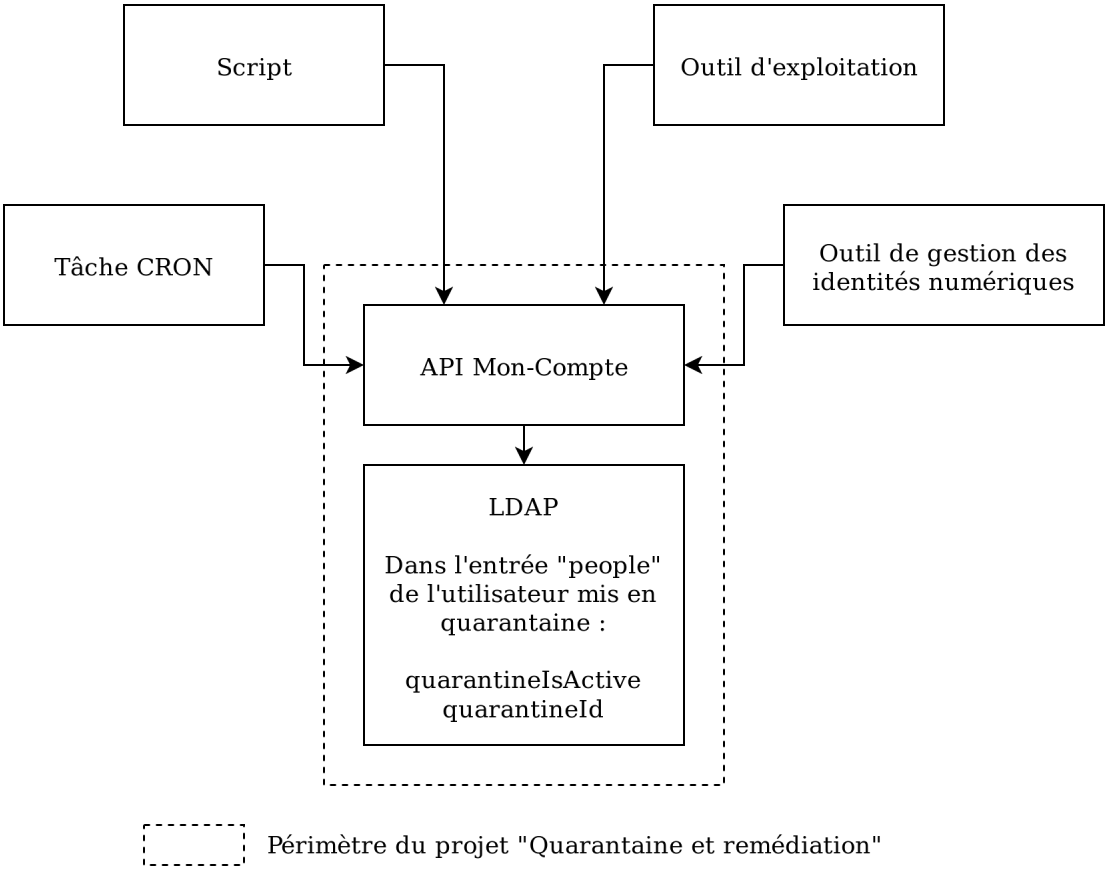

Figure 1 - Pose de quarantaine, manuellement ou automatiquement, après un événement. Les mécaniques de pose de quarantaine faisant appel à l'API sont hors périmètre du projet.

Si une quarantaine a été posée, l'authentification SSO est alors bloquée et lorsque l'utilisateur se connecte, il est redirigé vers une application lui montrant :

- la ou les quarantaines qui sont appliquées, avec de préférence une explication. ;
- les moyens pour lever cette quarantaine quand c'est possible.

Un script en langage Groovy (méthode la plus adaptée parmi celles proposées par Apereo CAS, permettant de disposer d'attributs issus du LDAP au sein du traitement) est systématiquement appelé lors d'une tentative d'authentification afin de vérifier la valeur de l'attribut *quarantineIsActive* (la source de cet attribut est détaillée au chapitre suivant).

Si l'attribut est absent ou vaut *false*, cela signifie que le compte ne fait l'objet d'aucune quarantaine et l'authentification se poursuit normalement.

Si l'attribut vaut *true*, le compte est sous le coup d'au moins une quarantaine et doit être bloqué. L'usager en est alors averti par une page spéciale présentée par le CAS et est renvoyé vers l'application « Mon compte » qui l'informe en détails des motifs de ce blocage et des moyens d'y remédier.

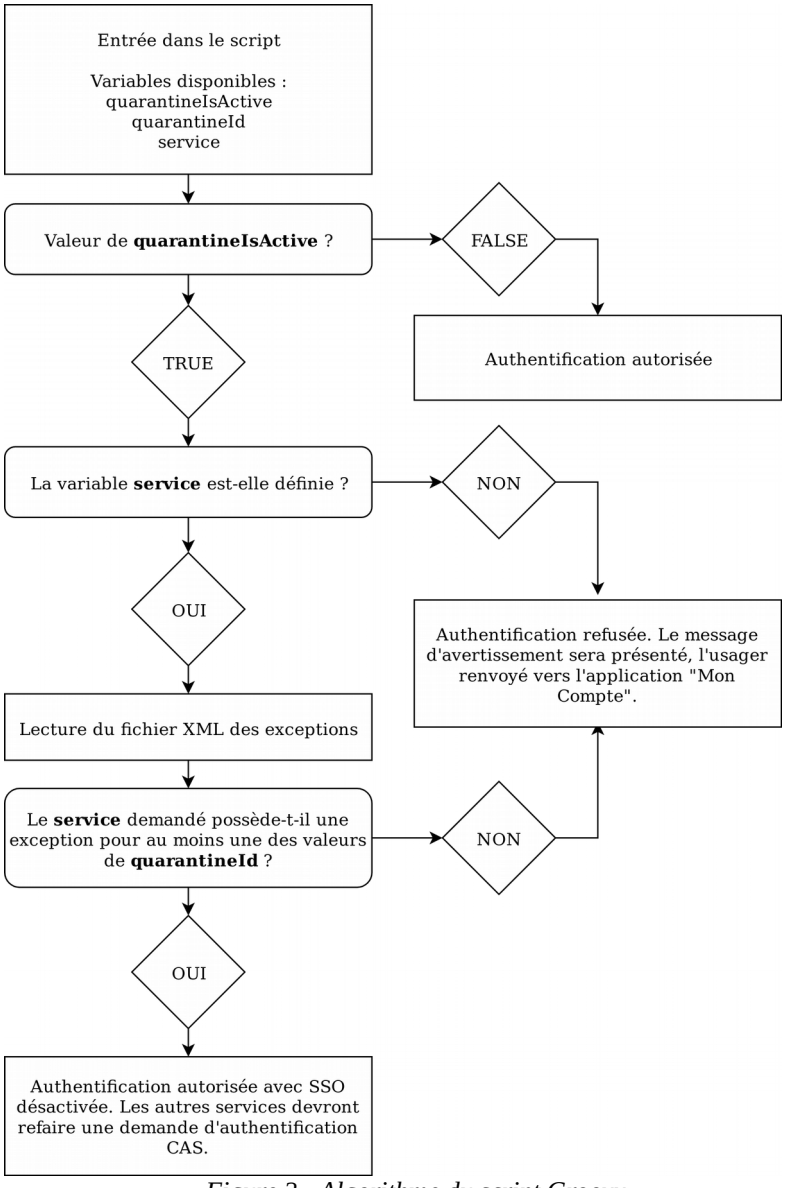

Figure 2 - Algorithme du script Groovy

Lorsqu'un service doit être accessible malgré la présence d'une quarantaine active, des exceptions sont possibles. C'est par exemple le cas pour l'application « Mon compte » ainsi que pour les services de remédiation. Pour cela, on associe la liste des motifs à ignorer à la définition d'un service CAS. L'authentification n'est alors que partielle, le protocole CAS n'autorisant l'accès que pour le service ayant demandé l'authentification (désactivation du *Single Sign On*).

Sur l'application « Mon Compte », l'utilisateur peut, pour chaque quarantaine :

- **La résoudre immédiatement** : il est alors renvoyé vers le service de remédiation défini pour cette quarantaine, sur lequel il entreprend les actions nécessaires à la résolution du problème. On peut aussi choisir de ne pas proposer de remédiation autonome et informer l'usager qu'il doit se présenter en personne ou par un moyen dématérialisé. La quarantaine résolue, elle est entièrement levée et disparaît du compte. Ses attributs LDAP sont supprimés, puis l'utilisateur est ramené vers « Mon Compte » pour poursuivre la résolution des problèmes ou, s'il n'y en a plus, continuer son authentification.
- Si la quarantaine l'autorise, l'usager peut choisir de **reporter la résolution du problème**. Lorsque la résolution est reportée, la quarantaine reste présente mais devient inactive. L'attribut *quarantineId* est supprimé, l'attribut *quarantineStatus* est créé ou mis à jour afin de conserver les informations sur le report : nombre de reports effectués, date du dernier report. Les futures tentatives d'authentification ne seront pas impactées. À l'issue de la période de report, la quarantaine est réactivée (retour de l'attribut *quarantineId*) et devient à nouveau bloquante.

A chaque action sur une quarantaine, l'attribut *quarantineIsActive* est recalculé : en présence d'au moins une quarantaine active (donc de la présence d'au moins un attribut *quarantineId*), il reste *vrai*. Sinon, il devient *faux*.

Lorsqu'un choix (résolution ou report) a été fait pour toutes les quarantaines actives, l'authentification se termine normalement.

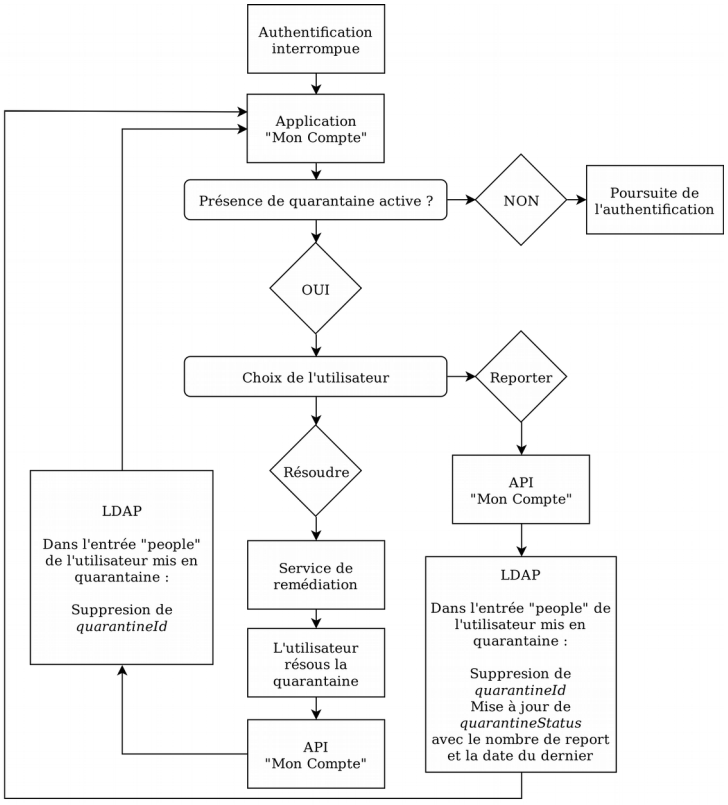

Figure 3 - Cheminement de l'utilisateur renvoyé vers l'application « Mon Compte »

3 LDAP

L'annuaire LDAP est utilisé pour stocker d'une part la liste détaillée des motifs de quarantaine et d'autre part l'état actuel de chaque compte utilisateur vis-à-vis des quarantaines.

3.1 Motifs de quarantaine

La liste détaillée des motifs de quarantaine est stockée dans une nouvelle branche de l'annuaire LDAP : *quarantine.*

Dans cette branche, chaque entrée comporte 4 attributs :

- *quarantineId* : le nom court du motif de quarantaine, faisant office de référence.
- *quarantineName* : le nom complet du motif de quarantaine (internationalisation possible).
- *quarantineDescription* : la description du motif de quarantaine, telle que présentée à l'usager bloqué (internationalisation possible).
- *quarantineParameters* : les options du motif de quarantaine et de son service de remédiation, à savoir :
  - *type* : la nature du service de remédiation (*url* pour un site web ; levée manuelle de la quarantaine après discussion)
  - *delay* : le nombre et la durée des reports possibles pour ce motif
  - *target* : l'adresse du service de remédiation

objectClass	***top (abstract)***
objectClass	***userQuarantineDef (structural)***
quarantineDescription	{ "fr": "Pour diverses raisons, veuillez changer votre mot de passe.", "en": "For some reasons, please change your password." }
quarantineId	**chpw**
quarantineName	{ "fr": "Changement du mot de passe", "en": "Changing password" }
quarantineParameters	{ "type": "url", "delay": ["1h", "2h", "3h"], "target": "https://mon-compte-test.univ-avignon.fr/mdp" }

Figure 4 - Exemple d'entrée de la branche quarantine

3.2 Motifs de quarantaine

L'état des comptes utilisateurs vis-à-vis des quarantaines est stocké dans des attributs ajoutés aux entrées de la branche *people*. Pour chaque compte utilisateur, on prévoit les 3 attributs suivants :

- *quarantineIsActive* : booléen, état global de quarantaine. Vrai si au moins une quarantaine est active.
- *quarantineId* : chaîne, multivalué. Identifiants des quarantaines actives.
- i : JSON, multivalué. Pour chaque quarantaine (*quarantineId*), active ou reportée/inactive, cet attribut stocke le nombre de reports (*nbBypass*) et la date du dernier report (*lastByPass*). Ces informations permettent de réactiver la quarantaine au bon moment ou de ne plus autoriser le report le cas échéant.

quarantineId	chpw
quarantineIsActive	**FALSE**
quarantineStatus	{"quarantineId":"chpw","nbByPass":1,"lastByPass":"2019-06-26 11:38:03"}

Figure 5 - Exemple d'attributs ajoutés à une entrée de la branche people

4 CAS

Disponible à partir de la version 5.3 de CAS, la mécanique *Authentication Interrupt* permet de *« mettre en pause et d'interrompre le flux d'authentification pour appeler des services et ressources externes, fournissant des états et paramètres susceptibles de guider la façon dont CAS doit gérer et contrôler la session SSO »*. [1]

Parmi toutes les implémentations de cette mécanique, nous choisissons d'utiliser un script Groovy. Ce script reçoit les attributs fournis par CAS au moment de la tentative d'authentification *(quarantineIsActive, quarantineId, quarantineStatus)* et le *service* d'origine (afin de renvoyer l'usager au bon endroit après une procédure de remédiation).

Afin que l'application « Mon compte » et les services résolvant les quarantaines puissent être authentifiés, il est indispensable de gérer une mécanique d'exception.

5 Gestion des exceptions

Le script Groovy utilisé par CAS lors de la phase *Authentication Interrupt* lit un fichier XML contenant une liste, par service (au sens CAS du terme), des motifs de quarantaine autorisés. Si au moins une des quarantaines autorisées pour un service est active pour l'utilisateur en train de s'authentifier, l'accès à ce service est autorisé mais le *Single Sign On* est désactivé pour limiter l'authentification à ce seul service.

Afin de maintenir facilement la liste des exceptions, le fichier XML sera généré depuis les informations contenues dans les commentaires des fichiers JSON définissant les services CAS. Au début de chaque fichier définissant un service, les exceptions sont saisies selon cet exemple :

```
/*
 motif-1
 motif-2
*/
```

Ou, dans le cas où le service doit être autorisé systématiquement (par exemple, pour l'application « Mon compte ») :

```
/*
 ALL
*/
```

NB : Le mot clé ALL est réservé et ne doit pas être employé comme valeur de quarantineId

La génération du fichier XML est facilement adaptable si une autre méthode a été retenue pour la définition des services CAS.

6 L'application « mon compte »

Nous avons décidé d'implémenter une application « Mon compte » permettant de regrouper tout ce qui concerne l'utilisateur connecté. Cette application est organisée en sous-modules dont « QuarMed » qui nous intéresse dans cet article.

Elle est développée avec Angular 7 pour le front office et Symfony 3 pour l'API back office, des outils déjà employés et maîtrisés par la DOSI.

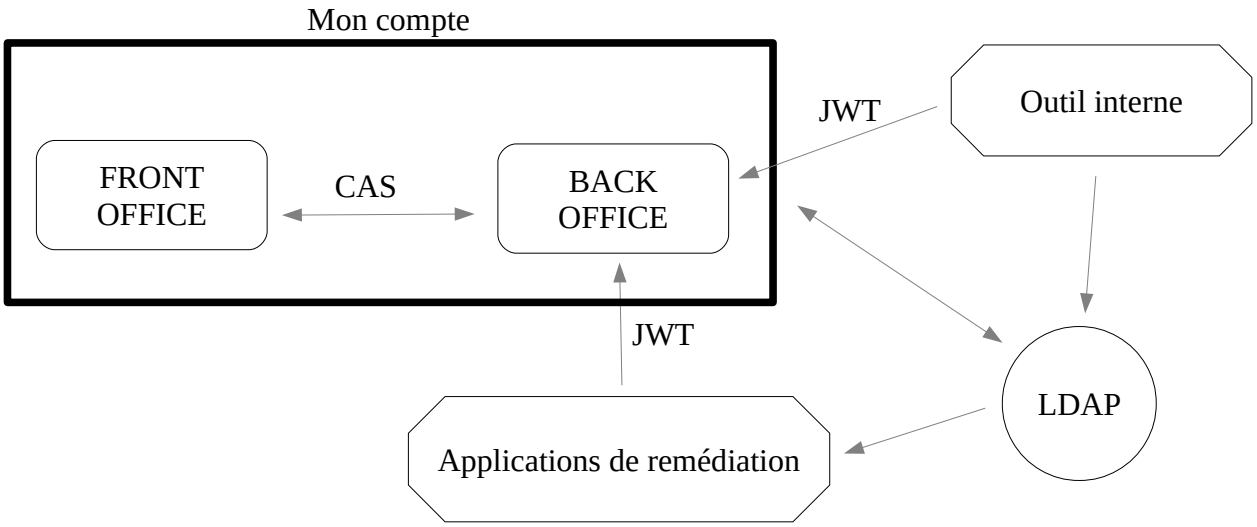

Figure 6 - Interactions de l'application « Mon Compte »

6.1 Front office

Le front office permet à l'utilisateur de :

- visualiser les informations des quarantaines actives et inactives associées à son compte :
  - Noms (*quarantineName*)
  - Descriptions (*quarantineDescription*)
  - Dates d'activations pour les quarantaines inactives (*quarantineStatus*);
- reporter les quarantaines actives si cela est autorisé dans leur paramétrage ;
- résoudre les quarantaines actives et inactives.

6.2 Back office

Le back office est appelé par le front office pour effectuer des actions comme récupérer les quarantaines actives ou encore reporter une quarantaine.

L'API dispose de deux types d'authentification :

- Une authentification « CASsifiée » pour le Front office
- Une authentification JWT pour les applications voulant résoudre ou reporter une quarantaine (appelées applications de remédiation)

6.3 Taches récurrentes

Nous planifions l'exécution régulière d'une tâche (CRON) permettant de basculer les quarantaines inactives (pour lesquelles l'utilisateur a choisi de reporter l'action) en actives. Les conditions d'activation (délai de report, nombre de reports autorisés) sont déterminées par les paramètres associés aux quarantaines.

6.4 Outils de visualisation et de gestion des quarantaines

Certaines équipes, notamment le pôle assistance informatique, ont besoin de disposer d'une interface leur permettant de voir l'état d'un compte (quarantaines actives et inactives sur un compte donné…) et de reporter ou supprimer une quarantaine sur un compte en cas de besoin (par exemple pour un étudiant bloqué lors d'un partiel ou la résolution de quarantaines pour lesquelles l'utilisateur n'est pas autonome.)

Afin de ne pas disperser les tâches d'exploitation du pôle assistance, nous n'avons pas inclus cette visibilité ni ces actions dans l'application *Mon compte*. Ces fonctions ont été intégrées à un outil interne existant, *Easymin*, qui couvre déjà la majorité des tâches courantes de la DOSI.

Le mode ajouté sur *Easymin* permet de voir les quarantaines posées sur un compte, de poser ou lever une quarantaine manuellement et de forcer la suppression d'une quarantaine non résolue (pour pallier une éventuelle défaillance).

Ces actions pourraient êtres prévues au sein de l'application Mon Compte dans une future version du projet.

7 Perspectives

La mise en production de la première quarantaine (la compromission du compte PARTAGE) est imminente (au moment de la rédaction de l'article) et nous pourrons communiquer nos premiers retours à l'occasion de la présentation aux JRES.

Le principal défaut de la solution retenue est qu'elle ne couvre, en l'état, que les authentifications via CAS. Les autres méthodes d'authentification (LDAP, ouverture de session Windows, Wifi, etc …) ne seront pas affectées par la présence de quarantaines. Nous avons cependant choisi de commencer à passer la solution en exploitation, les services authentifiés par CAS représentant déjà une part non négligeable des authentifications.

Les services s'appuyant sur les autres méthodes devront faire l'objet d'un travail d'intégration pour prendre en compte la gestion des quarantaines. Pour cela, nous avons de nombreuses pistes : filtrage LDAP sur l'attribut quaratineIsActive, SAML (pouvant être fourni par Apereo CAS), activation / désactivation intégrées au flux de pose / levée de quarantaines.

Ces pistes étant nombreuses, variées et spécifiques au périmètre d'authentification de chaque établissement, il conviendra d'envisager au cas par cas, pour chaque produit ou service authentifié, l'intégration complète de ce processus.

Nous prévoyons également d'améliorer le système de gestion des exceptions afin de gérer un principe de priorité permettant d'assurer qu'une quarantaine critique soit bloquante même en présence d'autres quarantaines non critiques.

Bibliographie

[1] Authentication Interrupt. Documentation officielle de la fonction pour Apereo de CAS 5.3.x ; https://apereo.github.io/cas/5.3.x/installation/Webflow-Customization-Interrupt.html