

# Automatisation et délégation de traitements avec Rundeck

## David CHOCHOI

Académie de Dijon  
2G rue du Général Delaborde  
21000 DIJON

## Guillaume LAVILLE

Académie de Dijon  
2G rue du Général Delaborde  
21000 DIJON

## Résumé

*Dans les SI actuels, les services sont de plus en plus distribués sur de nombreux serveurs, physiques ou virtuels.*

*Comment avoir une vue synthétique des tâches programmées et leur résultat d'exécution ? Comment déléguer certaines actions sensibles de manière isolée, sécurisée et traçable ? Comment automatiser facilement des scénarios et ainsi économiser des manipulations, sans compromettre la sécurité ?*

*Rundeck est une réponse à toutes ces problématiques, testée et mise en place au sein du rectorat de l'Académie de Dijon (environ 300 serveurs pour 46 000 personnels).*

*Cet outil permet de décrire et d'automatiser les processus quotidiens d'une infrastructure informatique.*

*Il fournit également une API REST permettant son intégration dans des applications tierces existantes ou créées pour répondre à des besoins spécifiques.*

*Cet article s'articule en cinq parties :*

- les facteurs ayant amené à cette réflexion et le choix de Rundeck ;*
- une présentation de l'outil Rundeck et de ses fonctionnalités ;*
- l'illustration de la manière dont il peut s'intégrer à des processus de travail existants par le biais de trois exemples ;*
- l'utilisation de l'API REST Rundeck pour s'intégrer avec d'autres applications ;*
- la sécurisation des serveurs, des travaux et des règles d'accès.*

*En conclusion, il se focalise sur les évolutions supplémentaires que peut encore apporter Rundeck dans le cadre d'une structure institutionnelle comme le rectorat.*

## Mots-clefs

*Rundeck, orchestration, délégation, exploitation, tâches, intégration, sécurisation, ACL, REST*

## 1 Introduction

Dans cet article nous présentons le résultat du déploiement de l'outil Rundeck au sein de l'académie de Dijon dans le cadre d'une expérimentation visant à automatiser les traitements existants. Nous utilisons cet outil depuis plusieurs mois pour une quantité croissante de nos traitements informatiques, ce qui nous a permis d'explorer ses différentes possibilités et les manières de l'intégrer dans un système d'information existant, celui de la DSI.

## 2 Contexte

Les ingénieurs du service d'exploitation de l'académie de Dijon sont confrontés à deux problèmes.

D'une part, le suivi des multiples tâches programmées de manière indépendante sur chaque serveur sans gestion globale. Celles-ci peuvent être des sauvegardes, des scripts de maintenance ou des traitements métier, déclenchés à heure fixe ou sur des conditions particulières.

D'autre part, du fait de leurs autorisations étendues, la nécessité d'effectuer de nombreux actes techniques pour le compte des autres services, tels que l'assistance académique. Le fait de dépendre des ingénieurs d'exploitation ralenti le traitement des demandes des utilisateurs et interrompt également les travaux sur les projets en cours.

Pour améliorer cette situation, les besoins du service sont les suivants :

- rassembler l'ensemble des traitements automatiques dans une seule interface ;
- avoir des rapports et une visibilité sur le résultat de l'exécution de ces traitements ;
- permettre de déléguer des actions techniques à des personnels extérieurs à l'équipe d'exploitation sans compromettre la sécurité et l'intégrité du système d'information ;
- rendre possible le contrôle des traitements au moyen d'une API depuis d'autres outils de gestion déjà présents au niveau académique.

Pour répondre à ces besoins, nous avons étudié et mis en œuvre l'outil Rundeck qui nous a été suggéré par les équipes ministérielles.

## 3 Rundeck

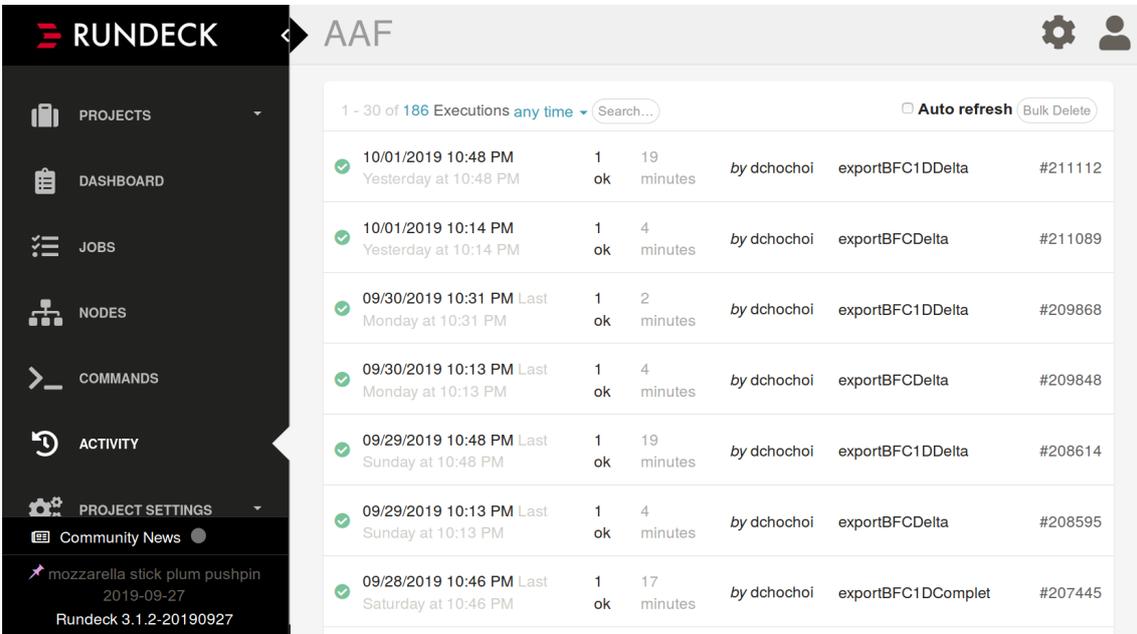
### 3.1 Présentation des fonctionnalités

Rundeck [1] est un logiciel libre sous licence Apache. Il s'agit d'un orchestrateur, c'est-à-dire un logiciel permettant d'automatiser des tâches sur un ensemble de serveurs. Ces tâches ou travaux sont associés à des projets et s'exécutent sur des nœuds qui représentent des serveurs du système d'information.

Une tâche est définie en 6 parties :

- son identité : nom, description ;
- son déroulement : les options, les différentes étapes à réaliser et la stratégie d'exécution de ces étapes ;
- ses cibles : le ou les nœuds sur lesquels elle sera exécutée ;
- sa planification : une exécution à la demande ou de manière récurrente ;
- ses résultats : l'envoi d'un rapport par mail, l'appel d'une adresse de retour applicative, etc.
- ses réglages : le niveau de verbosité des journaux, d'éventuelles limites de temps, un nombre de tentatives maximum.

Rundeck dispose d'un panneau complet au suivi de l'activité des travaux de chaque projet. Celui-ci permet de consulter les résultats de chaque exécution et d'avoir une vue synthétique sur les éventuelles erreurs qui ont pu se produire.



| 1 - 30 of 186 Executions any time Search... |  |         |               |             |                   |         | Auto refresh Bulk Delete |
|---|--|---------|---------------|-------------|-------------------|---------|--------------------------|
| ✓   | 10/01/2019 10:48 PM<br>Yesterday at 10:48 PM     | 1<br>ok | 19<br>minutes | by dchochoi | exportBFC1DDelta  | #211112 |                          |
| ✓   | 10/01/2019 10:14 PM<br>Yesterday at 10:14 PM     | 1<br>ok | 4<br>minutes  | by dchochoi | exportBFCDelta    | #211089 |                          |
| ✓   | 09/30/2019 10:31 PM Last<br>Monday at 10:31 PM   | 1<br>ok | 2<br>minutes  | by dchochoi | exportBFC1DDelta  | #209868 |                          |
| ✓   | 09/30/2019 10:13 PM Last<br>Monday at 10:13 PM   | 1<br>ok | 4<br>minutes  | by dchochoi | exportBFCDelta    | #209848 |                          |
| ✓   | 09/29/2019 10:48 PM Last<br>Sunday at 10:48 PM   | 1<br>ok | 19<br>minutes | by dchochoi | exportBFC1DDelta  | #208614 |                          |
| ✓   | 09/29/2019 10:13 PM Last<br>Sunday at 10:13 PM   | 1<br>ok | 4<br>minutes  | by dchochoi | exportBFCDelta    | #208595 |                          |
| ✓   | 09/28/2019 10:46 PM Last<br>Saturday at 10:46 PM | 1<br>ok | 17<br>minutes | by dchochoi | exportBFC1DComple | #207445 |                          |

Figure 1 - Interface de suivi des travaux d'un projet Rundeck

Une autre partie de l'interface logicielle permet une gestion fine des utilisateurs, des groupes et des règles d'accès. Nous développerons plus spécifiquement cette fonctionnalité dans une partie dédiée à la sécurité et la gestion des accès.

Rundeck offre enfin la possibilité d'installer des plugins permettant d'étendre les fonctionnalités de l'outil en termes de traitements pour s'interconnecter par exemple avec des outils d'intégration continue, des forges applicatives ou des services de stockage de données.

## 3.2 Installation et adaptations spécifiques à notre SI

Plusieurs méthodes sont disponibles pour l'installation de Rundeck :

- l'installation par le biais de paquets Debian/RPM natifs ;
- le lancement d'une archive Java de type WAR comprenant l'ensemble des fichiers du logiciel.

Dans le cadre de notre déploiement, nous avons privilégié le choix d'une plateforme Debian 9 comme base d'installation, par souci de cohérence avec le reste du parc de serveurs académique.

Rundeck permet quatre types d'authentification :

- au moyen d'un serveur SSO externe, en utilisant un serveur compatible OpenID tel que Okta ou Ping ;
- interne grâce à un des modules JAAS fournis (Java Authentication and Authorization Service). Trois mécanismes sont alors supportés : un fichier texte plat, un annuaire LDAP, ou le système d'autorisation PAM présent sur la plupart des systèmes UNIX ;
- par le biais d'un proxy authentifiant, configuré en frontal de Rundeck. Dans ce cas, l'utilisateur et le rôle sont indiqués dans l'environnement de chaque requête relayée. Il est alors important que Rundeck soit accessible uniquement par des serveurs mandataires de confiance, car il n'effectue plus aucune validation d'identité à son niveau.

N'ayant pas de serveur OpenID actuellement déployé, notre choix s'est rapidement orienté vers deux pistes : l'utilisation de notre annuaire LDAP ou l'utilisation de notre proxy authentifiant RSA Access Manager (anciennement ClearTrust).

Nous avons finalement préféré cette dernière solution pour deux raisons :

- la possibilité d'exiger une authentification forte OTP (One Time Password, avec token physique) pour l'accès depuis internet ;
- la conservation d'une session existante de type SSO si l'utilisateur est déjà authentifié sur d'autres outils académiques présents sur le même portail.

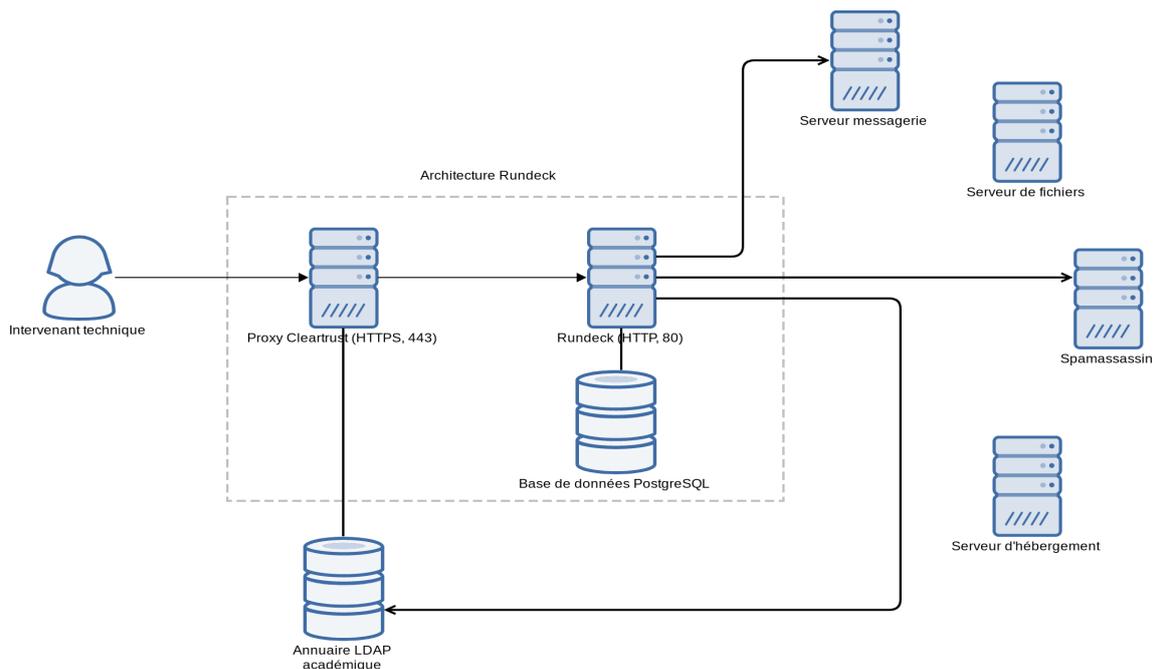


Figure 2 - Schéma d'architecture du déploiement Rundeck académique

Par défaut Rundeck fonctionne avec une base de données embarquée H2 pour stocker ses informations, mais il permet aussi l'utilisation d'autres SGBDR tels que PostgreSQL ou MariaDB.

Nous avons fait le choix d'utiliser PostgreSQL pour notre déploiement, selon les recommandations ministérielles. Ce choix permet de faciliter une future montée en charge en déportant à terme la base Rundeck sur un serveur ou un cluster dédié en fonction des besoins futurs.

## 4 Cas concrets d'utilisation

L'exploitation nécessite très souvent l'accès au compte root sur les infrastructures concernées, seule habilité à effectuer la plupart des commandes d'administration. Rundeck permet de déléguer ces opérations à des utilisateurs autorisés n'ayant pas les droits suffisants dans un environnement contrôlé.

Pour illustrer l'utilisation de Rundeck, nous allons décrire trois processus que nous avons pu mettre en place avec cette solution dans notre environnement académique.

### 4.1 Sauvegarde et maintenance d'une base PostgreSQL

Une partie importante des tâches automatiques effectuées dans un service informatique correspond à la sauvegarde et à la maintenance des bases de données présentes dans le système d'information.

Nous avons regroupé ces tâches dans un projet nommé « Backups » au niveau de notre instance Rundeck, qui comprend tous les travaux de ce type devant s'exécuter à une heure spécifique.

Le but est d'utiliser Rundeck comme une « crontab » afin de centraliser ce genre d'opérations.

Nous gérons plusieurs systèmes de gestion de bases de données tels que PostgreSQL, MariaDB, DB2 et Informix.

Dans cet exemple, nous prenons comme illustration une base de données PostgreSQL pour laquelle la maintenance comporte les étapes suivantes :

- une sauvegarde quotidienne au format binaire ;
- l'optimisation de la structure et la mise à jour des statistiques internes utilisées par le moteur de requêtes ;
- une fois par semaine, une réindexation complète de la base de données.

Nous avons mis en place deux travaux afin de gérer ces deux cycles de lancement.

Pour la première tâche de maintenance journalière, aucun script ni aucune donnée ne sont stockés directement sur le serveur Rundeck. Toutes les étapes correspondent à des appels de commandes distantes sur le serveur PostgreSQL concerné : « pg\_dump » pour la sauvegarde, « vacuumdb » pour la réorganisation des blocs et la mise à jour des statistiques d'optimisation. Le protocole utilisé pour toutes les communications est SSH, qui permet un échange totalement crypté et sécurisé entre les machines. Celui-ci nécessite au préalable l'enregistrement de la clé publique de Rundeck dans la configuration de chaque serveur.

Cette maintenance est programmée pour s'exécuter tous les jours à 21h00 et envoie un rapport d'exécution aux administrateurs en fin de traitement.

**Workflow** If a step fails:

Stop at the failed step.  Run remaining steps before failing.

**Strategy:** Sequential

Run each step in order. Execute a step on all nodes before proceeding to the next step

Explain >

**Global Log Filters** + add

Undo Redo

1. `$HOME/.bash_profile ; pg_dump -U pgilsun -h localhost -p 4001 -d lsun -Fc > /pg_backup/pgilsun/offline/lsun-$(date +%Y%m%d).sql`  
Backup Database
2. `$HOME/.bash_profile ; vacuumdb -a -z -v -p 4001 1>/home/pgilsun /vacuum.log 2>&1`  
Vacuumdb

+ Add a step

Cancel Save

Figure 3 - Définition des étapes pour la maintenance d'une base PGSQL

La seconde tâche hebdomadaire est elle aussi constituée d'un appel SSH à une commande distante, « reindexdb ». Elle s'exécute une fois par semaine le samedi à 23h10, en dehors des heures ouvrées de manière à s'assurer que l'application n'est pas en cours d'utilisation. Une notification de succès ou d'échec est également envoyée en fin d'exécution.

## 4.2 Création d'hébergements et de bases de données

Dans le cadre de son offre de service, le rectorat de Dijon propose plusieurs solutions d'hébergement aux établissements scolaires et aux projets portés au sein de l'académie.

Une de ces solutions est la mise à disposition d'espaces d'hébergement nus, pour déposer et gérer son propre site dans le cadre d'une charte. Pour cela, deux éléments sont fournis :

- un compte FTP associé à une adresse web, pour le dépôt de fichiers ;
- un compte d'accès à une ou plusieurs bases de données MySQL.

Ces espaces d'hébergement sont mutualisés sur un même serveur dont le matériel arrive en fin de support et l'architecture logicielle est vieillissante (environnement PHP 5.6, MySQL 5.5). Ce serveur héberge actuellement environ 500 sites.

Dans le cadre de la politique de sécurité académique, un nouvel environnement a été déployé, basé sur PHP 7.2 et un cluster MariaDB 10.2.

Le processus de migration de ces sites implique plusieurs acteurs dont le webmestre académique et les équipes système et réseau de la DSI.

Il doit respecter les étapes suivantes pour chaque site :

- la création d'un espace d'hébergement sur le nouveau serveur PHP 7.2 (équipe système) ;
- la recopie des données (fichiers et bases) sur le nouvel espace (équipe système) ;
- la validation de la compatibilité du site et de son bon fonctionnement (webmestre académique) ;
- la mise à jour des enregistrements DNS pour pointer vers le nouvel espace d'hébergement (équipe réseau) ;
- la clôture de l'ancien espace d'hébergement (équipe système).

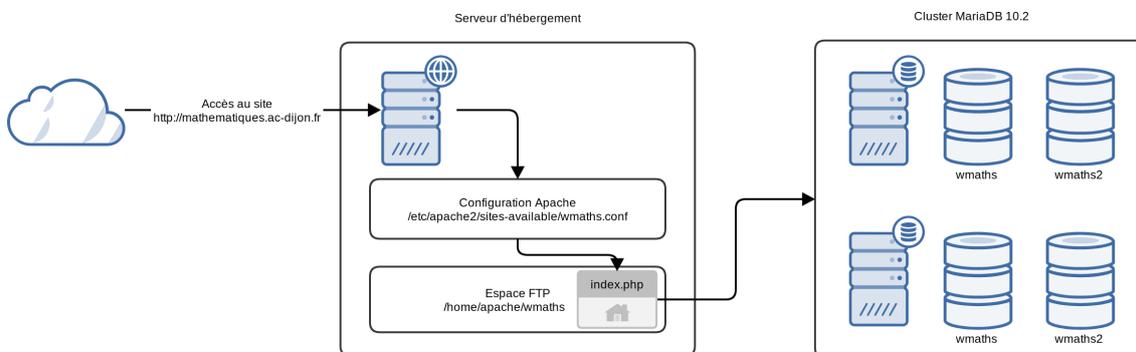


Figure 4 - Principe de fonctionnement d'un espace d'hébergement de site

Ce processus impliquant la validation de plusieurs acteurs humains, il n'est pas possible de le traiter en une seule tâche Rundeck.

Il est cependant intéressant, du fait du volume de sites à migrer, d'en automatiser les étapes répétitives et systématiques.

Elles sont essentiellement au nombre de deux : la création des nouveaux espaces d'hébergement et la recopie des données.

#### **4.2.1 Création de nouveaux espaces d'hébergement**

L'objectif de la migration sur la nouvelle plateforme nommée « webpublic2 » est également de régulariser la configuration et la nomenclature des espaces d'hébergement académique.

Pour cela, chaque espace d'hébergement est basé sur un identifiant unique, utilisé à la fois dans les chemins de stockage, dans le nommage des fichiers de configuration, de journaux et comme identifiant de connexion FTP et MySQL.

Par exemple, pour un site disciplinaire consacré aux mathématiques, une valeur possible pour cet identifiant est « wmaths » que nous utiliserons dans la suite de notre exemple.

La création des nouveaux espaces d'hébergement est automatisée par un script nommé « adm\_add\_site » sur le serveur « webpublic2 ». Ce script écrit en Python accepte deux paramètres :

- l'adresse à attribuer au site (par exemple « mathematiques.ac-dijon.fr ») ;
- l'identifiant unique du site.

À partir de ces informations, le script :

- enregistre le nouvel utilisateur FTP « wmaths » ;
- crée le répertoire racine /home/apache/wmaths/www pour stocker les données web ;
- ajoute le site dans la configuration du serveur web à travers le fichier /etc/apache2/sites-available/wmaths.conf ;
- définit le chemin des journaux d'accès et d'erreur à utiliser, respectivement /var/log/apache2/wmaths-access.log et /var/log/apache2/wmaths-error.log ;
- enfin, il termine par la création de l'utilisateur wmaths et lui attribue tous les droits sur une base de données MySQL portant le même nom.

Certains hébergements peuvent disposer de plusieurs bases de données sur l'ancien serveur : dans ce cas, des bases de données supplémentaires peuvent être créées avec le script « adm\_create\_database », en respectant la nomenclature précédente.

L'utilisation d'un script local permet de tester manuellement ces opérations et de garantir une possibilité d'intervention en cas d'inaccessibilité de la plateforme Rundeck. Celui-ci peut être aisément invoqué depuis l'orchestrateur au moyen d'une tâche effectuant un appel distant en SSH.

Un avantage offert par Rundeck au niveau de ce processus est la possibilité de valider et d'effectuer un retour utilisateur sur les paramètres fournis avant l'exécution du script lui-même : cela améliore l'expérience utilisateur et réduit le risque d'erreurs.

Ces options sont facilement paramétrables, il peut s'agir d'une liste déroulante ou d'un texte libre. Le champ peut être multi-valué, obligatoire, invisible et il est possible de définir des restrictions par l'utilisation d'expressions régulières afin d'éviter les dérives ou les valeurs non voulues.

#### **4.2.2 Recopie des données**

Pour que le site fonctionne correctement sur la nouvelle plateforme « webpublic2 », deux types de contenus doivent être déplacés :

- les fichiers présents dans l'espace d'hébergement ;
- la ou les bases de données utilisées par cet espace.

Nous avons fait le choix de déléguer la copie des fichiers à chaque responsable d'espace d'hébergement. De cette manière, ils peuvent effectuer un nettoyage des fichiers qui ne seraient plus nécessaires sur la nouvelle plateforme (anciennes copies du site, tests, code obsolète, etc.) Ce nettoyage permet de renforcer la sécurité du site, en réduisant la surface d'attaque exploitable.

La migration des bases demandant des changements plus importants (passage de MySQL vers MariaDB), nous avons mis en place une tâche Rundeck spécialisée qui effectue toutes les corrections et les opérations d'adaptation nécessaires de manière systématique.

#### **4.3 Gestion des boîtes mail bloquées pour cause de piratage**

Dans le cadre de nos missions académiques, nous gérons plusieurs dizaines de milliers de boîtes de messagerie. Il arrive donc régulièrement que certaines d'entre elles se livrent à des envois de mails suspects.

Un script Rundeck analyse donc régulièrement la file d'attente des relais SMTP de messagerie. En cas de volumétrie d'envoi inhabituelle de la part d'une unique adresse mail, il les met en attente et avertit l'administrateur.

Ce dernier peut alors analyser la situation et déterminer s'il s'agit effectivement d'un compte compromis ou d'une fausse alerte.

Dans le premier cas, cette situation est souvent liée à la diffusion d'un identifiant et d'un mot de passe à un pirate informatique en réponse à un mail de type « phishing » (hameçonnage).

Plusieurs actions sont effectuées :

- le rejet de tous les messages envoyés par cette adresse sur les différents relais SMTP ;
- le blocage de l'accès aux services de la messagerie (IMAP, POP, SMTP) au moyen de la modification de certains attributs de la fiche LDAP de l'utilisateur ;

- le changement du mot de passe de l'utilisateur dont la confidentialité n'est plus garantie ;
- la diffusion d'un mail d'information au secrétariat de l'établissement dans lequel est affecté l'agent. Celui-ci doit attendre au minimum 48h avant de pouvoir demander le déblocage de son compte de messagerie.

Cette opération de déblocage est assurée par une autre tâche Rundeck accessible à la hotline académique par le biais de leur application d'assistance. Cette application utilise l'API Rundeck pour interagir avec l'orchestrateur ce qui fluidifie le traitement des demandes d'assistance.

Elle attend un paramètre permettant de déterminer le compte concerné : il peut s'agir de l'identifiant de l'utilisateur ou de son adresse mail.

Deux nouvelles problématiques apparaissent : le passage d'informations d'étape en étape et la nécessité d'avoir recours à une collaboration entre plusieurs travaux distincts s'exécutant sur des ensembles de nœuds différents.

Pour répondre à la première, nous avons utilisé le système de filtres offert par Rundeck permettant de créer des variables à partir de la sortie d'étapes précédentes.

En ce qui concerne la seconde problématique, nous avons utilisé la possibilité de faire appel à des sous-travaux dans une tâche Rundeck. Pour éviter toute dépendance par rapport à un nom qui peut être amené à évoluer, un identifiant unique (UUID) est utilisé pour tous les appels.

Comme les travaux ne partagent pas le même contexte d'exécution, il est nécessaire d'échanger toutes les données par le biais du contexte du projet. Cela est possible par l'utilisation de la fonctionnalité d'export des variables.

Cela se manifeste de la façon suivante lors de l'appel de la seconde tâche :

```
-uid ${export.uid} -mail ${export.mail}
```

La première tâche est exécutée sur le serveur local.

Elle réalise les actions suivantes :

- l'appel d'un script Python permettant de rétablir les attributs LDAP liés au blocage du profil concerné. L'identifiant et l'adresse mail de l'utilisateur étant tous les deux nécessaires pour la suite du traitement, ils sont récupérés à la sortie de ce script grâce à un filtre Rundeck ;
- l'export de ces deux paramètres au niveau du contexte du projet ;
- l'appel de la seconde tâche responsable de la suite des traitements.

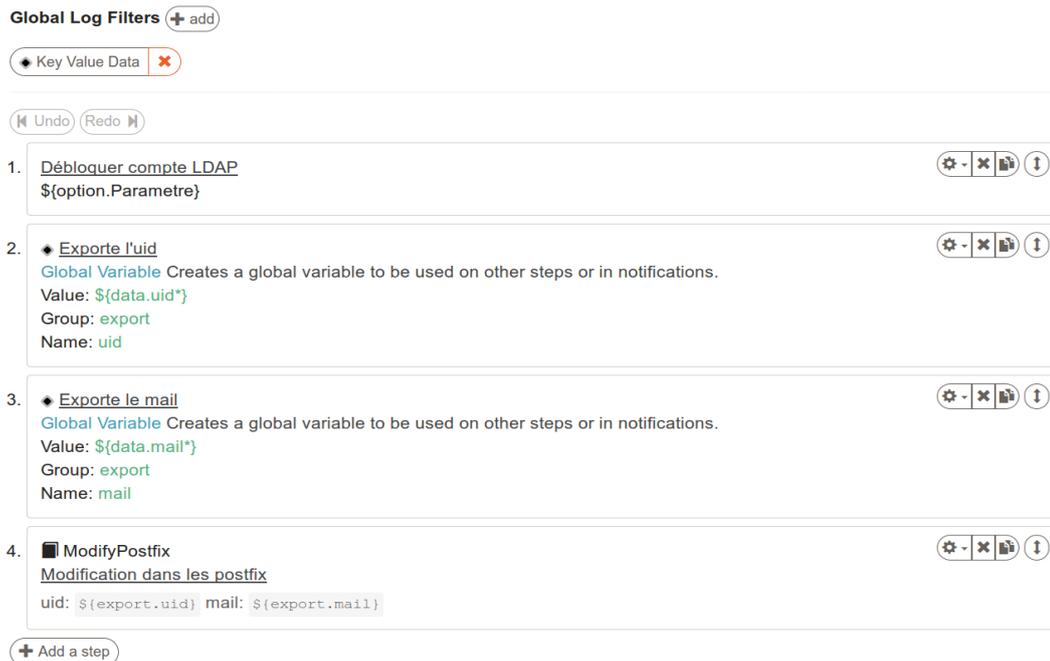


Figure 5 - Liste des étapes du job principal

La seconde tâche se connecte sur l'ensemble des serveurs Postfix concernés.

Elle nettoie les listes des expéditeurs indésirables grâce aux variables communiquées par la tâche précédente et recharge le service une fois les modifications effectuées.

## 5 API REST

Une API REST [2] est un moyen d'interagir avec une application par le moyen de requêtes HTTP. Ces requêtes peuvent être au format JSON ou XML suivant les applications.

Rundeck fournit une interface de ce type [3]. Celle-ci permet de déclencher des actions sans passer par l'interface web. Cette interface permet également d'obtenir des informations sur les travaux en cours, l'état de santé du système, les utilisateurs, les autorisations, etc.

### 5.1 Format de la requête API

Rundeck gère l'authentification des requêtes REST par le biais de deux méthodes :

- soit en indiquant directement un identifiant d'utilisateur et un mot de passe dans les en-têtes ;
- soit au moyen d'un token utilisateur secret enregistré au préalable dans l'application web.

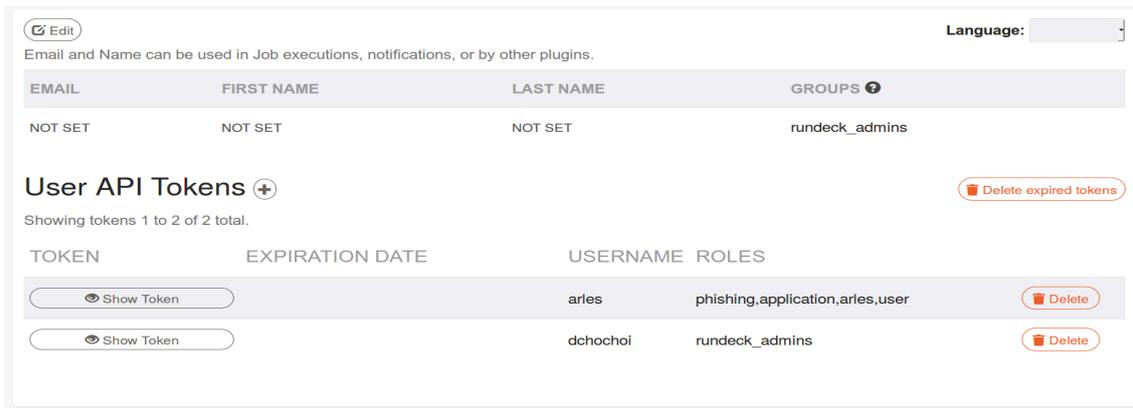


Figure 6 - Écran d'administration des Tokens API

Nous avons fait le choix d'utiliser l'authentification par token pour éviter d'échanger des informations nominatives dans chaque requête conformément à la RGPD.

L'URL de base est la suivante :

`https://<serveur>/rundeck/api/<version API>`

La requête suivante permet d'obtenir la liste des projets en utilisant la commande CURL :

```
$ curl -H "X-Rundeck-Auth-Token: XXXXXXXX" -H "Accept: application/json" -X GET https://rundeck.in.ac-dijon.fr/rundeck/api/32/projects
```

Décryptons cette commande :

- `-H "X-Rundeck-Auth-Token: XXXXXXXX"` : utilise le token XXXXXXXX pour authentifier la requête ;
- `-H "Accept: application/json"` : préfère le format JSON plus lisible pour les échanges, par défaut l'API RunDeck utilise le format XML ;
- `-X GET` : méthode HTTP. Chaque objet offert par l'API RunDeck supporte plusieurs méthodes (GET, POST, PUT, DELETE) ;
- `https://rundeck.in.ac-dijon.fr/rundeck/api/32/projects` : chemin d'appel de l'API REST.

Exemple d'une requête permettant d'obtenir les informations du système :

```
$ curl -H "X-Rundeck-Auth-Token: XXXXXXXX" -H "Accept: application/json" -X GET https://rundeck.in.ac-dijon.fr/rundeck/api/32/system/info
```

Il est possible de spécifier des paramètres lors du lancement de l'exécution d'une tâche dans le contenu d'une requête de type POST :

```
$ curl -H "X-Rundeck-Auth-Token: XXXXXXXX" -H "Accept: application/json" -X POST -d "option.parametre=tdirecteur1d" https://rundeck.in.ac-dijon.fr/rundeck/api/32/job/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/run
```

## 5.2 Utilisation dans le cadre de la gestion de la messagerie

Comme vu dans la partie 4.3, l'API est aujourd'hui utilisée par l'assistance académique dans une application locale développée en PHP.

Cette application se connecte au LDAP académique contenant l'ensemble des profils des agents. Elle offre la possibilité de consulter la fiche d'un utilisateur, de tester la connexion, d'envoyer un mail de test à l'utilisateur, ou encore de générer un code temporaire pour la récupération du mot de passe.

La fonctionnalité de déblocage des comptes LDAP verrouillés pour cause de comportement suspect se présente sous la forme d'un bouton accessible une fois la période d'invalidité de 48h écoulée.

Dans un souci de sécurité et d'isolation, un compte fonctionnel dédié à cette application a été créé dans Rundeck avec un token de sécurité associé. Les droits de ce compte sont limités à la seule utilisation de cette tâche.

Cette application interagit de deux manières avec l'API :

- le lancement de la tâche concernée en lui passant l'identifiant de l'utilisateur en paramètre ;
- la réception d'une notification de la part de Rundeck à chaque tâche terminée. Cette notification passe par la définition d'un « webhook » applicatif appelé par l'orchestrateur au moment de la réussite ou de l'échec du traitement.

Send Notification?  No  Yes

**On Success**  Send Email  Webhook

http://xxxxx.in.ac-dijon.fr/aries/rundecks/retour/\${execution.id}/\${execution.status},http://xxxxx.in.ac-dijon.fr/aries/rundecks/retour/\${execution.id}/\${execution.status}

Enter comma-separated URLs

---

**On Failure**  Send Email  Webhook

http://xxxxx.in.ac-dijon.fr/aries/rundecks/retour/\${execution.id}/\${execution.status},http://xxxxx.in.ac-dijon.fr/aries/rundecks/retour/\${execution.id}/\${execution.status}

Enter comma-separated URLs

Figure 7 - Programmation de notifications de type « Webhook »

## 6 Sécurisation des accès

### 6.1 Protection RSA Access Manager

Suite à notre choix présenté dans la partie 3.2 concernant la pré-authentification par RSA Access Manager (anciennement RSA Cleartrust) de tous les accès à Rundeck, l'orchestrateur n'effectue lui-même aucune validation de l'identité de l'utilisateur. Il se repose directement sur l'identifiant de l'utilisateur et le groupe indiqués dans les entêtes HTTP. Cela signifie qu'un serveur proxy, ou un client, peuvent falsifier ces informations.

Par sécurité, il est donc essentiel de s'assurer que le serveur Rundeck est accessible uniquement par le biais du seul proxy autorisé.

Cela est assuré au niveau de notre déploiement par plusieurs mécanismes :

- le serveur Rundeck est hébergé sur une IP interne privée, accessible uniquement à des machines et des réseaux de confiance (notamment celui de la DSI) ;
- la configuration Apache du serveur n'accepte des en-têtes d'authentification que depuis une liste blanche d'adresses proxy de confiance. Dans tous les autres cas, ceux ci sont ignorés et une redirection vers la mire d'authentification est effectuée :

```
SetEnvIf Remote_Addr ^xxx\.xxx\.xxx\.xxx TRUSTED
RequestHeader unset CT_REMOTE_USER env=!TRUSTED
RequestHeader unset ctgrps env=!TRUSTED
```

La variable « ctgrps » comprend par défaut l'ensemble des groupes auxquels appartient l'utilisateur.

Pour minimiser la complexité des ACL et éviter toute interaction avec d'autres groupes auxquels appartiendrait l'utilisateur, la configuration Apache de Rundeck retire également de cette liste tous les groupes dont le nom ne commence pas par le préfixe « rundeck- ».

## 6.2 ACL

L'attribution de droits à des utilisateurs ou des groupes dans l'application s'effectue au moyen de règles ACL.

Celles-ci sont décrites au format YAML [4].

Nous allons illustrer l'utilisation de ces règles par le biais d'un exemple.

Notre objectif est que seuls les utilisateurs appartenant au groupe « rundeck\_imagin » aient accès au projet « Imagin ». Ils doivent avoir l'autorisation de déclencher un nouveau déploiement des ressources web d'une source officielle sur les frontaux Apache. Ils ne doivent par contre avoir aucun accès sur le reste de la plateforme.

Pour ce faire, deux règles ACL sont nécessaires : une première pour restreindre les accès aux autres ressources de l'interface web, l'autre pour attribuer les droits sur le projet.

La première règle (ci-dessous) limite l'accès à l'ensemble des ressources à part la visualisation du projet « Imagin ».

```
description: Rundeck imagin
context:
  application: "rundeck";
for:
  resource:
    - deny: "*"
  project:
    - match:
      name: "Imagin"
      allow: [read]
  project_acl:
    - deny: "*"
  storage:
    - deny: "*"
by:
  group: rundeck_imagin
```

La seconde règle attribue des permissions plus fines sur le projet « Imagin ». Le groupe est autorisé à consulter les événements (« event ») et à surveiller et exécuter les tâches du projet (« job ») sur l'ensemble des nœuds prévus.

```
description: Accès au job Imagin pour le déploiement des
ressources web weblogic
context:
  project: "Imagin"
for:
  resource:
    - equals:
      kind: "event"
      allow: [read]
  adhoc:
    - deny: "*"
  job:
    - match:
      name: "Deploiement ressources Imagin"
      allow: [view,run]
    - match:
      name: ".*"
      allow: [run]
  node:
    - allow: "*"
by:
  group: rundeck_imagin
```

## 7 Conclusion

Ces quelques mois d'utilisation de Rundeck nous ont permis de prouver son utilité dans un cadre académique. Il gère actuellement plus de 10 projets pour un total de 25 traitements automatisés. Il nous a permis de réduire la fréquence des recours à l'équipe d'exploitation tout en assurant un meilleur suivi de ces traitements. L'exemple le plus frappant est le déblocage des comptes de messagerie où le nombre d'appels internes à la DSI est tombé pratiquement à zéro.

Toutes les fonctionnalités de Rundeck ne sont cependant pas encore exploitées. Nous sommes en particulier intéressés par la possibilité de travailler avec des dépôts Git et des playbooks Ansible. Il serait ainsi possible d'automatiser des mises à jour applicatives de bout en bout, depuis la récupération des sources jusqu'à la validation du bon fonctionnement.

Nos prochains projets auront comme objectifs d'approfondir l'utilisation du produit et de l'étendre à d'autres processus de notre système d'information.

## Bibliographie

- [1] Rundeck, site officiel ; <https://www.rundeck.com/>
- [2] Wikipédia, Representational state transfer ;  
[https://fr.wikipedia.org/wiki/Representational\\_state\\_transfer](https://fr.wikipedia.org/wiki/Representational_state_transfer)
- [3] Rundeck, API Reference | Version 32 ;  
<https://docs.rundeck.com/docs/api/index.html>
- [4] Rundeck, Access Control Policy ;  
<https://docs.rundeck.com/docs/administration/security/access-control-policy.html>