RUDDER

L'audit en continu : clé de la conformité démontrable

Présentation OSSIR du 12 septembre 2017

Alexandre BRIANCEAU
Responsable de production
+33 01 83 62 26 96
abr@normation.com

Benoît PECCATTE
Architecte
+33 01 83 62 26 96
bpe@normation.com

Normation

- **Editeur logiciel**
  - Basé à **Paris**
  - Fondé en 2010
- Automatisation et conformité infrastructures de production.
- Focus unique sur Rudder, solution de Continuous Auditing & Configuration.
- Solution **open source**

Normation – 87 rue de Turbigo, 75003 PARIS, France
contact@normation.com – +33 1.83.62.26.96 – http://www.normation.com/

RUDDER

Sommaire

RUDDER

1. **Introduction**
2. RUDDER
3. Mise en application
4. Conclusion

Continuous*

Croissance
continue

Connexion
continue

Menace
continue

Normation – 87 rue de Turbigo, 75003 PARIS, France
contact@normation.com – +33 1.83.62.26.96 – http://www.normation.com/

Continuité

Croissance
continue

Connexion
continue

Menace
continue

La gestion de la production informatique
doit devenir **continue**

Conformité

Nombreux référentiels de conformités

Politiques de sécurités (PSSI)

PCI-DSS

Recommandations ANSSI

ISO/CEI 27002

GDPR

Socle agile et dynamique

DevOps

Virtualisation

Containers

Cloud

Et l'audit dans tout ça ?

Démontrable...

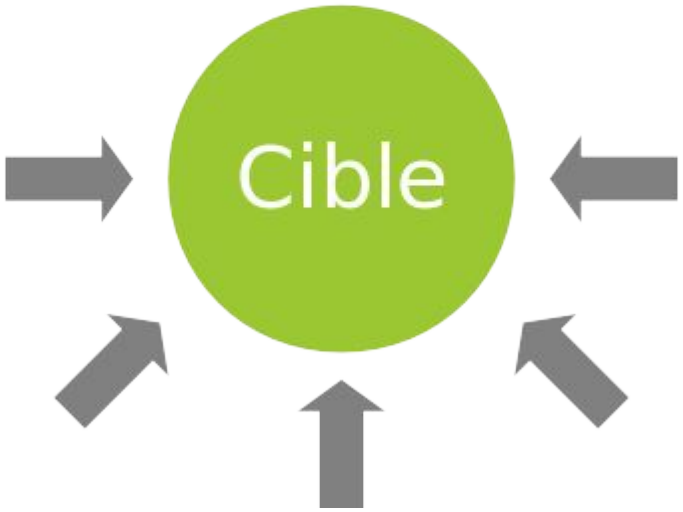
...malgré la dérive !

RUDDER

1. Introduction
2. **RUDDER**
3. Mise en application
4. Conclusion

Définition d'un état

Imperatif → Declaratif



Action impérative	État déclaré
Installer un paquet	Un paquet doit être installé
Mettre une ligne dans un fichier	Un fichier doit contenir une ligne
Démarrer un service	Un service doit être démarré

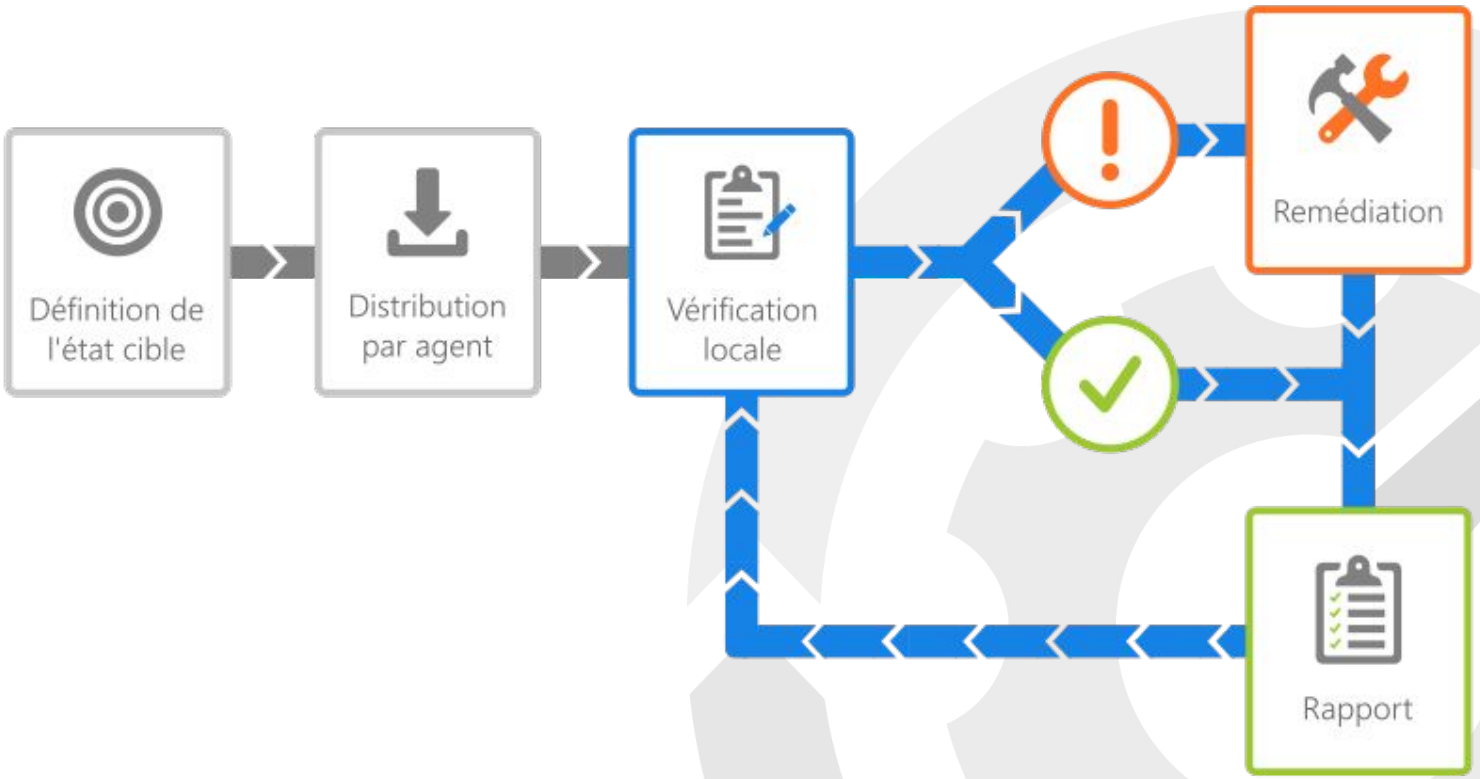
Définition d'un état

Un état se différencie d'une action par :

- **Son comportement en cas d'erreur**
- **La vérification du résultat**

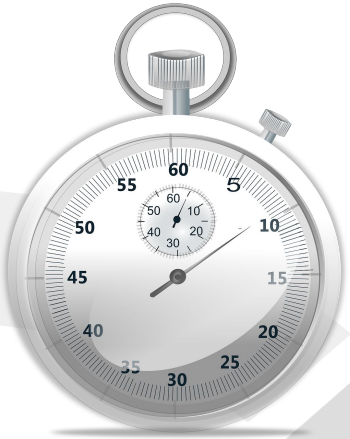
Action impérative	État déclaré
Installer un paquet	Un paquet doit être installé
Mettre une ligne dans un fichier	Un fichier doit contenir une ligne
Démarrer un service	Un service doit être démarré

Cycle de vie dans Rudder



RUDDER applique ses règles fréquemment :

- Toutes les 5 minutes par défaut



L'agent est léger :

- Écrit en C
- Faible consommation mémoire
- Faible consommation CPU

Une centaines de règles sont exécutées
en moins de 10 secondes

Normation – 87 rue de Turbigo, 75003 PARIS, France
contact@normation.com – +33 1.83.62.26.96 – http://www.normation.com/

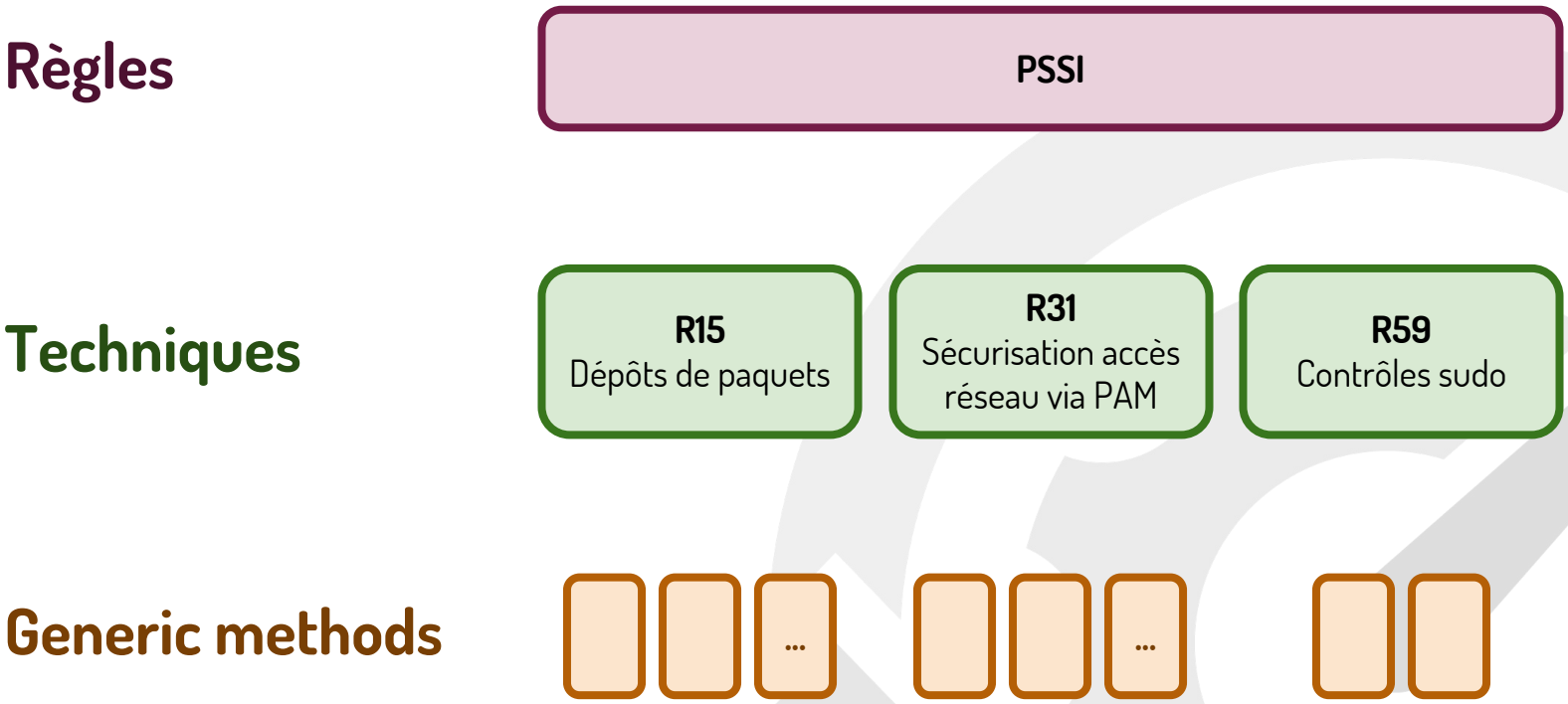
RUDDER est déclaratif

- On déclare **l'état souhaité**

- On choisit ensuite si on veut :
  - valider l'état → **audit**
  - mettre à jour l'état → **enforce**

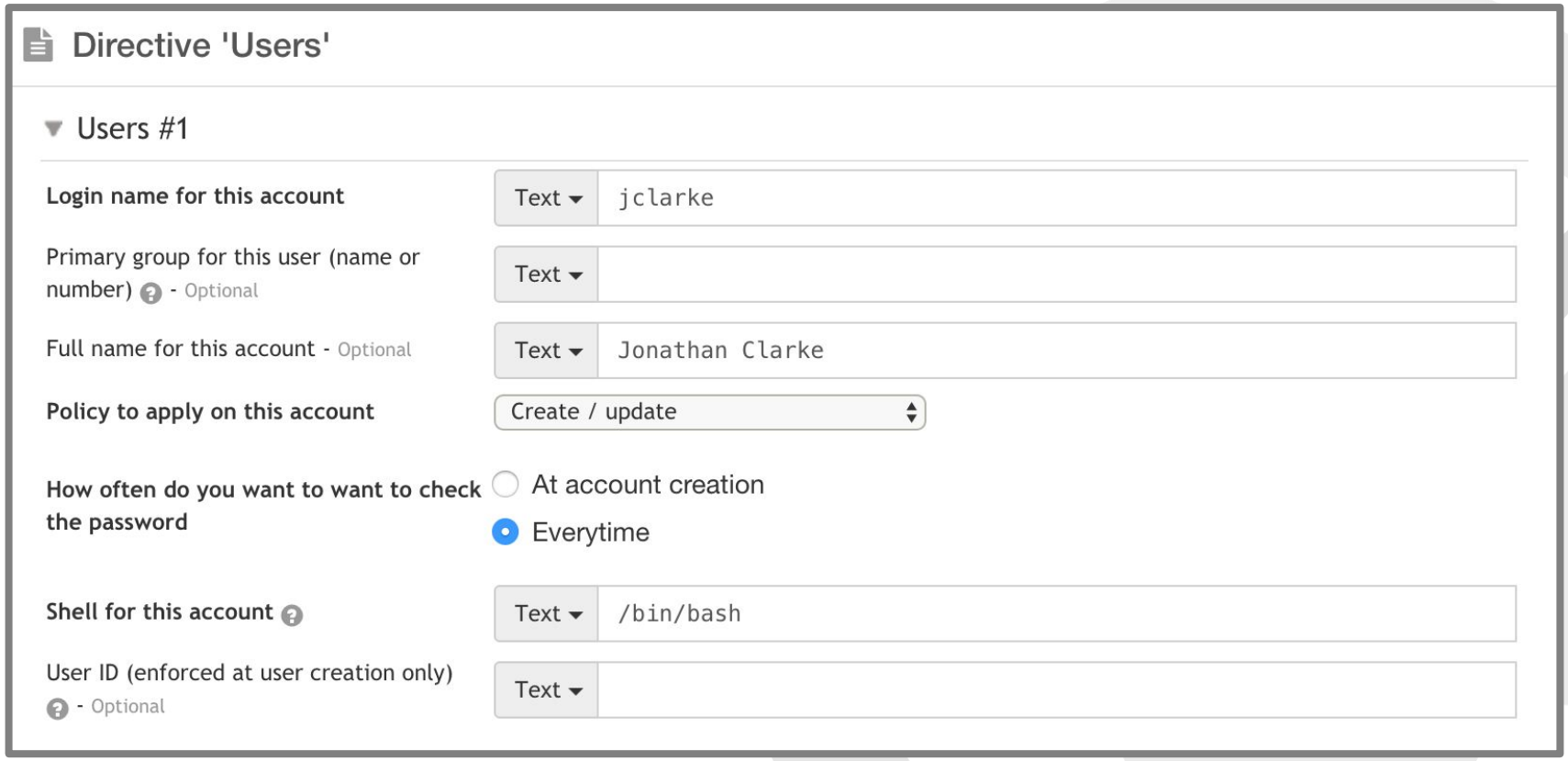
Normation – 87 rue de Turbigo, 75003 PARIS, France
contact@normation.com – +33 1.83.62.26.96 – http://www.normation.com/

RUDDER et son découpage logique

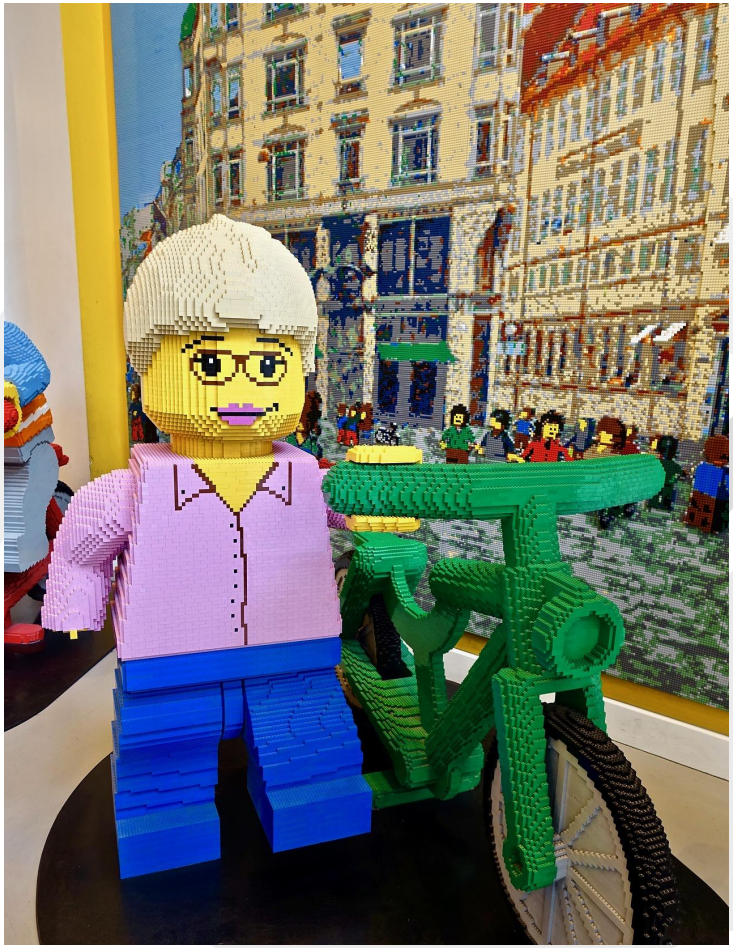


Normation – 87 rue de Turbigo, 75003 PARIS, France
contact@normation.com – +33 1.83.62.26.96 – http://www.normation.com/

Un état est décrit dans Rudder à travers des techniques.



RUDDER : édition des techniques via le Technique Editor



RUDDER : édition des techniques via le Technique Editor

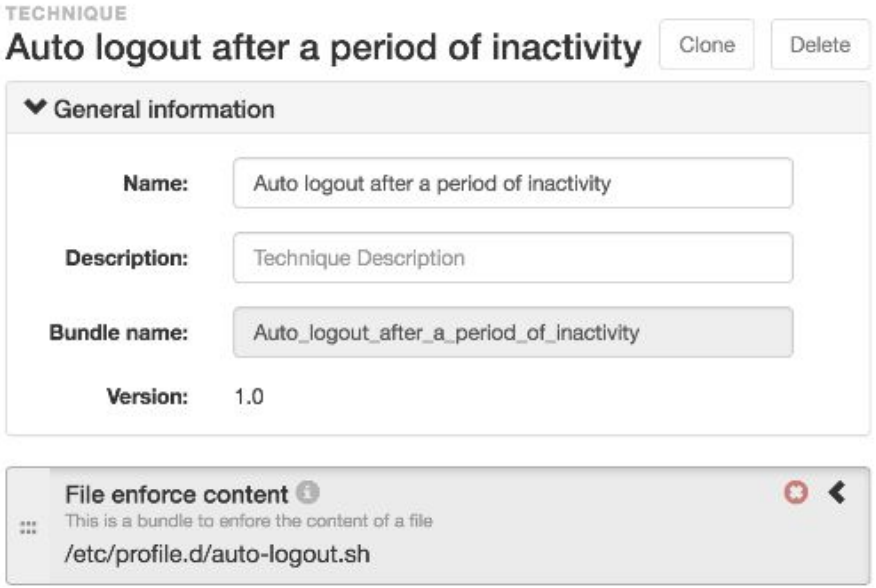
Déconnexion automatique

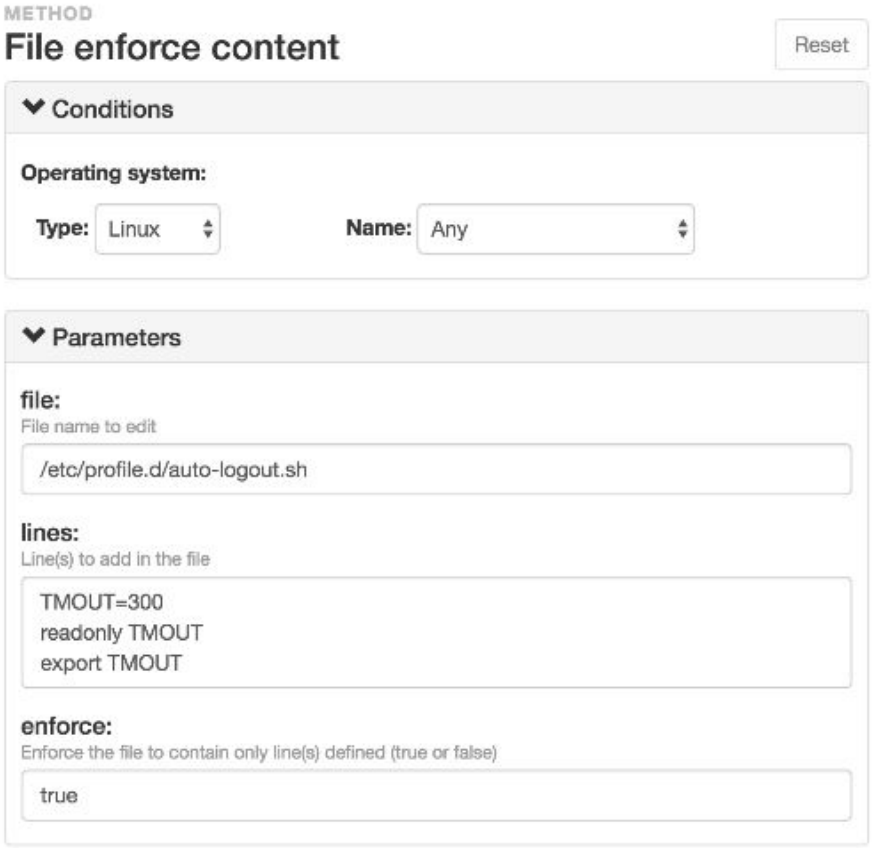
But

Sécurisation accès

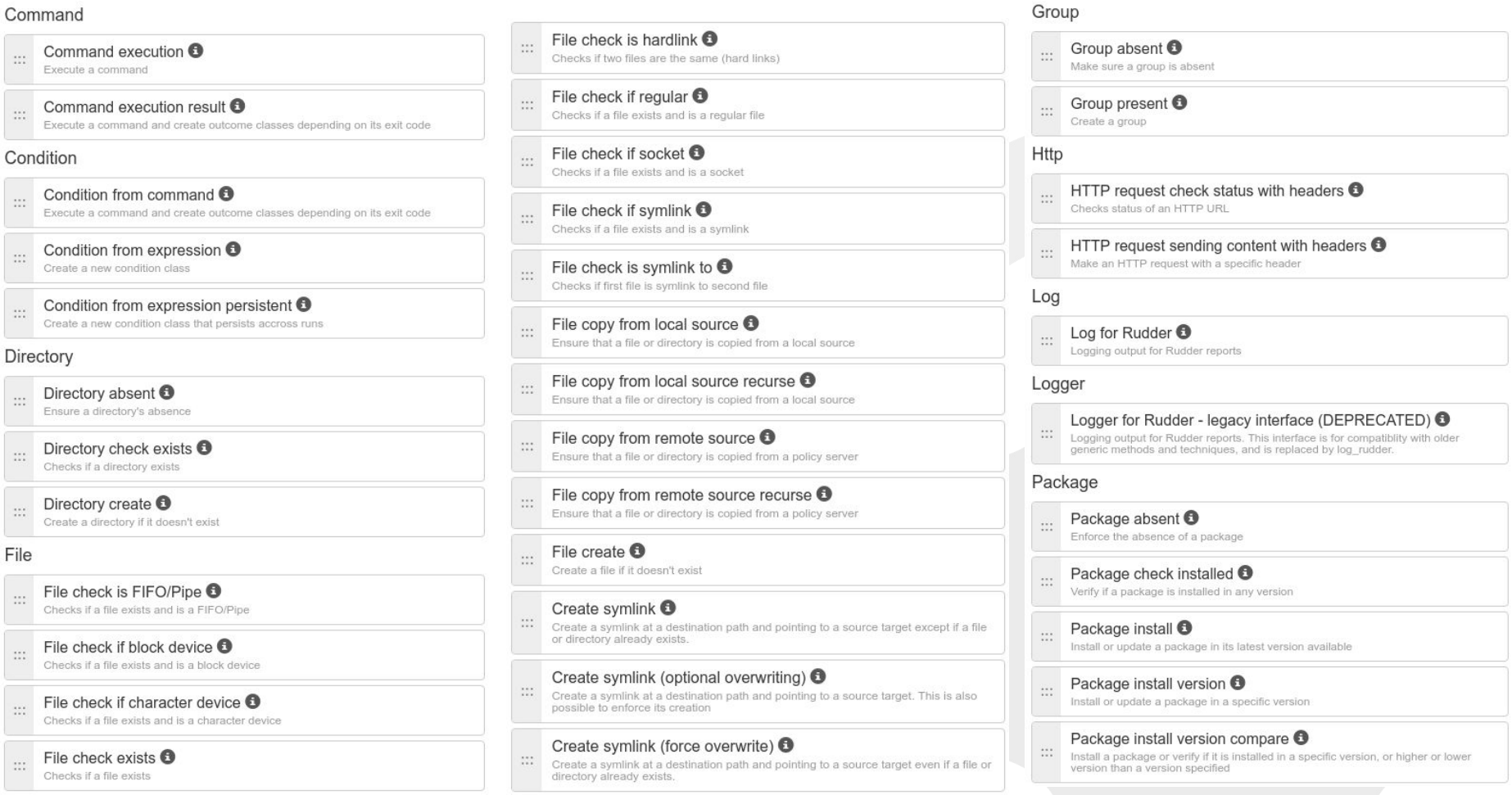
Implémentation

Edition fichier ou registre





RUDDER : édition des techniques via le Technique Editor



RUDDER

1. Introduction
2. RUDDER
3. **Mise en application**
4. Conclusion

Application d'une 1ère itération de PSSI

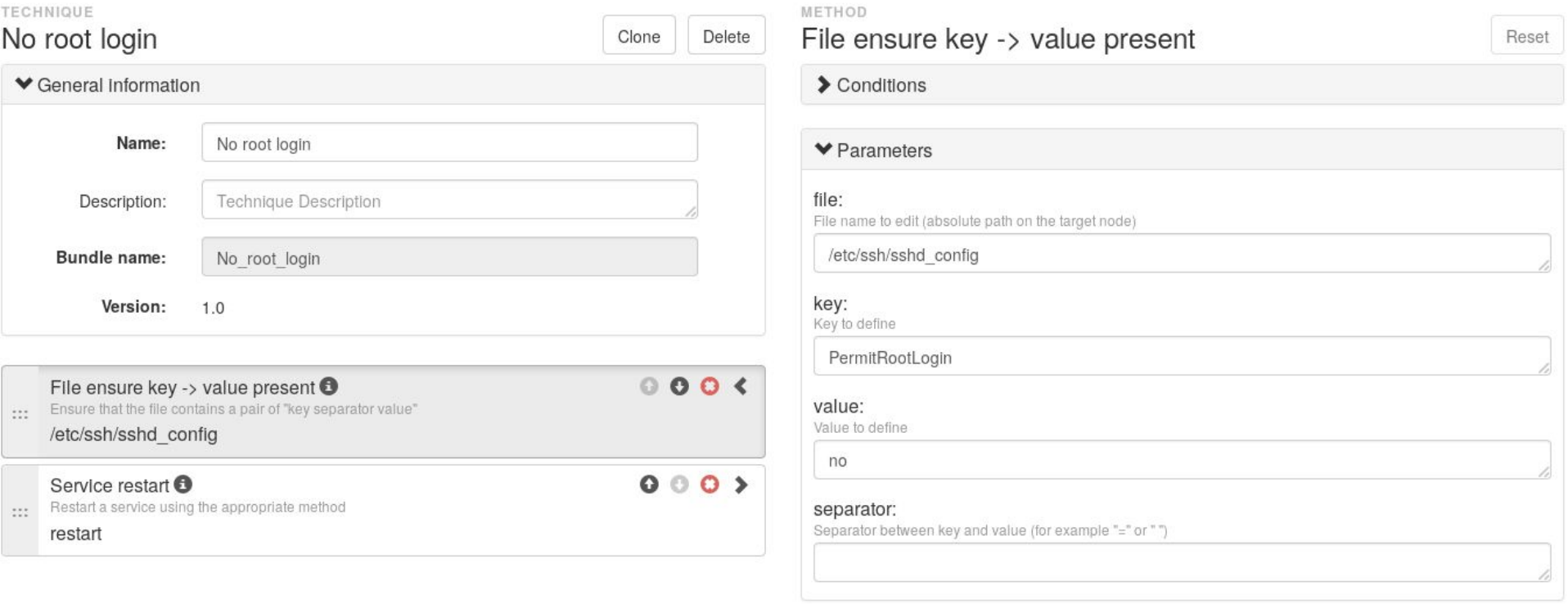
Basée sur recommandations ANSSI

Contenu de la règle :

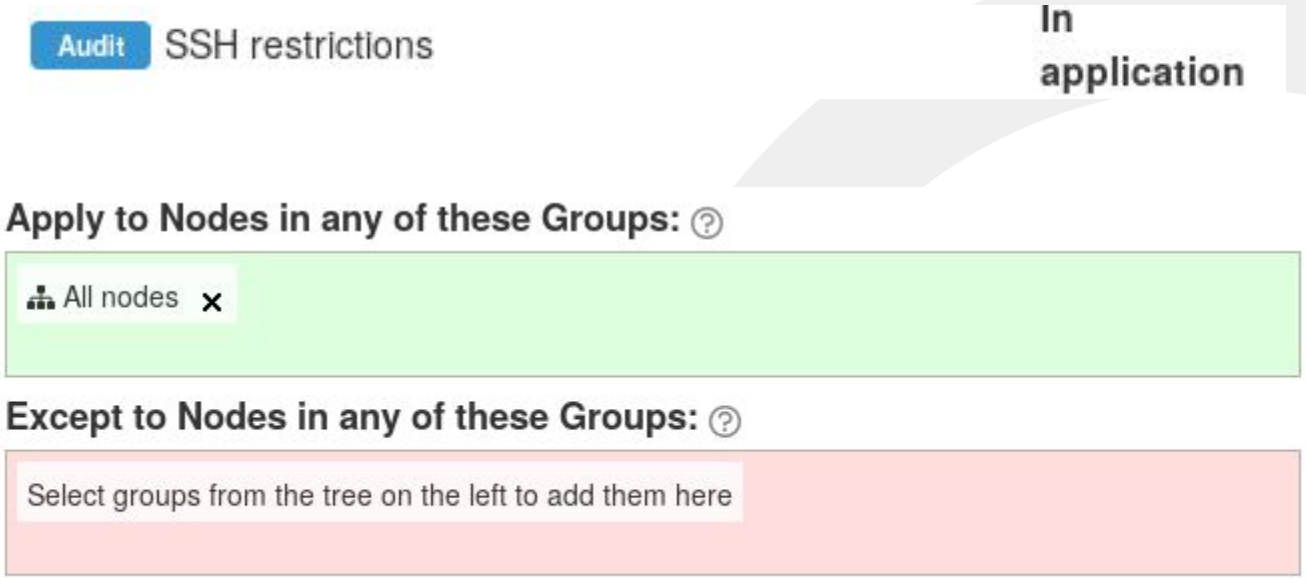
- Chaque utilisateur doit se connecter avec son propre compte
- La clé publique des utilisateurs doit être déployée sur le parc

Mise en application

Pas de connexion en root



Création de la règle en mode audit



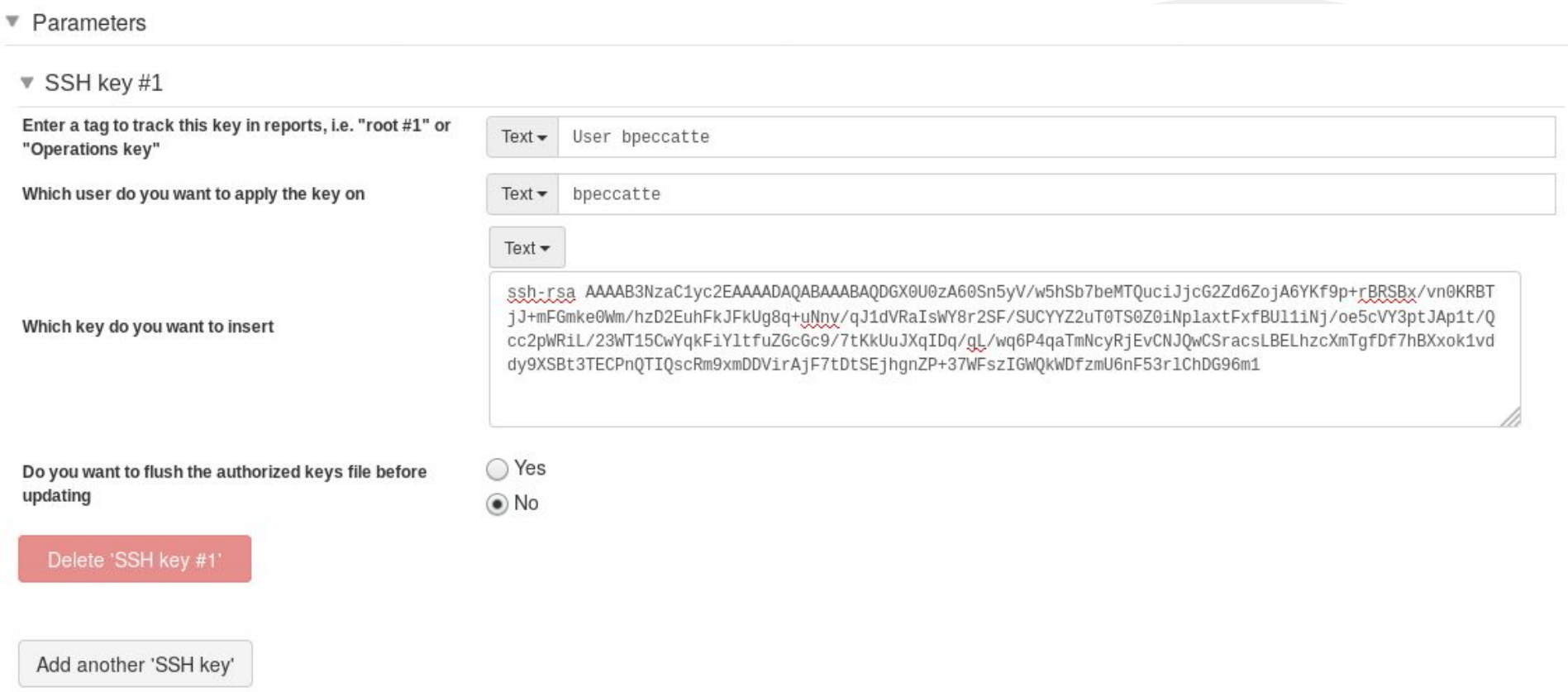
Mise en application

Affichage des résultats de compliance

Mise en application

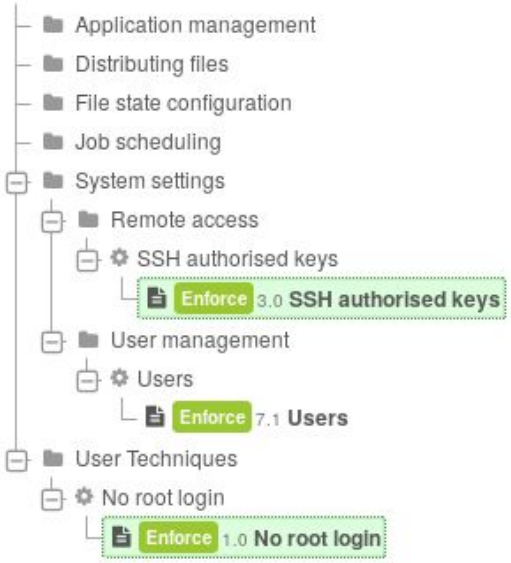
Passage en mode enforce de la règle

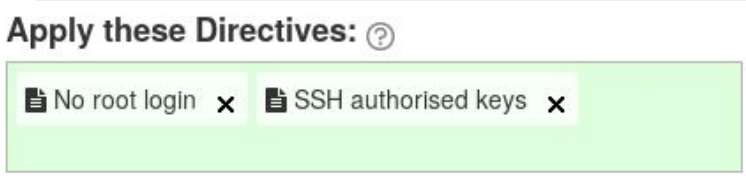
Déploiement des clés ssh



Mise en application

Ajout à la règle



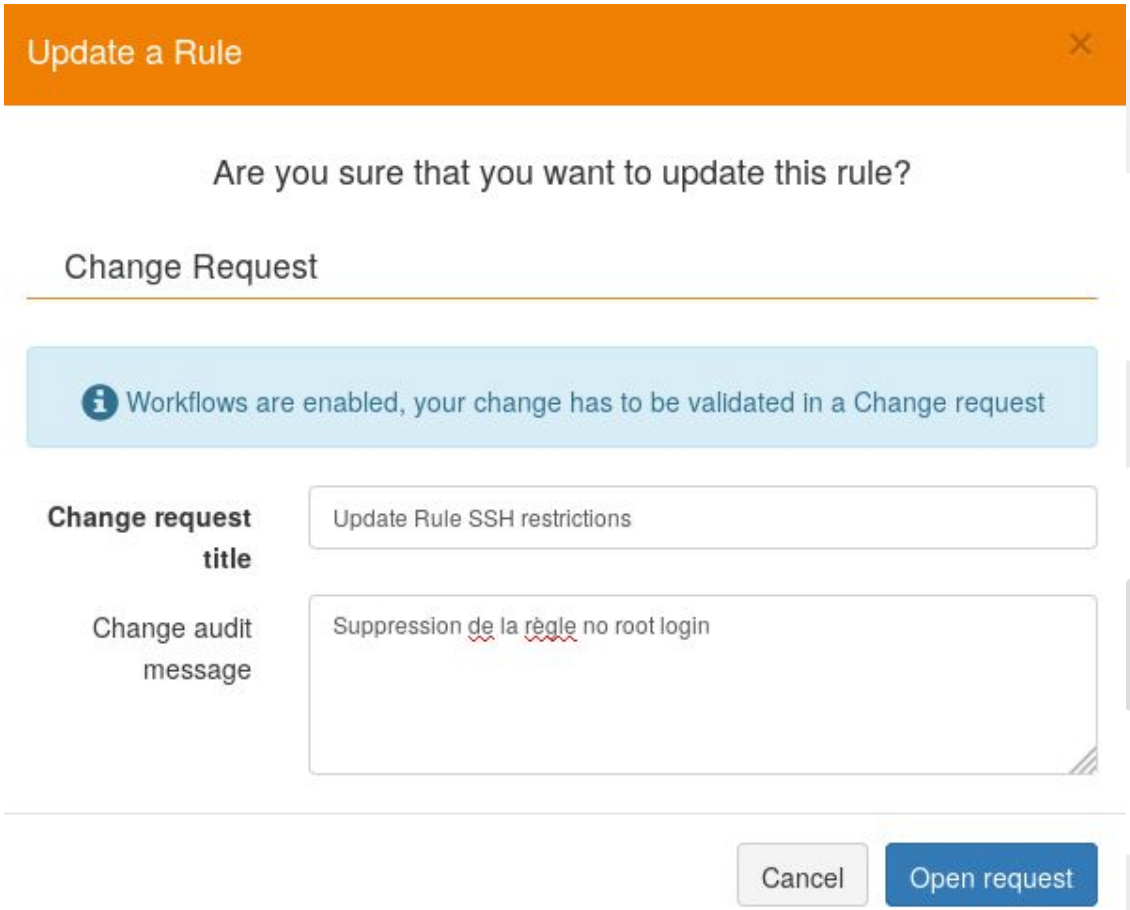


Outils de contrôle de Rudder

- Change request
- Audit log
- Réparations
- Backup de fichiers modifiés

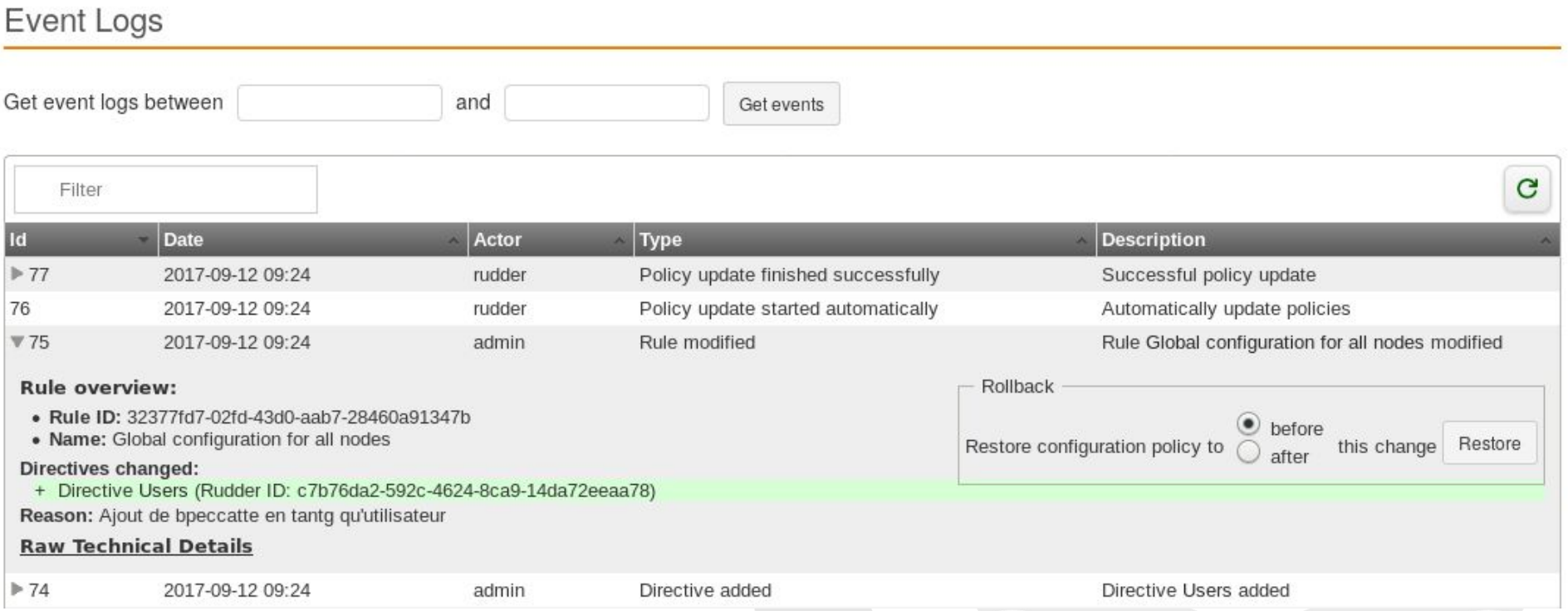
Mise en application

Les modifications peuvent être validées à travers des change request



Mise en application

Les modifications sur le serveur donnent lieu à un log d'audit



Mise en application

Les modification sur les noeuds donnent lieu à un historique de réparation

Changes during period **2017-09-12 06:00 - 12:00** (selected in graph above)

Filter

Execution Date	Node	Directive	Component	Value	Message
2017-09-12 09:13	agent3.rudder.local	No root login	File ensure key -> value present	/etc/ssh/sshd_config	Ensure line in format key value in /etc/ssh/sshd_config was repaired
2017-09-12 09:14	agent2.rudder.local	No root login	File ensure key -> value present	/etc/ssh/sshd_config	Ensure line in format key value in /etc/ssh/sshd_config was repaired
2017-09-12 09:25	server.rudder.local	SSH authorised keys	SSH key	User bpeccatte	SSH key "User bpeccatte" for user bpeccatte was repaired
2017-09-12 09:26	agent1.rudder.local	SSH authorised keys	SSH key	User bpeccatte	SSH key "User bpeccatte" for user bpeccatte was repaired
2017-09-12 09:26	agent2.rudder.local	SSH authorised keys	SSH key	User bpeccatte	SSH key "User bpeccatte" for user bpeccatte was repaired
2017-09-12 09:26	agent3.rudder.local	SSH authorised keys	SSH key	User bpeccatte	SSH key "User bpeccatte" for user bpeccatte was repaired

Show 25 entries Showing 1 to 6 of 6 entries First Previous 1 Next Last

Mise en application

Les modifications sur les noeuds donnent lieu à une sauvegarde des fichiers modifiés

```
root@agent3:~# ls -1 /var/rudder/modified-files/

_etc_shadow_1505208303_Tue_Sep_12_09_25_04_2017_cf_before_edit
_etc_ssh_sshd_config_1505207580_Tue_Sep_12_09_13_01_2017_cf_before_ed
it
_home_bpeccatte__ssh_authorized_keys_1505208397_Tue_Sep_12_09_26_38_2
017_cf_before_edit
```

Mise en application

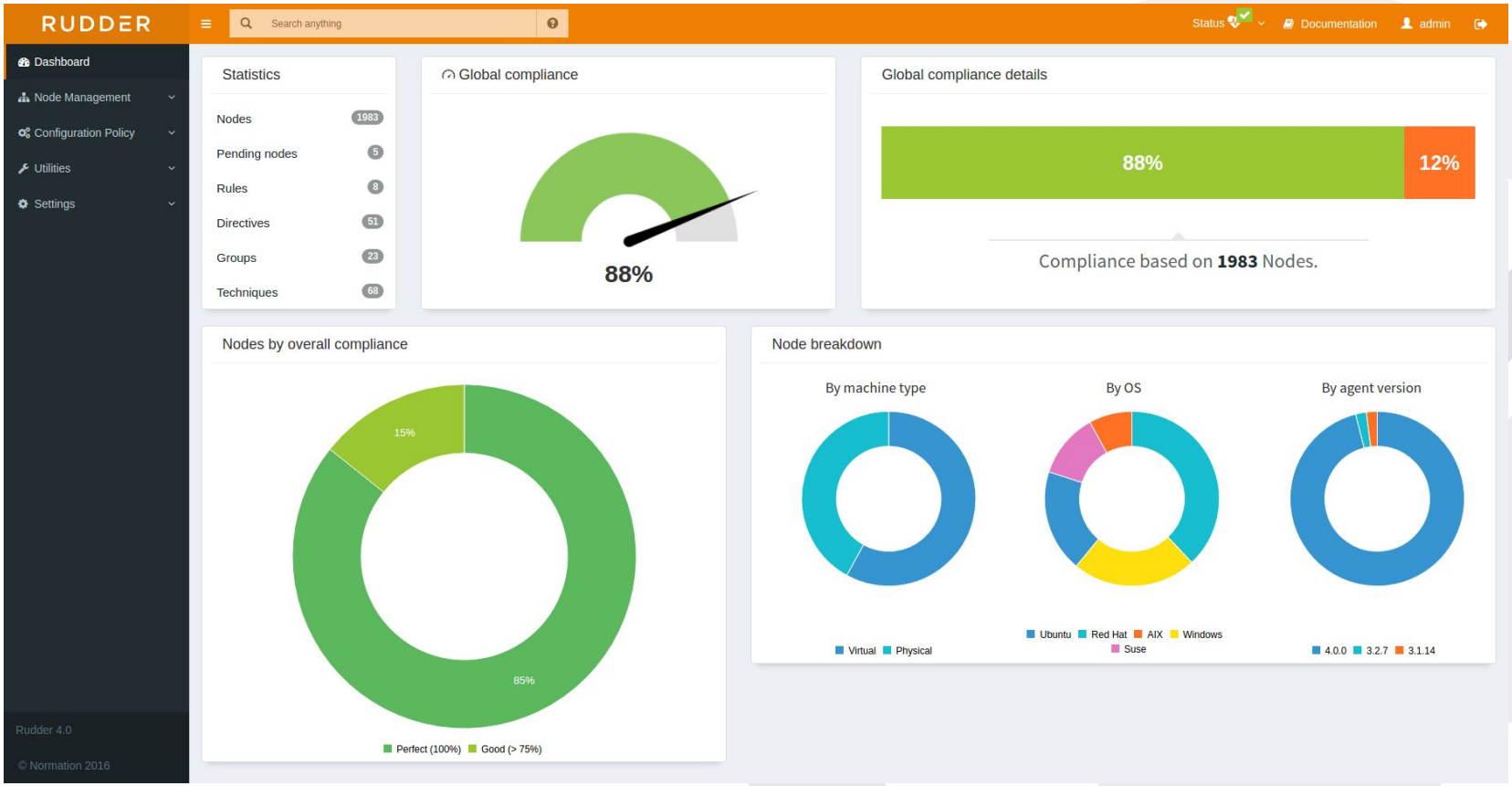
L'application d'une règle se fait au travers d'un groupe

- Groupes statiques ou dynamiques
- Défini via l'inventaire, via des propriétés ou via CMDB
- Toute nouvelle machine dans le parc est intégrée à des groupes

Exemple de groupes statiques et dynamiques

Mise en application

Dashboard principal renseignant la conformité globale



RUDDER

1. Introduction
2. RUDDER
3. Mise en application
4. **Conclusion**

Conclusion

- **Améliore la visibilité**
- **Audit en quasi-temps réel**
- **Démontrable à tout moment**

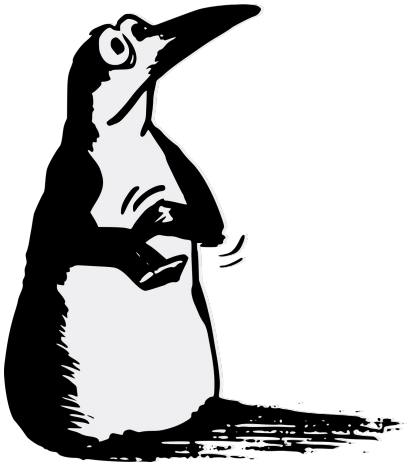
Conclusion

- **Toute politique est pérenne**
  - Audit
  - Remédiation
- **Améliore la cohérence et le suivi**
- **Accélère l'analyse**

Conclusion

Audit en continu

Amélioration en continu



RUDDER

Merci pour votre écoute

www.normation.com

Images sous CC0 issues de pixabay.com
Icones sous CC-BY 3.0 de Dave Gandy sur www.flaticon.com