



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

- **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**



RUDDER

Sommaire

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



RUDDER

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

Continuous*



Croissance
continue



Connexion
continue



Menace
continue



Croissance
continue



Connexion
continue



Menace
continue



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

Nombreux référentiels de conformités

Politiques de sécurités (PSSI)

PCI-DSS

Recommandations ANSSI

ISO/CEI 27002

GDPR

Socle agile et dynamique

Virtualisation

DevOps

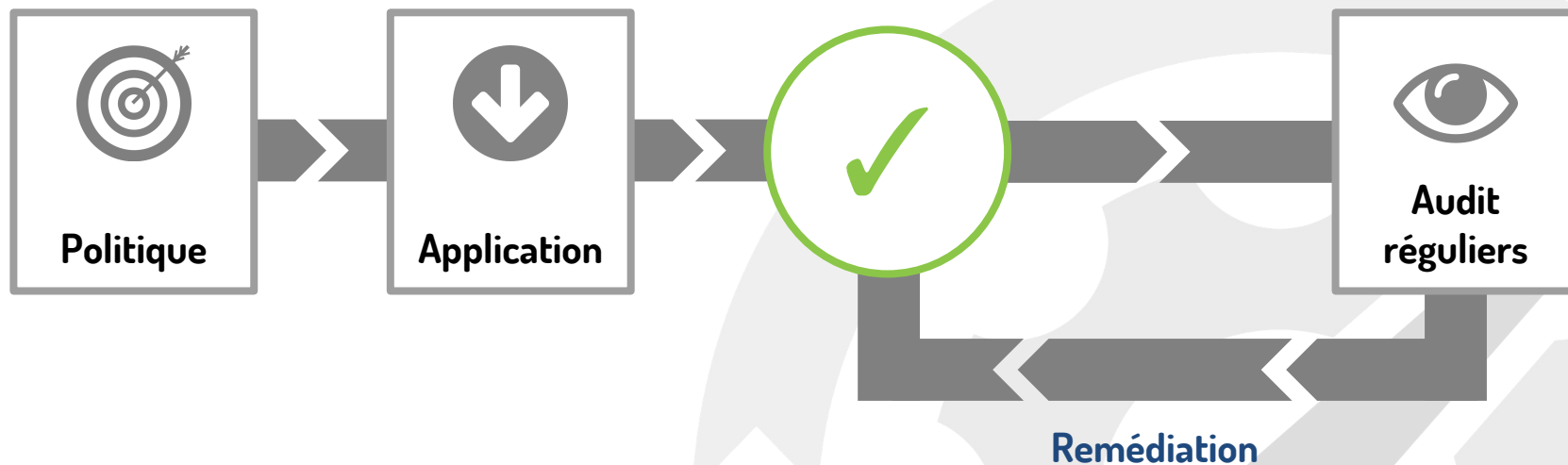
Containers

Cloud

Et l'audit dans tout ça ?



Démontrable...



..malgré la dérive !



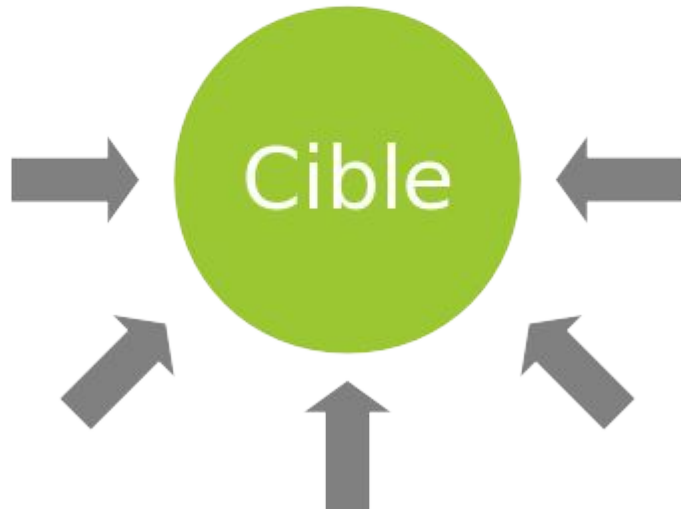


RUDDER

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

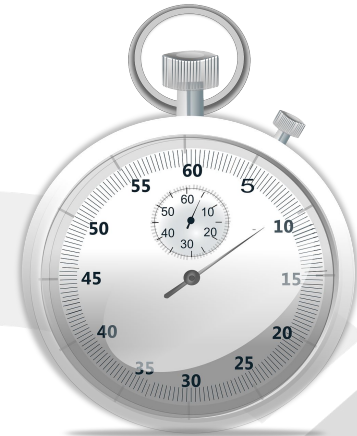


RUDDER applique ses règles fréquemment :

- Toutes les 5 minutes par défaut

L'agent est léger :

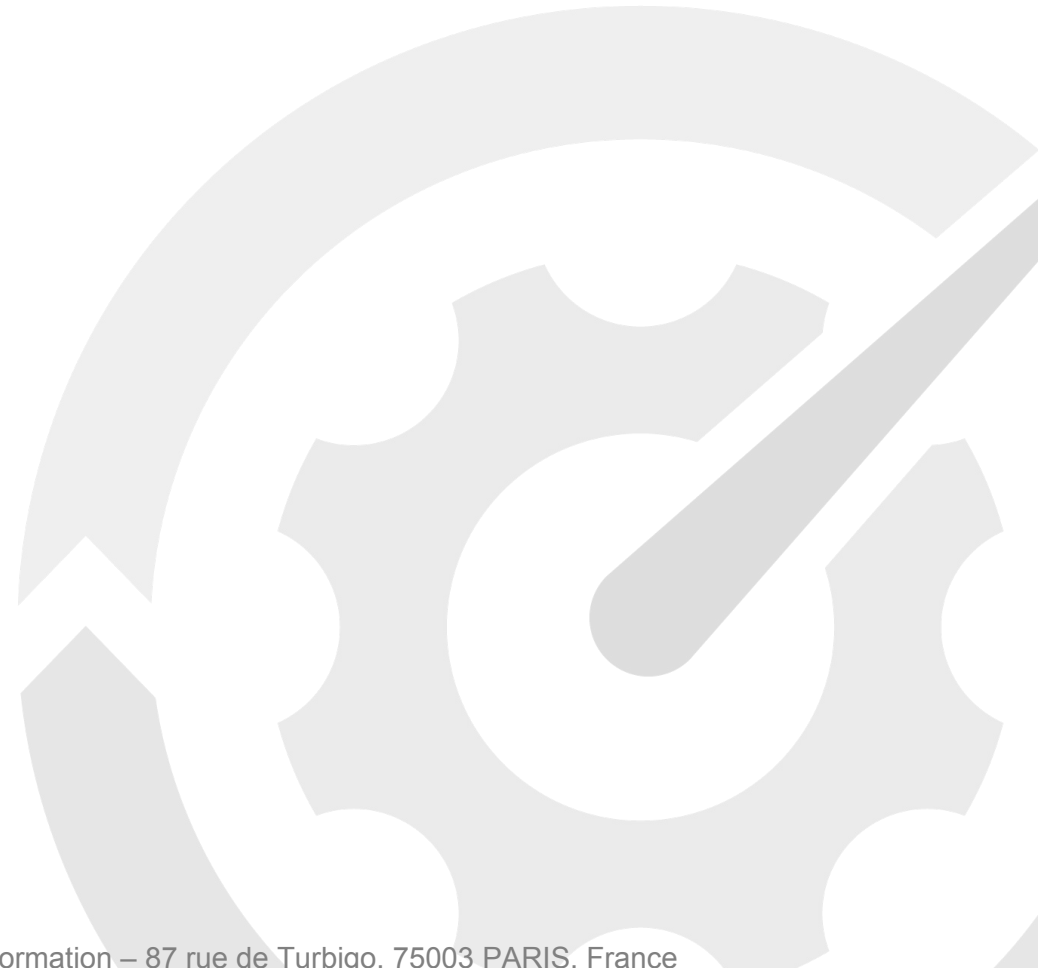
- Écrit en C
- Faible consommation mémoire
- Faible consommation CPU



Une centaines de règles sont exécutées
en moins de 10 secondes

RUDDER est déclaratif

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



RUDDER et son découpage logique

Règles

PSSI

Techniques

R15

Dépôts de paquets

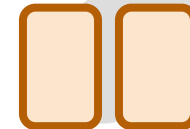
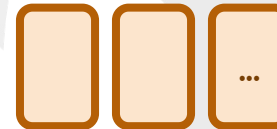
R31

Sécurisation accès
réseau via PAM

R59

Contrôles sudo

Generic methods



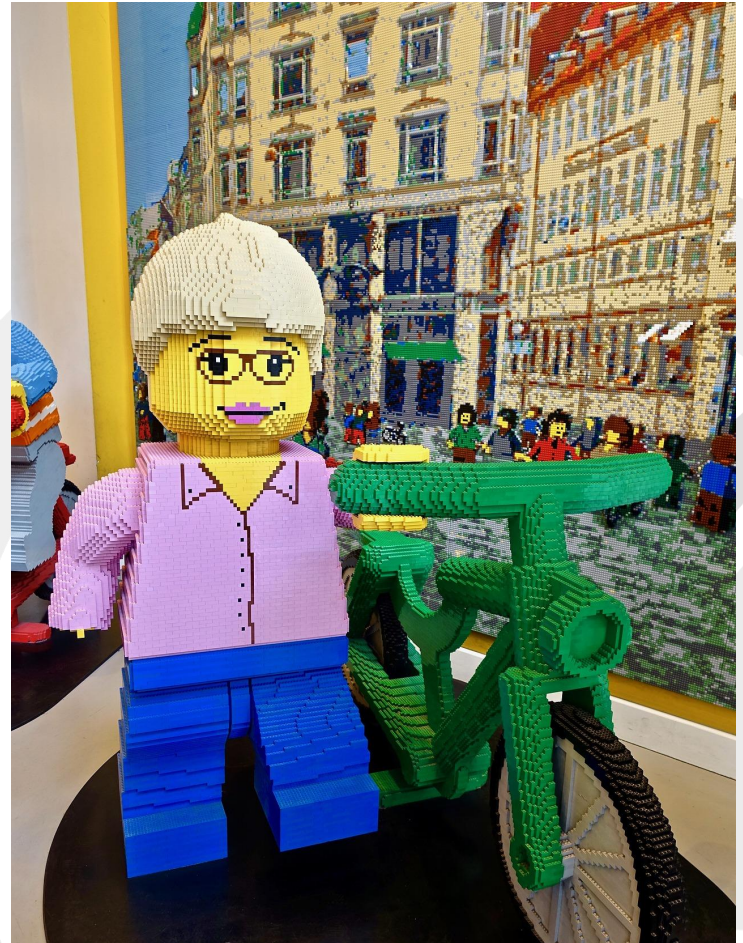
Un état est décrit dans Rudder à travers des techniques.

Directive 'Users'

▼ Users #1

Login name for this account	Text ▼ jclarke
Primary group for this user (name or number) ⓘ - Optional	Text ▼
Full name for this account - Optional	Text ▼ Jonathan Clarke
Policy to apply on this account	Create / update
How often do you want to want to check the password	<input type="radio"/> At account creation <input checked="" type="radio"/> Everytime
Shell for this account ⓘ	Text ▼ /bin/bash
User ID (enforced at user creation only) ⓘ - Optional	Text ▼

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

TECHNIQUE

Auto logout after a period of inactivity Clone Delete

▼ General information

Name:

Description:

Bundle name:

Version:

File enforce content ⓘ ✖ ◀

⋮ This is a bundle to enforce the content of a file

`/etc/profile.d/auto-logout.sh`

METHOD

File enforce content Reset

▼ Conditions

Operating system:

Type: ⌵ **Name:** ⌵

▼ Parameters

file:
File name to edit

lines:
Line(s) to add in the file

enforce:
Enforce the file to contain only line(s) defined (true or false)

RUDDER : édition des techniques via le Technique Editor

Command

... **Command execution** ⓘ
Execute a command

... **Command execution result** ⓘ
Execute a command and create outcome classes depending on its exit code

Condition

... **Condition from command** ⓘ
Execute a command and create outcome classes depending on its exit code

... **Condition from expression** ⓘ
Create a new condition class

... **Condition from expression persistent** ⓘ
Create a new condition class that persists across runs

Directory

... **Directory absent** ⓘ
Ensure a directory's absence

... **Directory check exists** ⓘ
Checks if a directory exists

... **Directory create** ⓘ
Create a directory if it doesn't exist

File

... **File check is FIFO/Pipe** ⓘ
Checks if a file exists and is a FIFO/Pipe

... **File check if block device** ⓘ
Checks if a file exists and is a block device

... **File check if character device** ⓘ
Checks if a file exists and is a character device

... **File check exists** ⓘ
Checks if a file exists

... **File check is hardlink** ⓘ
Checks if two files are the same (hard links)

... **File check if regular** ⓘ
Checks if a file exists and is a regular file

... **File check if socket** ⓘ
Checks if a file exists and is a socket

... **File check if symlink** ⓘ
Checks if a file exists and is a symlink

... **File check is symlink to** ⓘ
Checks if first file is symlink to second file

... **File copy from local source** ⓘ
Ensure that a file or directory is copied from a local source

... **File copy from local source recurse** ⓘ
Ensure that a file or directory is copied from a local source

... **File copy from remote source** ⓘ
Ensure that a file or directory is copied from a policy server

... **File copy from remote source recurse** ⓘ
Ensure that a file or directory is copied from a policy server

... **File create** ⓘ
Create a file if it doesn't exist

... **Create symlink** ⓘ
Create a symlink at a destination path and pointing to a source target except if a file or directory already exists.

... **Create symlink (optional overwriting)** ⓘ
Create a symlink at a destination path and pointing to a source target. This is also possible to enforce its creation

... **Create symlink (force overwrite)** ⓘ
Create a symlink at a destination path and pointing to a source target even if a file or directory already exists.

Group

... **Group absent** ⓘ
Make sure a group is absent

... **Group present** ⓘ
Create a group

Http

... **HTTP request check status with headers** ⓘ
Checks status of an HTTP URL

... **HTTP request sending content with headers** ⓘ
Make an HTTP request with a specific header

Log

... **Log for Rudder** ⓘ
Logging output for Rudder reports

Logger

... **Logger for Rudder - legacy interface (DEPRECATED)** ⓘ
Logging output for Rudder reports. This interface is for compatibility with older generic methods and techniques, and is replaced by log_rudder.

Package

... **Package absent** ⓘ
Enforce the absence of a package

... **Package check installed** ⓘ
Verify if a package is installed in any version

... **Package install** ⓘ
Install or update a package in its latest version available

... **Package install version** ⓘ
Install or update a package in a specific version

... **Package install version compare** ⓘ
Install a package or verify if it is installed in a specific version, or higher or lower version than a version specified



RUDDER

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

Application d'une 1^{ère} 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

Pas de connexion en root

TECHNIQUE

No root login

Clone Delete

▼ General Information

Name:

Description:

Bundle name:

Version: 1.0

File ensure key -> value present ⓘ

Ensure that the file contains a pair of "key separator value"

/etc/ssh/sshd_config

Service restart ⓘ

Restart a service using the appropriate method

restart

METHOD

File ensure key -> value present

Reset

► Conditions

▼ Parameters

file:

File name to edit (absolute path on the target node)

key:

Key to define

value:

Value to define

separator:

Separator between key and value (for example "=" or " ")

Création de la règle en mode audit

Audit SSH restrictions

In application

Apply to Nodes in any of these Groups: ?

All nodes x

Except to Nodes in any of these Groups: ?

Select groups from the tree on the left to add them here

Affichage des résultats de compliance

Node	Status
Audit agent1.rudder.local	100%
Audit agent2.rudder.local	50% 50%
Audit agent3.rudder.local	50% 50%
Audit server.rudder.local	100%

Show 25 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

Directive	Status
Audit No root login	50% 50%

Component	Status
File ensure key -> value present	100%

Value	Messages	Status
/etc/ssh/sshd_config	Ensure line in format key value in /etc/ssh/sshd_config was not correct	Non compliant

Passage en mode enforce de la règle

Node	Status
▶ Enforce agent1.rudder.local 🔍	100%
▶ Enforce agent2.rudder.local 🔍	100%
▶ Enforce agent3.rudder.local 🔍	100%
▶ Enforce server.rudder.local 🔍	100%

Show entries Showing 1 to 4 of 4 entries

Déploiement des clés ssh

▼ Parameters

▼ SSH key #1

Enter a tag to track this key in reports, i.e. "root #1" or "Operations key"

Text ▼ User bpeccatte

Which user do you want to apply the key on

Text ▼ bpeccatte

Which key do you want to insert

Text ▼

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDGx0U0zA60Sn5yV/w5hSb7beMTQuc1JjcG2Zd6ZojA6YKf9p+rBRsBx/vn0KRBT  
jJ+mFGmke0Wm/hzD2EuhFkJFkUg8q+uNny/qJ1dVRaIsWY8r2SF/SUCYYZ2uT0TS0Z0iNp1axtFxfBU11iNj/oe5cVY3ptJAp1t/Q  
cc2pWRiL/23WT15CwYqkF1Y1tFuZGcGc9/7tKkUuJXqIDq/gL/wq6P4qaTmNcyRjEvCNJQwCSracsLBELhzcXmTgDf7hBXxok1vd  
dy9XSBt3TECPnQTIQscRm9xmDDVirAjF7tDtSEjhgnZP+37WFszIGWQkWDfzmU6nF53r1ChDG96m1
```

Do you want to flush the authorized keys file before updating

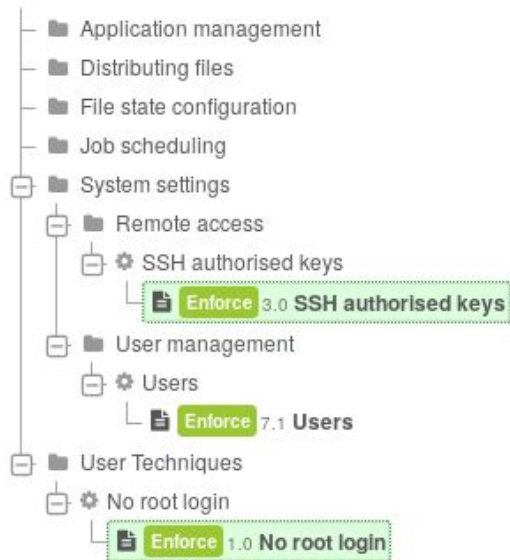
Yes

No

Delete 'SSH key #1'

Add another 'SSH key'

Ajout à la règle



Apply these Directives: ?

No root login SSH authorised keys

Outils de contrôle de Rudder

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



Les modifications peuvent être validées à travers des change request

Update a Rule ✕

Are you sure that you want to update this rule?

Change Request

i Workflows are enabled, your change has to be validated in a Change request

Change request title

Change audit message

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

Event Logs

Get event logs between and

Id	Date	Actor	Type	Description
▶ 77	2017-09-12 09:24	rudder	Policy update finished successfully	Successful policy update
76	2017-09-12 09:24	rudder	Policy update started automatically	Automatically update policies
▼ 75	2017-09-12 09:24	admin	Rule modified	Rule Global configuration for all nodes modified

Rule overview:

- Rule ID: 32377fd7-02fd-43d0-aab7-28460a91347b
- Name: Global configuration for all nodes

Directives changed:

- + Directive Users (Rudder ID: c7b76da2-592c-4624-8ca9-14da72eeaa78)

Reason: Ajout de bpeccatte en tantq qu'utilisateur

Raw Technical Details

▶ 74	2017-09-12 09:24	admin	Directive added	Directive Users added
------	------------------	-------	-----------------	-----------------------

Rollback

Restore configuration policy to before after this change

Les modifications 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/ssh_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/ssh_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



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

```
root@agent3:~# ls -l /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_edit
_home_bpeccatte__ssh_authorized_keys_1505208397_Tue_Sep_12_09_26_38_2017_cf_before_edit
```

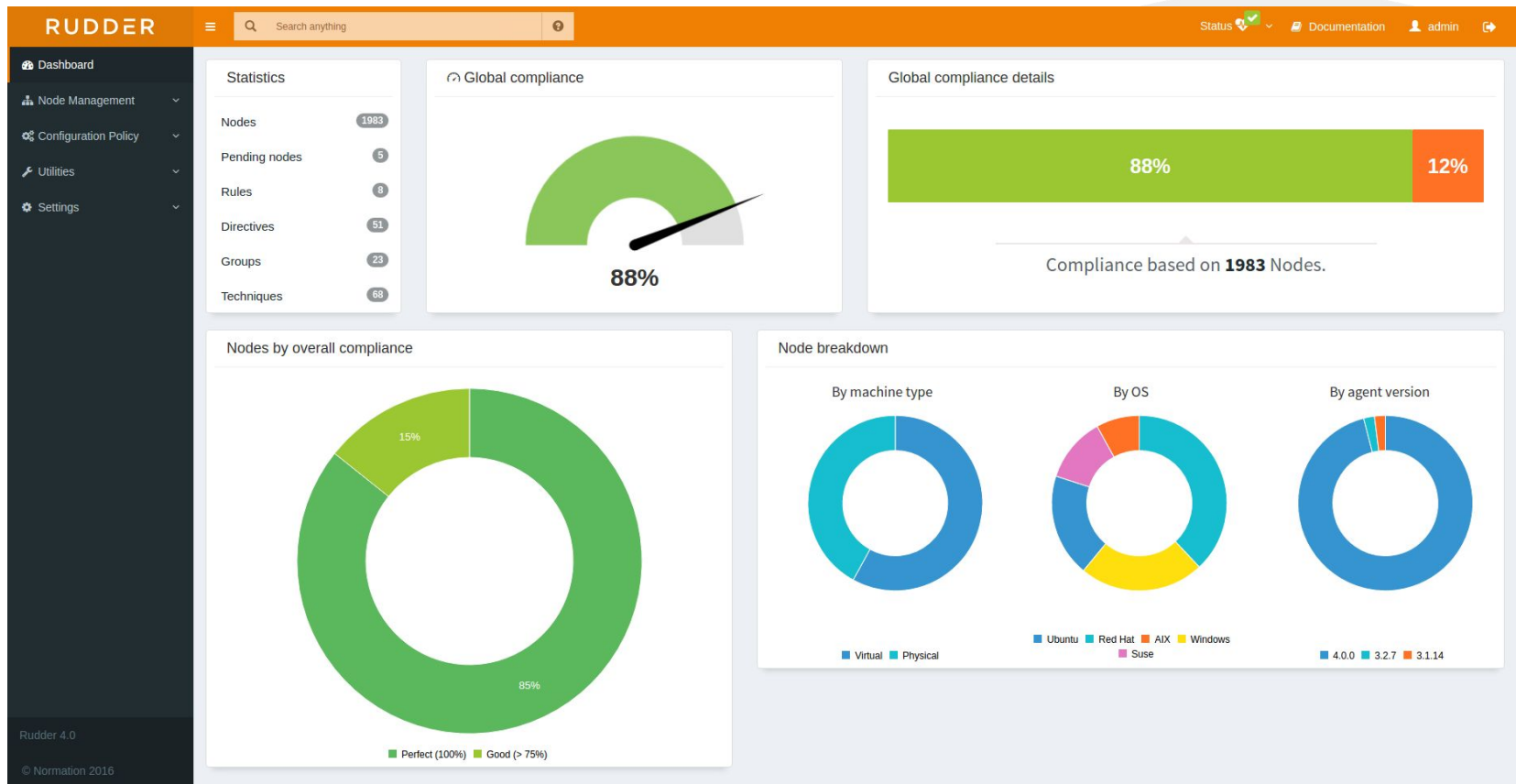
L'application d'une règle se fait au travers d'un groupe

- 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



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**



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