Rudder

Poziom: podstawy **Dotyczy: Rudder 7.x, agent na Linux** **Czas: ~15 min**

Rudder odpowiada na inne pytanie niż Ansible — nie „jak wykonać zmianę teraz", tylko „jak upewnić się, że nikt jej po cichu nie cofnął".

Skróty użyte na tej stronie (2)

Skrót	Co znaczy
HMAC	Hash-based Message Authentication Code: kod potwierdzający, że wiadomość pochodzi od kogoś, kto zna klucz, i nie została zmieniona; w genericDDNS na FortiGate używany jest HMAC-MD5
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera

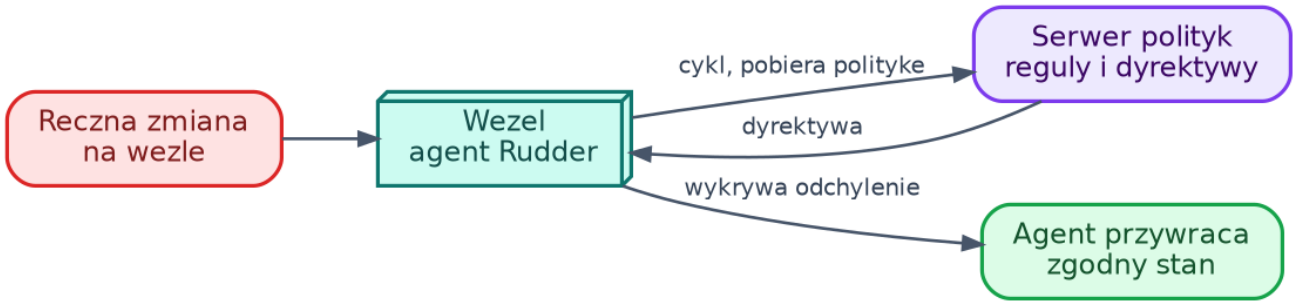
Z życia wzięte

Z ŻYCIA WZIĘTE

Tomek poprawia w piątek ręcznie `sshd_config` na `app01`, żeby naprawić pilny problem z połączeniem agenta Jenkinsa, i zapomina zgłosić zmianę reszcie zespołu. W poniedziałek zmiana już nie istnieje, a Tomek jest przekonany, że coś ją cofnęło samo z siebie. Dopiero Ola przypomina mu, że `app01` jest objęty regułą Rudder pilnującą dokładnie tego pliku, więc jedyny trwały sposób zmiany to edycja dyrektywy na serwerze polityk.

Czym jest Rudder

Pojęcie: Rudder. Narzędzie do ciągłego zarządzania konfiguracją w modelu pull — w odróżnieniu od Ansible (patrz Ansible, AWX, Semaphore, Rudder, Terraform: co do czego) nie łączy się z zarządzanymi maszynami z zewnątrz, tylko instaluje na każdej z nich agenta, który sam, cyklicznie (domyślnie co kilka minut), sprawdza politykę zapisaną na centralnym serwerze i stosuje ją lokalnie, niezależnie od tego, czy ktokolwiek akurat o tym pamięta.



Reczna zmiana na wezle zostaje wykryta przez agenta Rudder przy najblizszym cyklu i cofnieta do stanu zgodnego z dyrektywa (kliknięcie otwiera pełny rozmiar)

Ta różnica ma konkretną konsekwencję operacyjną — jeśli ktoś ręcznie zmieni konfigurację objętą polityką Rudder (na przykład edytując plik, który polityka pilnuje), agent przy najbliższym cyklu wykryje odchylenie i przywróci stan zgodny z polityką sam, bez interwencji administratora. Ansible tego nie robi — playbook naprawia stan tylko wtedy, gdy ktoś go faktycznie uruchomi ponownie.

Reguły i dyrektywy

> **Pojęcie: dyrektywa.** Konkretna, sparametryzowana instancja gotowej techniki (technique) — np. „upewnij się, że w pliku `sshd_config` istnieje wpis `MACs` z określoną listą algorytmów" z konkretnymi wartościami parametrów wypełnionymi dla danego przypadku.

> **Pojęcie: reguła.** Powiązanie dyrektywy z grupą węzłów, na których ma zostać zastosowana — sama dyrektywa nic nie robi, dopóki nie zostanie przypisana regułą do konkretnego zestawu maszyn.

Przykład z życia: gdy centralny system (w tym wypadku Jenkins łączący się po SSH do agentów, patrz Agenci: dodanie, diagnostyka, utrzymanie) wymaga konkretnego algorytmu HMAC w negocjacji SSH, a maszyny docelowe mają ten algorytm scentralizowanie wymuszony przez Rudder, ręczna zmiana `sshd_config` na jednej maszynie nie utrzyma się długo — reguła Rudder przywróci oczekiwaną wartość przy najbliższym cyklu agenta, dopóki zmiana nie zostanie wprowadzona właściwie, czyli przez modyfikację samej dyrektywy na serwerze polityk.

Węzły i ich akceptacja

> **Pojęcie: węzeł (node).** Maszyna z zainstalowanym agentem Rudder, zarejestrowana w systemie. Nowy węzeł po pierwszym uruchomieniu agenta nie zaczyna od razu otrzymywać polityk — trafia do kolejki oczekujących na ręczną akceptację przez administratora serwera polityk, co jest świadomym punktem kontrolnym zapobiegającym przypadkowemu (albo złośliwemu) dołączeniu nieautoryzowanej maszyny do zarządzanej floty.

Instalacja agenta i podłączenie węzła do serwera polityk

```
curl https://repository.rudder.io/tools/rudder-setup | bash -s setup-agent 7.2
rudder.zielona.example
```

Skrypt instaluje agenta w podanej wersji (`7.2`) i konfiguruje go tak, żeby łączył się do wskazanego serwera polityk (`rudder.zielona.example`) — od tego momentu węzeł czeka na akceptację po stronie serwera, zanim zacznie faktycznie otrzymywać i stosować jakiekolwiek reguły.

Raportowanie zgodności

> **Pojęcie: raport zgodności (compliance report).** Agent po każdym cyklu wysyła do serwera polityk wynik zastosowania każdej reguły — czy stan był już zgodny, czy wymagał naprawy, czy naprawa się nie powiodła. Interfejs Rudder agreguje te raporty w widoczny na pierwszy rzut oka procent zgodności per węzeł i per reguła, co pozwala od razu zobaczyć, które maszyny odbiegają od oczekiwanego stanu, bez ręcznego sprawdzania każdej z osobna.

Częste błędy

Ręczna, punktowa zmiana konfiguracji objętej regułą Rudder zamiast zmiany samej dyrektywy. Zmiana wprowadzona bezpośrednio na maszynie zostaje cofnięta przy najbliższym cyklu agenta — jedyny trwały sposób zmiany to edycja dyrektywy na serwerze polityk.

Automatyczna akceptacja nowych węzłów bez weryfikacji. Punkt akceptacji węzła istnieje po to, żeby ktoś świadomie potwierdził, że dana maszyna ma prawo dołączyć do zarządzanej floty — wyłączenie tego kroku jako „uciążliwej formalności" znosi tę kontrolę.

Ćwiczenia

> Zadania sprawdzające.

1. Wyjaśniamy, co się stanie, jeśli administrator ręcznie zmieni plik konfiguracyjny objęty regułą Rudder na jednej maszynie.
2. Opisujemy różnicę między techniką, dyrektywą i regułą w Rudder.
3. Nowy serwer ma zainstalowanego agenta Rudder i łączy się do serwera polityk, ale nie otrzymuje żadnych reguł. Wskazujemy najbardziej prawdopodobny powód.

Powiązane: Ansible, AWX, Semaphore, Rudder, Terraform: co do czego · Agenci: dodanie, diagnostyka, utrzymanie

---

Revision #37
Created 2026-09-25 07:40:09 UTC by Tomasz Konieczny
Updated 2026-10-26 14:13:35 UTC by Tomasz Konieczny