Zmiany i porządek

Bezpieczne zmiany, konfiguracja w NetBoksie i wiedza w BookStacku.

- Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć
- Konfiguracja i wiedza: NetBox jako CMDB i BookStack jako baza wiedzy

Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć

◫◫ Poziom: średnio

◫◫ Dotyczy: każda zmiana w infrastrukturze Zielonej, GLPI, repozytorium konfiguracji w Gitea

▯ Czas: ~40 min

Większość awarii w firmie takiej jak Zielona zaczyna się od zmiany: aktualizacji, nowej reguły na zaporze, „szybkiej poprawki" w piątek. Strona opisuje trzy rodzaje zmian, kto w dwuosobowym zespole zatwierdza którą, kiedy wolno je robić, jak ocenić ryzyko kolorem karty z Fiszki i jak zapisać plan wycofania. Na końcu jest szablon wniosku o zmianę.

◫◫ Skróty użyte na tej stronie (7)

Skrót	Co znaczy
CAB	Change Advisory Board: rada do spraw zmian, grupa osób oceniająca i zatwierdzająca zmiany; w ITIL 4 tylko jeden z możliwych organów zmian, nie obowiązek
ECAB	Emergency Change Advisory Board: wąski skład zatwierdzający zmiany awaryjne, w małej firmie zwykle drugi administrator przez telefon
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

TYLKO ODCZYT

Ocena rodzaju zmiany: standardowa, normalna, awaryjna

```
Standardowa: jest na liście zmian standardowych, ma artykuł z krokami, robiliśmy ją wiele razy bez awarii
Normalna:    każda inna planowana zmiana; wymaga oceny ryzyka i zatwierdzenia przed wykonaniem
Awaryjna:    trzeba ją zrobić teraz, żeby przywrócić usługę albo zamknąć lukę bezpieczeństwa
```

Gdy wahamy się między standardową a normalną, wybieramy normalną. Awaryjna nie jest sposobem na pominięcie zatwierdzenia, tylko na przyspieszenie go.

TYLKO ODCZYT

Ocena ryzyka zmiany: kolor najgroźniejszej karty

```
Zielona:      plan zawiera tylko odczyt (sprawdzenia, raporty); zmiana konfiguracji w GLPI nie jest potrzebna
Pomarańczowa: plan zawiera polecenia, które zmieniają albo restartują system, a wycofanie trwa do 30 minut
Czerwona:     plan zawiera polecenia nieodwracalne (usuwanie, formatowanie, migracja schematu bazy)
              albo wycofanie trwa dłużej niż 30 minut, albo dotyczy usługi krytycznej w jej szczycie
```

Kolor zmiany to kolor najgroźniejszej karty w jej planie, tak jak oznacza je konwerter na stronach tej bazy. Czerwona zmiana zawsze ma drugą parę oczu i świeżą kopię.

TYLKO ODCZYT

Sprawdzenie okna zmian: kalendarz Zielonej

```
Okno tygodniowe:        wtorek 17:00 do 20:00 (serwery i sieć)
Okno aktualizacji Windows: trzeci wtorek miesiąca, 18:00 do 21:00 (tydzień po Patch
Tuesday)
Zakaz zmian normalnych: 15 listopada do 6 stycznia
Bez zmian:              ostatnie 3 dni robocze miesiąca dla sql01 i Optimy
Bez zmian:              5:30 do 8:00 dla ora01, WMS i sieci Swarzędza
Bez zmian normalnych:   piątek od 14:00
```

Patch Tuesday to drugi wtorek miesiąca, dzień, w którym Microsoft wydaje poprawki. Tydzień przerwy daje czas na pilotaż na kilku komputerach i serwerze testowym.

□□ TYLKO ODCZYT

Zapisanie planu wycofania: przed wykonaniem

```
Punkt powrotu: kopia albo migawka (nazwa, godzina), eksport konfiguracji (plik, miejsce)
Kryterium wycofania: po czym poznamy, że trzeba wracać (np. WMS nie loguje skanera w 5
minut)
Kroki wycofania: ponumerowane, z poleceniami do skopiowania
Czas wycofania: ile minut, sprawdzone albo oszacowane
Decyzja: kto decyduje o wycofaniu i do której godziny najpóźniej
```

Plan wycofania piszemy przed zmianą, gdy mamy spokojną głowę. Zmiana bez planu wycofania nie dostaje zatwierdzenia, nawet jeśli wydaje się prosta.

□□ ZMIENIA SYSTEM

Wpis do dziennika zmian: numer zmiany w opisie commita

```
git commit -m "CHG-NNNN: krótki opis zmiany"
```

Każda zmiana konfiguracji trzymanej w repozytorium (`compose.yaml`, playbooki, eksporty konfiguracji `fw01`) ma w opisie numer zmiany z GLPI. Po roku `git log --grep CHG-0042` pokazuje, co dokładnie ta zmiana zmieniła.

Przykład:

```
$ git log --oneline --grep "CHG-0042"
3f1c9a2 CHG-0042: GLPI 12.0.0, nowy obraz i MariaDB 11.4.13
```

□□ **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 · **git** = system kontroli wersji (nazwa to brytyjski slang: nieznośny typ)

□□ TYLKO ODCZYT

Zamknięcie zmiany: przegląd po wdrożeniu

```
Czy zmiana osiągnęła cel? tak / nie / częściowo
Czy były incydenty w ciągu 48 godzin po zmianie? numery INC
Czy NetBox i baza wiedzy są zaktualizowane? tak / nie dotyczy
Czy plan wycofania był potrzebny? tak / nie
Wynik: udana / udana z problemami / wycofana / nieudana
```

Zmianę zamykamy po 48 godzinach obserwacji, a nie zaraz po wykonaniu. Wynik zasila jedną z metryk zespołu: odsetek zmian bez incydentu.

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Piątek, 15:50. Tomek dodaje na `fw01` regułę dla nowego dostawcy etykiet, bo „to jedna linijka”, i wychodzi do domu. O 16:20 handlowcy w terenie tracą VPN, bo nowa reguła stanęła w kolejności przed regułą dla puli 10.20.200.0/24. Starszy administrator przez godzinę szuka przyczyny w logach, bo nigdzie nie ma zapisu, że ktoś coś zmieniał. Po tym piątku na tablicy w pokoju IT wisi kartka: zmiany normalne do czwartku, każda z numerem w GLPI.

Jak to działa

□□ **Rozwiń: jak to działa pod spodem**

Zmiana i trzy jej rodzaje

> **Pojęcie: umożliwianie zmian (change enablement).** Praktyka, której celem jest zwiększenie liczby udanych zmian przez rzetelną ocenę ryzyka, zatwierdzanie zmian i zarządzanie ich harmonogramem [1]. Do edycji 2011 praktyka nazywała się zarządzaniem zmianami (change management). W pierwszym wydaniu ITIL 4 Foundation nazwano ją kontrolą zmian (change control), a po krytycznych głosach branży nazwę poprawiono na umożliwianie zmian, żeby podkreślić, że chodzi o to, by zmiany były możliwe i bezpieczne, a nie żeby je blokować.

> **Pojęcie: zmiana standardowa.** Zmiana o niskim ryzyku, dobrze znana, w pełni opisana i zatwierdzona z góry; wykonujemy ją bez osobnego zatwierdzania za każdym razem [1]. Zwykle zaczyna się od wniosku o usługę albo jest rutyną.

> **Pojęcie: zmiana normalna.** Zmiana, którą trzeba zaplanować, ocenić i zatwierdzić przed wykonaniem, według jej ryzyka [1].

> **Pojęcie: zmiana awaryjna.** Zmiana, którą trzeba wdrożyć jak najszybciej, na przykład żeby zakończyć incydent albo załatać aktywnie wykorzystywaną lukę [1]. Ocena i zatwierdzenie są przyspieszone, a dokumentację uzupełniamy po fakcie.

Lista zmian standardowych Zielonej (każda pozycja z artykułem w bazie wiedzy):

Zmiana standardowa	Warunek	Artykuł
Aktualizacja Windows na stacjach przez pierścienie Intune	według harmonogramu pierścieni	Aktualizacje Windows i raporty: pierścienie, Autopatch, zgodność floty
Aktualizacja serwera Windows w oknie miesięcznym	poza `sql01` w zamknięciu miesiąca i poza `dc01` i `dc02` naraz	Standardowa aktualizacja systemu produkcyjnego (Windows)
Dodanie użytkownika do grupy z wniosku	wniosek zatwierdzony w katalogu	Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu
Odnowienie certyfikatu bez zmiany nazwy	ten sam urząd certyfikacji, ta sama nazwa	artykuł w bazie wiedzy dla danej usługi
Aktualizacja poprawkowa obrazu kontenera (ta sama wersja główna, np. 12.0.0 do 12.0.1)	aplikacja ma stronę kopii i aktualizacji, kopia sprzed zmiany	strona „Kopia zapasowa i aktualizacja” danej aplikacji

Zmiana standardowa	Warunek	Artykuł
Dodanie adresu do istniejącej grupy adresów na `fw01`	bez nowych reguł i bez zmiany kolejności	artykuł w bazie wiedzy o `fw01`

Wszystko spoza tej listy jest zmianą normalną. Pozycję dopisujemy do listy dopiero wtedy, gdy zmianę zrobiliśmy kilka razy jako normalną bez incydentu i mamy do niej artykuł.

Kto zatwierdza w małej firmie

> **Pojęcie: organ zatwierdzający zmianę.** Osoba albo grupa, która ma prawo zatwierdzić daną zmianę [1]. W starszych wersjach ITIL rolę tę pełnił CAB (Change Advisory Board), czyli komitet doradczy do spraw zmian, a dla zmian awaryjnych ECAB (Emergency CAB). ITIL 4 zaleca, żeby organ dobierać do rodzaju i ryzyka zmiany, a zatwierdzanie przesuwać jak najbliżej osób, które znają system.

W dwuosobowym zespole nie zwołujemy komitetu na każdą zmianę. Organem zatwierdzającym jest najczęściej drugi administrator, a dla zmian dotykających usług krytycznych dochodzi klient usługi.

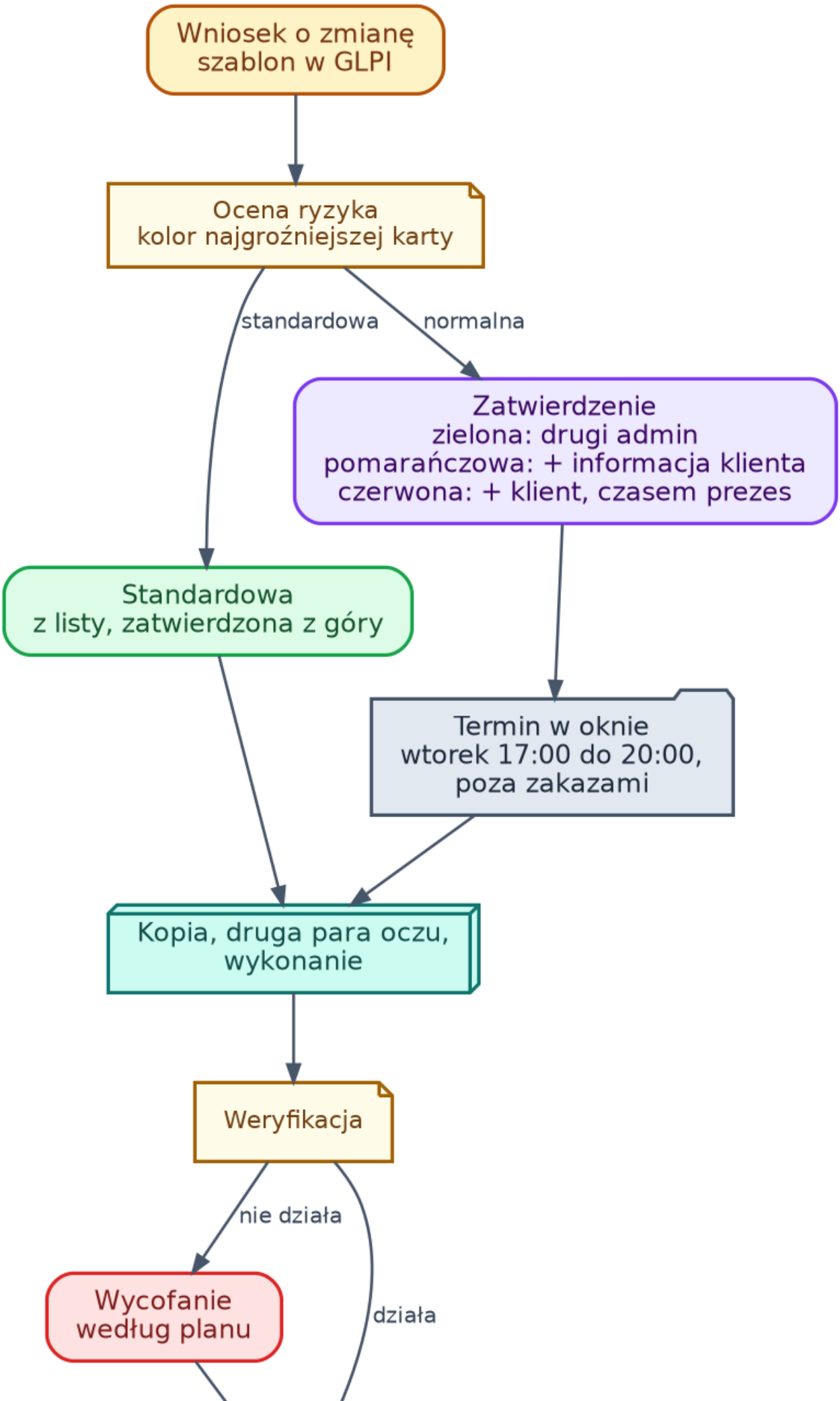
Rodzaj i kolor	Kto zatwierdza	Jak
Standardowa	zatwierdzona z góry (lista wyżej)	wykonujemy według artykułu, wpis w GLPI
Normalna zielona	drugi administrator	akceptacja w GLPI
Normalna pomarańczowa	drugi administrator, klient usługi informowany	akceptacja w GLPI, mail do klienta z terminem
Normalna czerwona	drugi administrator i klient usługi; pan Zbigniew, gdy zmiana dotyczy całej firmy albo kosztuje	akceptacja w GLPI obu osób, omówienie na przeglądzie tygodniowym
Awaryjna	drugi administrator telefonicznie; gdy nieosiągalny, kierujący incydentem sam, z decyzją decydenta biznesowego	wpis w GLPI w ciągu jednego dnia roboczego, omówienie na najbliższym przeglądzie

Przegląd tygodniowy we wtorek rano pełni w Zielonej rolę CAB: piętnaście minut na zmiany planowane w tym tygodniu, z Olą, gdy dotyczą jej aplikacji. Opisuje go strona Standard pracy administratora Zielonej: zasady na pierwszy dzień.

> ⚠ Zatwierdzenie przez drugą osobę ma sens tylko wtedy, gdy ta osoba naprawdę przeczytała plan i plan wycofania. Kliknięcie „akceptuję” bez lektury to formalność, która daje fałszywe poczucie bezpieczeństwa.

Przepływ zmiany

Każda zmiana normalna przechodzi tę samą drogę. Zmiana standardowa skraca ją do wykonania i zamknięcia, a awaryjna przesuwa dokumentację na koniec.


Wniosek o zmianę szablon w GLPI
Ocena ryzyka kolor najgroźniejszej karty
standardowa
normalna
Zatwierdzenie zielona: drugi admin pomarańczowa: + informacja klienta czerwona: + klient, czasem prezes
Standardowa z listy, zatwierdzona z góry
Termin w oknie wtorek 17:00 do 20:00, poza zakazami
Kopia, druga para oczu, wykonanie
Weryfikacja
nie działa
działa
Wycofanie według planu

Rysunek 1. Przepływ zmiany normalnej w Zielonej: wniosek, ocena ryzyka kolorem karty, zatwierdzenie dobrane do koloru, zaplanowanie w oknie, kopia i wykonanie, weryfikacja albo wycofanie, przegląd po 48 godzinach i zamknięcie (kliknięcie otwiera pełny rozmiar)

Okna zmian i zakazy

> **Pojęcie: okno zmian.** Umówiony czas, w którym wolno wykonywać zmiany normalne, wybrany tak, żeby ewentualna awaria dotknęła jak najmniej osób i żeby został czas na wycofanie.

Zmiany normalne wykonujemy w oknie. Poza oknem tylko wyjątkowo, za zgodą organu zatwierdzającego zapisaną w GLPI, i nigdy w okresach z tabeli niżej.

> **Pojęcie: zakaz zmian.** Okres, w którym zmian normalnych nie wykonujemy wcale, bo każda przerwa kosztuje najwięcej. W Zielonej to szczyt sezonu od 15 listopada do 6 stycznia.

Okres	Co wolno	Dlaczego
Wtorek 17:00 do 20:00	zmiany normalne każdego koloru	biuro kończy pracę, magazyn ma jeszcze zmianę, ale przed nami trzy dni robocze na wykrycie skutków
Trzeci wtorek miesiąca 18:00 do 21:00	aktualizacje serwerów Windows	tydzień po Patch Tuesday, po pilotażu
Piątek od 14:00, weekend	tylko standardowe i awaryjne	nikt nie zauważy skutków do poniedziałku, a wsparcie jest najsłabsze
Ostatnie 3 dni robocze miesiąca	bez zmian na `sql01`, Optimie i jej zależnościach (domena, sieć biura, `fs01`)	zamknięcie miesiąca w księgowości
Codziennie 5:30 do 8:00	bez zmian na `ora01`, WMS, sieci i Wi-Fi Swarzędza	start zmiany, 40 skanerów loguje się naraz
15 listopada do 6 stycznia	tylko standardowe i awaryjne; normalne wyłącznie za zgodą pana Zbigniewa	szczyt sezonu, magazyn na trzy zmiany

> Zmiany planowane na grudzień przenosimy na drugi tydzień stycznia, a nie na pierwszy: 7 stycznia wszyscy wracają z zaległościami i każda awaria

> uderza mocniej.

Ocena ryzyka i karty z Fiszki

Na każdej stronie tej bazy konwerter koloruje karty Fiszki według tego, co robi polecenie: zielone tylko czytają, pomarańczowe zmieniają albo restartują, czerwone usuwają albo są nieodwracalne. Ten sam kolor wykorzystujemy do oceny zmiany: plan zmiany składa się z kart, a zmiana dostaje kolor najgroźniejszej z nich.

Kolor z kart to dopiero punkt wyjścia. Podnosimy go o stopień, gdy odpowiedź na którekolwiek z tych pytań jest niepokojąca:

Pytanie	Podnosi ryzyko, gdy
Czy zmiana dotyka usługi krytycznej (Optima, WMS, poczta, domena, `fw01`)?	tak
Czy robiliśmy to już w Zielonej?	nie, robimy pierwszy raz
Czy przetestowaliśmy na laboratorium albo na kopii?	nie
Czy wycofanie trwa dłużej niż 30 minut albo wymaga odtworzenia z kopii?	tak
Czy zmiana dotyka wielu elementów naraz (cały klaster, wszystkie stacje)?	tak
Czy zależy od dostawcy, który może być nieosiągalny?	tak

Czerwona zmiana zawsze ma: drugą parę oczu przy wykonaniu (druga osoba czyta polecenia przed wciśnięciem Enter), świeżą kopię albo migawkę sprawdzoną przed startem i plan wycofania z decyzją, do której godziny najpóźniej wycofujemy.

Szablon wniosku o zmianę

Ten sam szablon ustawiamy w GLPI dla zgłoszeń typu zmiana. Pola odpowiadają kartom z Fiszki.

```
numer: CHG-NNNN
tytuł: "[Usługa albo element] co zmieniamy"
rodzaj: "standardowa | normalna | awaryjna"
powód: "dlaczego, numer incydentu, problemu albo wniosku"
elementy_konfiguracji: [NazwaSerwera, NazwaUsługi]
```

```
wpływ_na_użytkowników: "kto, jak długo, czy będzie przerwa"
kolor_ryzyka: "zielona | pomarańczowa | czerwona"
uzasadnienie_koloru: "najgroźniejsza karta w planie i odpowiedzi na pytania o ryzyko"
termin: "RRRR-MM-DD GG:MM do GG:MM, okno"
plan:
  - "krok 1 z poleceniem"
  - "krok 2 z poleceniem"
weryfikacja: "po czym poznamy, że się udało"
plan_wycofania:
  punkt_powrotu: "kopia albo migawka, nazwa i godzina"
  kryterium: "kiedy wracamy"
  kroki: ["krok 1", "krok 2"]
  czas_minut: 30
  decyduje: "imię, najpóźniej o GG:MM"
zatwierdzający: [drugi administrator, klient usługi]
komunikat_dla_użytkowników: "treść albo: niepotrzebny"
aktualizacja_netbox_i_wiedzy: "co poprawiamy po zmianie"
```

> **Pojęcie: wniosek o zmianę.** Formalna prośba o wprowadzenie zmiany, opisująca, co, dlaczego, kiedy i z jakim ryzykiem zmieniamy. Bywa skracany jako RFC (Request for Change); w słowniku tej bazy RFC oznacza też dokumenty opisujące standardy internetu, więc znaczenie wynika z kontekstu.

Częste błędy

Objaw	Przyczyna	Co robimy
Awaria w poniedziałek po zmianie w piątek	zmiana normalna poza oknem	piątek od 14:00 tylko standardowe i awaryjne
Przy diagnozie nikt nie wie, co się zmieniło	zmiana bez wpisu	każda zmiana ma numer w GLPI, commit z numerem, lista z 48 godzin jako pierwszy krok diagnozy
Wszystko jest zmianą awaryjną	awaryjna jako sposób na pominięcie zatwierdzenia	przegląd tygodniowy liczy zmiany awaryjne; więcej niż jedna w miesiącu to temat do rozmowy
Wycofanie trwa trzy godziny zamiast trzydziestu minut	plan wycofania wymyślany w trakcie awarii	plan wycofania obowiązkowy przed zatwierdzeniem, czas sprawdzony na laboratorium

Objaw	Przyczyna	Co robimy
Migawka maszyny wisi od miesiąca	migawka zostawiona po zmianie	usunięcie migawki jest ostatnim krokiem planu, sprawdzane przy zamknięciu
Zatwierdzający nie wie, co zatwierdził	akceptacja bez lektury	drugi administrator zadaje co najmniej jedno pytanie do planu, zapisane w GLPI
NetBox nie zgadza się z rzeczywistością po zmianie	aktualizacja dokumentacji poza zmianą	aktualizacja NetBoksa i bazy wiedzy jest krokiem planu, bez niej zmiana nie jest zamknięta

□□ Ćwiczenia

1. W czwartek 12 listopada Ola prosi o nową wersję aplikacji cennika na `docker01` przed świętami. Co odpowiadamy?

Odpowiedź

Ostatnie okno tygodniowe przed zakazem (wtorek 10 listopada) już minęło, a następne (17 listopada) wypada w zakazie zmian. Zostaje wyjątek poza oknem, najpóźniej w piątek 13 listopada przed 14:00, za zgodą drugiego administratora i z oceną ryzyka, albo zgoda pana Zbigniewa na zmianę w czasie zakazu. Najczęściej rozsądna odpowiedź to drugi tydzień stycznia, chyba że brak nowej wersji kosztuje firmę pieniądze w sezonie.

1. Plan zmiany zawiera `docker compose pull`, `docker compose up -d` i migrację bazy uruchamianą automatycznie przy starcie nowej wersji. Jaki kolor?

Odpowiedź

Czerwony. Same polecenia Compose są pomarańczowe, ale migracja schematu bazy jest nieodwracalna bez odtworzenia z kopii, a wycofanie przez odtworzenie trwa zwykle dłużej niż 30 minut. Potrzebna jest świeża kopia bazy, druga para oczu i plan wycofania z odtworzeniem.

1. Wtorek, 22:30. Producent zapory ogłasza krytyczną lukę wykorzystywaną w atakach, a poprawka jest dostępna. Jak przebiega zmiana?

Odpowiedź

Jako zmiana awaryjna: telefon do drugiego administratora, szybka ocena (kopia konfiguracji `fw01`, plan wycofania do poprzedniego oprogramowania), komunikat do handlowców o możliwej przerwie VPN, wykonanie, weryfikacja. Wpis w GLPI uzupełniamy następnego dnia roboczego, a na przeglądzie tygodniowym omawiamy, czy dało się to przewidzieć.

1. Tomek chce dopisać do listy zmian standardowych „restart kontenera na `docker01`". Czy to dobry kandydat?

Odpowiedź

Tylko z zawężeniem: restart konkretnego kontenera bez bazy danych, poza oknem 5:30 do 8:00 i poza zamknięciem miesiąca dla aplikacji, od których zależy Optima, z artykułem i kryterium sukcesu. Ogólny „restart dowolnego kontenera" jest za szeroki, bo kontener z bazą albo MailCow to zupełnie inne ryzyko niż kontener z prostą stroną.

Powiązane: Standardowa aktualizacja systemu produkcyjnego (Windows) · Aktualizacje Windows i raporty: pierścienie, Autopatch, zgodność floty · Problemy, analiza przyczyn i postmortem: żeby ta sama awaria nie wróciła · Cykl życia produktu i usługi: osiem działań i pojęcia z pracy na co dzień

Źródła: [1] Parafraza własna na podstawie: AXELOS, „ITIL Foundation, ITIL 4 Edition" (2019), praktyka change enablement (rodzaje zmian, organ zatwierdzający, harmonogram zmian) i hasło change. · itsm.tools, „Change Enablement in ITIL 4" (historia nazw: change management, change control, change enablement). · Microsoft: Patch Tuesday, czyli drugi wtorek miesiąca, w którym Microsoft wydaje comiesięczne aktualizacje zabezpieczeń. · Okna, zakazy i lista zmian standardowych: standard Zielonej zatwierdzony 11 października 2026, oparty na kalendarzu awarii ze strony o świecie Zielonej.

Konfiguracja i wiedza: NetBox jako CMDB i BookStack jako baza wiedzy

Poziom: średnio

Dotyczy: NetBox na docker01 (netbox.zielona.example), BookStack (wiedza.zielona.example), GLPI

Czas: ~35 min

Dwie praktyki, bez których reszta tej książki działa na pamięć: zarządzanie konfiguracją (co mamy i co od czego zależy) i zarządzanie wiedzą (jak to robimy i co już wiemy). W Zielonej pierwszą prowadzimy w NetBoksie, drugą w tej bazie BookStack. Strona mówi, co dokładnie zapisujemy, jakie relacje między elementami są nam potrzebne, kiedy piszemy artykuł i jak pilnujemy, żeby wiedza się nie zestarzała.

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
CMDB	Configuration Management Database: baza konfiguracji, czyli spis elementów, z których składają się usługi, i ich powiązań; w Zielonej rolę tę pełni NetBox
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
ITSM	IT Service Management: zarządzanie usługami IT, czyli prowadzenie IT jak zestawu usług dla reszty firmy, a nie tylko utrzymanie sprzętu; tak też nazywa się klasa programów do zgłoszeń, jak GLPI

Skrót	Co znaczy
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

□□ KLIKAMY W INTERFEJSIE

Sprawdzenie, z czego składa się usługa: filtr tagu w NetBoksie

```
netbox.zielona.example → Virtualization → Virtual Machines → Filters → Tag: usluga-optima
```

Każdy element konfiguracji, od którego zależy usługa, ma tag usługi (`usluga-optima`, `usluga-wms`, `usluga-poczta`). Ta sama lista dla urządzeń fizycznych jest w Devices → Devices z tym samym filtrem.

□□ TYLKO ODCZYT

Odczyt elementów usługi przez API: curl i jq

```
curl -s -H "Authorization: Bearer nbt_KluczTokenu.TokenAPI" "https://netbox.zielona.example/api/virtualization/virtual-machines/?tag=NazwaTagu" | jq -r '.results[] | [.name, .cluster.name, .status.value] | @tsv'
```

> (gdzie `NazwaTagu` to tag usługi, np. `usluga-optima`, a token ma uprawnienia tylko do odczytu)

Zwraca maszyny wirtualne usługi z klastrem i stanem. Przydaje się w skryptach przed zmianą: od razu widać, co jeszcze dotknie restart.

Przykład:

```
sql01□hvclu01□active
fs01□hvclu01□active
dc01□hvclu01□active
```

API = Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą · **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

KLIKAMY W INTERFEJSIE

Dodanie tagu usługi: Customization → Tags

```
netbox.zielona.example → Customization → Tags → Add → Name: usluga-NazwaUslugi, Slug: usluga-nazwauslugi, Color
```

Tag zakładamy raz na usługę z katalogu. Nazwy tagów usług zaczynamy od `usluga-`, żeby w filtrach nie myliły się z tagami technicznymi.

TYLKO ODCZYT

Wyszukanie znanych błędów w bazie wiedzy: tag typ

```
[typ=znany-blad] objaw
```

Wpisane w wyszukiwarkę `wiedza.zielona.example` zwraca strony z tagiem `typ` o wartości `znany-blad`, które zawierają słowo objawu. Tak samo działa `[typ=postmortem]` i `[usluga=wms]`.

TYLKO ODCZYT

Wyszukanie stron do przeglądu: filtr updated_before

```
{updated_before:RRRR-MM-DD} {type:page} [wlasciciel=nazwa_usera]
```

> (gdzie data to dzień sprzed sześciu miesięcy, a `nazwa_usera` to właściciel strony z tagu)

Zwraca strony danego właściciela, których nikt nie zmieniał od pół roku. To lista na comiesięczny przegląd wiedzy.

KLIKAMY W INTERFEJSIE

Dopisanie artykułu po incydencie: Książka → Nowa strona

```
wiedza.zielona.example → książka usługi → New Page → szablon „Znany błąd” albo „Postmortem” → tagi: typ, usluga, wlasciciel → Save Page
```

Artykuł piszemy przed zamknięciem incydentu albo problemu, a link wklejamy do zgłoszenia. Bez linku zgłoszenie nie przechodzi przeglądu tygodniowego.

Z życia wzięte

Z ŻYCIA WZIĘTE

Wtorek, 17:05, okno zmian. Tomek ma zrestartować `hv02` po aktualizacji i sprawdza w NetBoksie, co na nim stoi: maszyny z klastra `hvclu01`, w tym `sql01`, przeniosą się na `hv01` bez przerwy. NetBox nie mówi mu jednak, że `app01` stoi na `hv02` lokalnie, poza klastrem, i że na nim działa serwer licencji programu do etykiet, od którego zależą drukarki etykiet w Swarzędzu. Restart przechodzi gładko, ale serwer licencji nie wstaje sam po starcie maszyny i etykiety stoją do rana. W postmortemie pierwszym działaniem nie jest naprawa `app01`, tylko dopisanie w NetBoksie tagu `usluga-etykiety` do `app01` i do drukarek oraz zapisanie, że ta maszyna nie przenosi się automatycznie.

Jak to działa

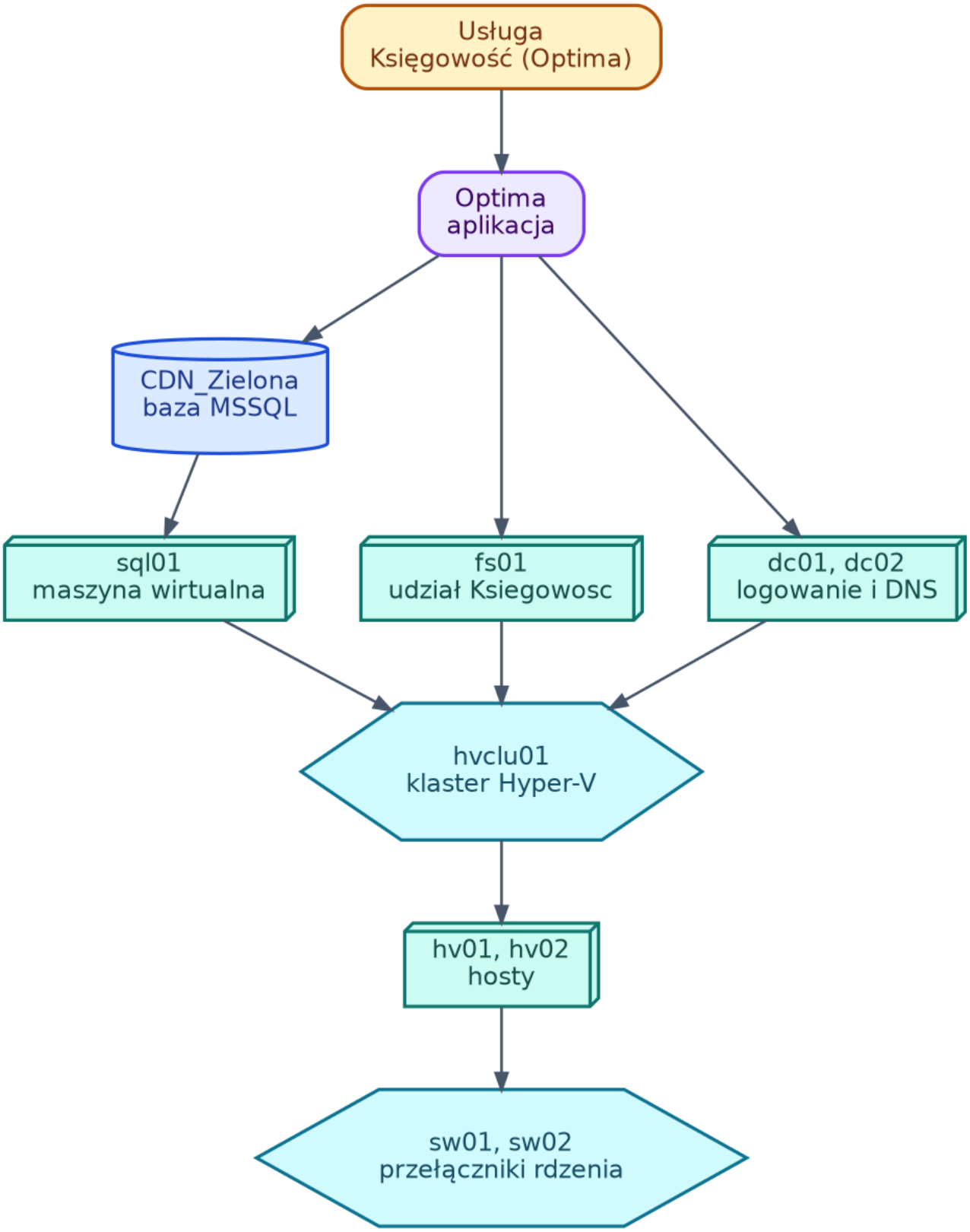
Rozwiń: jak to działa pod spodem

Zarządzanie konfiguracją

Pojęcie: zarządzanie konfiguracją usług. Praktyka, której celem jest zapewnienie, że dokładne i wiarygodne informacje o konfiguracji usług i elementów konfiguracji, w tym o relacjach między nimi, są dostępne wtedy i tam, gdzie są potrzebne [1].

Pojęcie: CMDB. Baza danych konfiguracji (Configuration Management Database): miejsce, w którym trzymamy elementy konfiguracji i ich relacje. ITIL v3 mówił obok niej o systemie zarządzania konfiguracją, czyli o zbiorze narzędzi i baz, które razem dają pełny obraz; w małej firmie ten system to kilka połączonych miejsc.

Dla Zielonej najważniejsze nie jest to, ile atrybutów ma każdy serwer, tylko to, czy przed zmianą i w trakcie awarii odpowiemy na dwa pytania: z czego składa się ta usługa i co jeszcze przestanie działać, jeśli ten element padnie. Do tego potrzebne są relacje, a nie tylko lista.



Rysunek 1. Relacje elementów konfiguracji dla usługi Księgowość (Optima): usługa zależy od aplikacji, bazy i serwera plików, te od maszyn wirtualnych, maszyny od klastra Hyper-V, klaster

od hostów i przełączników rdzenia, a logowanie od kontrolerów domeny (kliknięcie otwiera pełny rozmiar)

NetBox jako źródło prawdy i CMDB w Zielonej

NetBox stoi na `docker01` od dawna jako źródło prawdy o sieci i serwerowni: szafy, urządzenia, porty, kable, adresy IP, VLAN-y, maszyny wirtualne i klastry. Sam projekt opisuje się jako źródło prawdy o zamierzonym stanie sieci, czyli o tym, jak ma być, a nie o tym, co w tej sekundzie odpowiada na pingi; wśród rzeczy, którymi NetBox nie jest, wymienia monitoring sieci i zarządzanie konfiguracją w sensie narzędzi takich jak Ansible.

To dobrze pasuje do roli CMDB w małej firmie: zapisujemy stan zamierzony, a monitoring (Zabbix) mówi nam, kiedy rzeczywistość od niego odbiega. Pełnej CMDB w rozumieniu dużych systemów ITSM NetBox nie zastąpi, więc uzupełniamy go tak:

Co	Gdzie w Zielonej	Jak łączymy
Szafy, urządzenia, porty, kable, adresy, VLAN-y	NetBox (DCIM i IPAM)	źródło prawdy, inne narzędzia czytają przez API
Maszyny wirtualne i klastry	NetBox (Virtualization)	maszyna należy do klastra `hvclu01`, klaster do hostów `hv01` i `hv02`
Usługi z katalogu	tag `usluga-` w NetBoksie	każdy element usługi ma jej tag
Porty usług (np. MSSQL 1433 na `sql01`)	NetBox, obiekt Service przy maszynie	powiązanie aplikacji z maszyną i portem
Właściciel, krytyczność, poziom kopii	pola własne w NetBoksie	`wlasciciel`, `krytycznosc`, `poziom_kopii`
Laptopy i stacje użytkowników	Intune i GLPI	GLPI przypisuje sprzęt do użytkownika; NetBox ich nie prowadzi
Umowy z dostawcami, licencje	GLPI (Management)	numer umowy i czasy reakcji przy dostawcy
Historia zmian elementu	GLPI (zmiany) i dziennik zmian NetBoksa	numer zmiany w komentarzu do zmiany w NetBoksie

Relacje, które naprawdę zapisujemy. Żeby nie budować modelu na wyrost, zapisujemy tylko relacje, z których korzystamy przy zmianach i awariach:

1. Maszyna wirtualna należy do klastra, klaster do hostów (NetBox robi to sam).
2. Urządzenie ma interfejs połączony kablem z portem przełącznika (NetBox, okablowanie).

3. Element konfiguracji należy do usługi (tag `usluga-`).
4. Usługa ma właściciela i klienta (pole własne przy elementach i tabela usług w bazie wiedzy).
5. Element ma poziom kopii zapasowej z polityki retencji (pole własne `poziom_kopii`, wartości z tabeli na stronie Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje).

NetBox jest częścią zmiany. Zmiana, która dodaje, usuwa albo przenosi element, nie jest zamknięta, dopóki NetBox nie pokazuje nowego stanu. Krok „aktualizacja NetBoksa” stoi w szablonie wniosku o zmianę, a w komentarzu do zmiany w NetBoksie wpisujemy numer zmiany z GLPI.

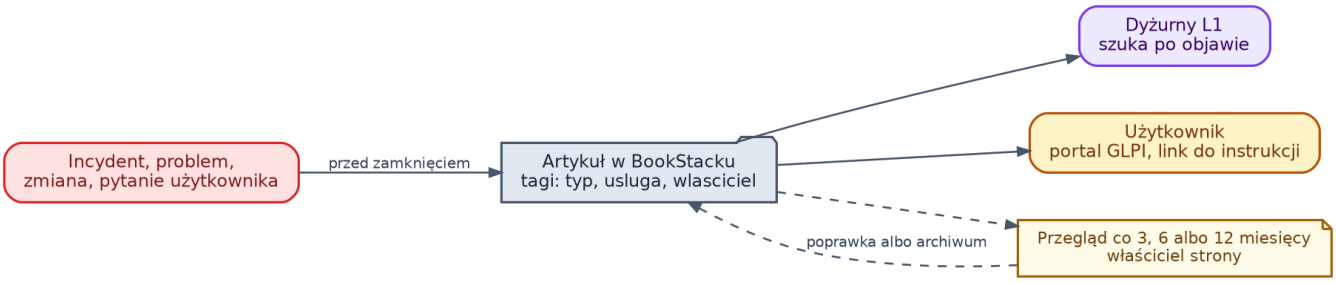
Przegląd zgodności. Raz na kwartał porównujemy NetBox z rzeczywistością: listę maszyn z Hyper-V, listę hostów z Zabbixa i listę adresów z DHCP. Każda różnica to albo brak w NetBoksie (dopisujemy), albo element, którego nie powinno być (zgłoszenie).

Instalację i codzienną pracę z NetBoksem opisują strony NetBox: źródło prawdy o sieci i serwerowni, Instalacja NetBoksa w Dockerze i NetBox: logowanie z AD, kopia i aktualizacja.

Zarządzanie wiedzą

> **Pojęcie: zarządzanie wiedzą.** Praktyka, której celem jest utrzymywanie i poprawianie skutecznego, wygodnego w użyciu korzystania z informacji i wiedzy w całej organizacji [1]. Chodzi nie o to, żeby wiedza była zapisana, tylko o to, żeby ktoś ją znalazł i jej użył w chwili, gdy jest potrzebna.

Bazą wiedzy Zielonej jest ta baza BookStack pod adresem `wiedza.zielona.example`. Ma półki, książki, rozdziały i strony, wersje każdej strony, wyszukiwarkę z tagami i logowanie kontem domenowym. GLPI ma własną bazę wiedzy; używamy jej tylko do krótkich odpowiedzi dla użytkowników w portalu, a każda taka odpowiedź linkuje do pełnej strony w BookStacku.



Rysunek 2. Obieg wiedzy w Zielonej: incydent, problem albo zmiana daje artykuł w BookStacku, artykuł ma właściciela i datę przeglądu, a L1 i użytkownicy korzystają z niego przy następnym zgłoszeniu (kliknięcie otwiera pełny rozmiar)

Rodzaje stron, które piszemy w ramach pracy z tej książki:

Rodzaj	Tag `typ`	Kiedy powstaje	Dla kogo
Znany błąd	`znany-blad`	gdy jest obejście problemu	L1, czasem użytkownik
Postmortem	`postmortem`	po każdym incydencie poważnym	zespół IT, zarząd (podsumowanie)
Procedura	`procedura`	gdy czynność powtarza się drugi raz	zespół IT
Zmiana standardowa	`zmiana-standardowa`	gdy zmiana trafia na listę standardowych	zespół IT
Instrukcja dla użytkownika	`instrukcja`	gdy to samo pytanie pada trzeci raz	użytkownicy, L0
Opis usługi	`usluga`	przy dodaniu usługi do katalogu	klient usługi, zespół IT

Artykuł po każdym incydencie. Każdy incydent P1 i P2 kończy się artykułem albo poprawką istniejącego: nowym znanym błędem, poprawioną procedurą albo instrukcją dla użytkownika. Incydent P3 i P4 kończy się artykułem, jeśli obejście nie było oczywiste. Link do artykułu wpisujemy w zgłoszeniu przed zamknięciem.

Tagi na każdej stronie. Trzy tagi są obowiązkowe: `typ` (z tabeli), `usluga` (z katalogu) i `wlasciciel` (login osoby, która odpowiada za aktualność). Dzięki nim wyszukiwanie z Fiszki działa, a przegląd da się zrobić jednym zapytaniem.

Cykl przeglądu. Wiedza się starzeje szybciej niż serwery. Raz w miesiącu każdy z nas uruchamia zapytanie z Fiszki dla swoich stron i dla każdej z wyników decyduje: aktualna (drobna poprawka, choćby zmiana daty w stopce, odnawia datę modyfikacji), do poprawy (zgłoszenie) albo do archiwum (przeniesienie do półki „Archiwum” z dopiskiem, czym ją zastąpiono).

Rodzaj strony	Przegląd co
Znany błąd	3 miesiące, a po trwałym rozwiązaniu oznaczenie jako rozwiązany
Procedura i zmiana standardowa	6 miesięcy i po każdej zmianie wersji systemu
Instrukcja dla użytkownika	12 miesięcy
Postmortem	bez przeglądu, to zapis historyczny

> □□ Najlepszym sprawdzianem artykułu jest Tomek: jeśli młodszy administrator wykona procedurę z samego artykułu, bez dopytywania, artykuł jest gotowy. Jeśli dopytuje, odpowiedź dopisujemy do artykułu, a nie tylko mówimy.

Częste błędy

Objaw	Przyczyna	Co robimy
Restart hosta wyłącza usługę, o której nikt nie pomyślał	brak relacji element do usługi	tag `usluga-` na każdym elemencie, sprawdzenie filtrem przed każdą zmianą na hoście
NetBox pokazuje serwer, którego nie ma od roku	aktualizacja NetBoksa poza zmianą	krok w szablonie zmiany, kwartalny przegląd zgodności
Próba zapisania w CMDB wszystkiego, łącznie z wersją każdej biblioteki	model na wyrost	zapisujemy tylko relacje, z których korzystamy przy zmianach i awariach
Artykuł istnieje, ale nikt go nie znajduje	brak tagów, tytuł w żargonie	trzy obowiązkowe tagi, tytuł słowami użytkownika
Procedura w bazie wiedzy nie działa	strona sprzed dwóch wersji systemu	przegląd co 6 miesięcy i po każdej zmianie wersji, właściciel w tagu
Ta sama wiedza w trzech miejscach (GLPI, BookStack, OneNote)	brak jednego źródła	BookStack jest źródłem, GLPI tylko linkuje, OneNote przenosimy

□□ Ćwiczenia

1. Przed aktualizacją `hv01` Tomek chce wiedzieć, które usługi dotknie restart. Jak to sprawdza?

Odpowiedź

W NetBoksie: maszyny wirtualne w klastrze `hvclu01` (które przejdą na `hv02`) i ich tagi `usluga-`. Potem sprawdza, czy `hv02` udźwignie wszystkie maszyny naraz, i czy któraś usługa nie jest w swoim oknie zakazu (Optima w zamknięciu miesiąca, WMS rano). Wynik wpisuje do wniosku o zmianę jako wpływ na użytkowników.

1. Ola dostaje drugi serwer na aplikacje zespołu, obok `app01`. Co musi się pojawić w NetBoksie, zanim zamkniemy zmianę?

Odpowiedź

Maszyna wirtualna w klastrze, adres IP przypisany do interfejsu, tagi usług, które na niej staną, pola własne (właściciel: Ola jako klient, właściciel w IT, krytyczność, poziom kopii) i obiekty Service dla portów aplikacji. W komentarzu do zmiany numer CHG z GLPI. Adres bierzemy z puli wolnych adresów w NetBoksie, a nie z pamięci.

1. Pani Halina trzeci raz w miesiącu pyta, jak dodać drukarkę w sekretariacie. Co robimy oprócz odpowiedzi?

Odpowiedź

Piszemy instrukcję dla użytkownika z tagami `typ=instrukcja`, `usluga=drukowanie`, właścicielem i krótkimi krokami ze zrzutami, a w GLPI dodajemy ją do odpowiedzi w portalu. Następne pytanie kończy się linkiem, a jeśli pytań jest dużo, zastanawiamy się, czy drukarka nie powinna instalować się sama przez GPO albo Intune.

1. Zapytanie przeglądowe zwraca procedurę aktualizacji MailCow sprzed ośmiu miesięcy. Co z nią robimy?

Odpowiedź

Sprawdzamy, czy od tamtej pory zmieniła się wersja MailCow albo sposób aktualizacji. Jeśli nie, poprawiamy drobiazg (datę sprawdzenia), co odnawia datę modyfikacji. Jeśli tak, zakładamy zgłoszenie na aktualizację procedury, a do tego czasu dopisujemy na górze ostrzeżenie, że strona może być nieaktualna.

Powiązane: NetBox: źródło prawdy o sieci i serwerowni · Problemy, analiza przyczyn i postmortem: żeby ta sama awaria nie wróciła · Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć · Jak czytać tę bazę wiedzy

Źródła: [1] Parafraza własna na podstawie: AXELOS, „ITIL Foundation, ITIL 4 Edition” (2019), praktyki service configuration management i knowledge management. · netboxlabs.com/docs/netbox/introduction (czym NetBox jest i czym nie jest, stan zamierzony, powiązania usług aplikacyjnych, pola własne). · bookstackapp.com/docs/user/searching (wyszukiwanie po tagach i filtry `{updated_before:}`, `{type:}`). · Częstotliwość przeglądów i zestaw tagów: propozycja autorów tej bazy.