Macierz usług Zielonej

Poziom rezerwy każdej usługi, zależności i kolejność prac.

- Macierz wysokiej dostępności usług Zielonej: poziom rezerwy każdej usługi, zależności i kolejność prac

Macierz wysokiej dostępności usług Zielonej: poziom rezerwy każdej usługi, zależności i kolejność prac

Poziom: średnio

Dotyczy: wszystkie usługi Zielonej, klaster hv01 i hv02, docker01, pg01, fw01, bkp01, zasilanie i chłodzenie serwerowni

Czas: ~45 min

Ta strona zbiera w jednej tabeli, jaki poziom rezerwy ma dziś każda usługa Zielonej, jaki proponujemy jej na przyszłość i jakim mechanizmem go osiągamy. Dokłada zależności między usługami, listę pojedynczych punktów awarii z kolejnością prac i kalendarz testów przełączenia. Wracamy tu przy planowaniu budżetu, przy rozmowie z właścicielem usługi i po każdej awarii.

ZAŁOŻENIA SCENARIUSZA

macierz przyjmuje stan dzisiejszy: pojedynczy `fw01` z jednym łączem (203.0.113.10), magazyn w sieci centrali (VLAN 30 na `fw01`, DHCP przez przekaźnik do `dc01` i `dc02`) i jedną serwerownię z dwoma hostami `hv01` i `hv02`. Parę FortiGate opisuje Para FortiGate w klastrze: FGCP aktywny-pasywny, a drugie łącze ze Starlinkiem Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate, jako wariant przyszły.

Skróty użyte na tej stronie (19)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

Skrót	Co znaczy
AI	Artificial Intelligence: sztuczna inteligencja, czyli programy naśladujące ludzkie rozumowanie
DFS	Distributed File System: usługa łącząca udziały z wielu serwerów pod jedną wspólną ścieżką sieciową
DHCP	Dynamic Host Configuration Protocol: usługa, która sama rozdaje komputerom adresy IP
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
etcd	etc distributed: rozproszony magazyn par klucz-wartość, w którym Kubernetes trzyma cały stan klastra, a zmiany uzgadnia protokołem Raft
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
HA	High Availability: wysoka dostępność, czyli działanie mimo awarii jednego elementu
HAProxy	High Availability Proxy: program, który rozdziela połączenia między kilka serwerów i omija te, które nie odpowiadają
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
RAC	Real Application Clusters: klaster Oracle, kilka serwerów na jedną bazę
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
S2D	Storage Spaces Direct: programowa macierz Windows Server z dysków wielu serwerów
SMB	Server Message Block: protokół udostępniania plików i drukarek w sieci Windows, na nim stoi zwykły udział sieciowy
SPOF	Single Point of Failure: element, którego awaria zatrzymuje całą usługę, bo nie ma dla niego zamiennika
UPS	Uninterruptible Power Supply: zasilacz awaryjny, podtrzymuje zasilanie urządzeń na czas zaniku napięcia z sieci
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
ZooKeeper	Apache ZooKeeper: osobny program, który w klastrze trzyma wspólną konfigurację i pilnuje, kto jest kim

Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Piątek, 16:05. Pan Zbigniew staje w drzwiach pokoju administratorów i pyta, które usługi mają drugi serwer, bo w poniedziałek chce to powiedzieć zarządowi. Tomek wymienia z pamięci kontrolery domeny, DHCP i Giteę, a Ola go poprawia: Gitea ma kopię, ale jej baza

> leży na `pg01`, a `pg01` jest jeden. Na tablicy powstaje pierwsza tabela z kolumnami „usługa”, „serwer”, „dziś” i „docelowo”, a przy `pg01` Tomek dopisuje pytanie, kto właściwie jest właścicielem tej bazy.

Tablica z piątku jest zalążkiem tej strony. Macierz niczego nie obiecuje firmie, bo zawiera propozycje do zatwierdzenia przez właścicieli usług. Mówi natomiast uczciwie, co mamy dziś, czego nie wiemy i w jakiej kolejności warto to poprawiać.

Jak czytać macierz

> **Pojęcie: macierz wysokiej dostępności.** Tabela, w której każdy wiersz opisuje jedną usługę: kto jest jej właścicielem, ile przerwy i ile utraconych danych firma zniesie, jaki poziom rezerwy usługa ma dziś i jaki proponujemy na przyszłość. Pozwala jednym spojrzeniem porównać usługi i zobaczyć, gdzie zabezpieczenie jest najcieńsze.

> **Pojęcie: właściciel usługi.** Osoba w firmie, która wie, ile kosztuje przerwa w usłudze, i zatwierdza dla niej RTO i RPO. Nie musi umieć jej administrować, bo administrujemy my, a właściciel mówi, co jest dla niego ważne.

> **Pojęcie: świadek kworum.** Dodatkowy głos w klastrze, który nie uruchamia usług, tylko rozstrzyga, kto ma większość, gdy dwa węzły przestają się widzieć. Może to być udział plikowy SMB poza klastrem albo konto magazynu w chmurze Azure (Cloud Witness) [1]. W MongoDB podobną rolę pełni arbiter, czyli proces, który głosuje, ale nie trzyma danych [8].

Pojęcia RTO (ile wolno nie działać), RPO (ile danych wolno stracić), zimnej, ciepłej i gorącej rezerwy tłumaczy strona Wysoka dostępność: pojęcia, liczenie dostępności i poziomy rezerwy. Tu zakładamy, że czytelnik je zna, i pokazujemy tylko, jak wpisują się w tabelę.

> Jak czytać kolumny macierzy: 1. RTO / RPO: to propozycje do zatwierdzenia przez właściciela usługi. Wpisujemy je po to, żeby rozmowa miała punkt wyjścia, a nie po to, żeby kogokolwiek zobowiązywać. Prawdziwe liczby poznajemy z testu przełączenia. 2. Dziś: zimna, ciepła, gorąca rezerwa albo brak, liczone dla usługi, a nie dla maszyny. Restart maszyny wirtualnej w klastrze Hyper-V chroni przed awarią sprzętu, ale nie przed uszkodzonym systemem wewnątrz maszyny, więc nie liczymy go jako poziomu usługi. 3. Mechanizm dziś: co baza wiedzy opisuje jako działające. Replik, drugich hostów i klastrów, które baza opisuje tylko jako scenkę albo procedurę (`pg02`, `my02`, `hana02`, `docker02`), nie liczymy jako istniejących. 4. Docelowo i mechanizm docelowy: poziom, który proponujemy.

> Nie każda usługa musi dążyć do gorącej rezerwy, bo dla usług, które mogą poczekać, uczciwą odpowiedzią jest zimna rezerwa z przetestowanym odtworzeniem. 5. Strona: odnośnik do istniejącej strony z opisem. Strony, które powstają równolegle, podajemy nazwą pliku w tekście, bez odnośnika.

Macierz usług

Wiersze podzieliliśmy na sześć grup, żeby tabele dało się czytać na ekranie. Wszystkie mają te same kolumny, a wpisy „my” w kolumnie właściciela oznaczają zespół IT. Właścicieli przypisaliśmy według ról z Świat przykładów: Zielona, co jest naszym założeniem do potwierdzenia, a nie ustaleniem.

Fundament: prąd, chłód, zapora, klaster

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona
Zasilanie	UPS 20 kVA, szafa baterii	my	RTO 0 przy zaniku do 15 min, potem łagodne wyłączenie / RPO 0	brak	jeden UPS online, tory A i B z tego samego UPS, baterie sześciolet nie dają około 8 minut, NUT na `bkp01` wyłącza serwerownię po 3 minutach na baterii	gorąca	nowe baterie i drugi komplet (etap 1), drugi UPS albo agregat z SZR (etap 3)	UPS, monitoring i wyłączanie
Chłodzenie	klimatyzacje A i B po 15 kW	my	RTO 0 przy awarii jednej jednostki / RPO nie dotyczy	gorąca	układ N+1, obie pracują razem, zasilane poza UPS, alarm zbiorczy do `wej01` i Zabbixa	gorąca	wyzwalacz wyłączania od temperatury wlotu (etap 1), zasilanie z agregatu przez SZR (etap 3)	planowanie chłodzenia

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona
Zapora, VPN i brama internetowa	`fw01` (FortiGate 100F)	my, koszt decyduje pan Zbigniew	RTO 15 min / RPO 0	brak	jedna sztuka, kopia konfiguracji do potwierdzenia	gorąca	druga sztuka w parze HA, tryb aktywny-pasywny (FGCP), licencje na obie sztuki [6] (etap 3)	sieć: opowieść
Klaster Hyper-V i S2D	`hv01`, `hv02`	my	RTO 15 min (restart maszyn na drugim węźle) / RPO 0 dla awarii węzła	gorąca	Failover Cluster z S2D (lustro dwukierunkowe), migracja na żywo przy pracach planowych, świadka kworum nie znaleźliśmy w żadnej stronie	gorąca	świadek poza klastrem (udział SMB na `bkp01` albo Cloud Witness) [1][2], wolne miejsce w puli, reguły rozmieszczenia maszyn (etapy 1 i 2)	Hyper-V na co dzień, S2D

Tożsamość i usługi Windows

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona

Active Directory	`dc01`, `dc02`	my	RTO 5 min / RPO 0	gorąca	replikacja wielomasterowa, klienci mają oba kontrolery	gorąca	bez zmian, kontrolery na różnych węzłach klastra (reguła rozmieszczenia), awaryjne konto lokalne w sejfie	AD od zera
DNS	`dc01`, `dc02`	my	RTO 5 min / RPO 0	gorąca	strefa zintegrowana z AD, każdy komputer ma oba serwery DNS	gorąca	bez zmian	DNS w domenie
DHCP	`dc01`, `dc02`	my, Marek (skanery)	RTO 5 min / RPO 0	gorąca	przełączanie awaryjne DHCP w trybie równoważenia po połowie	gorąca	bez zmian	DHCP

Serwer plików	`fs01`	pani Halina i kierownicy działów	RTO 4 h / RPO 24 h	zimna	restart w klastrze i nocna kopia restic do repozytorium `pliki` na `bkp01` według strony Kopia fs01: restic z migawką VSS do repozytorium pliki i test odtworzenia pliku oraz całego udziału	ciepła	drugi serwer plików z DFS Namespaces i replikacją DFS, wariant gorący jako rola klastra opisuje Klaster Windows dla własnych usług: rola, zasób, zależności, kworum i testy przełączenia	udziały i NTFS
Zdalne pulpity	`rds01`	Kasia (handlowcy)	RTO 8 h / RPO 24 h	zimna	kopia maszyny, aplikacje RemoteApp odtwarzamy z opisu kolekcji	zimna	bez zmian, z przetestowanym odtworzeniem, drugi host sesji tylko jeśli handlowcy uznają 8 godzin za zbyt długo	RemoteApps
Aktualizacje Windows	`wsus01`	my	RTO 3 dni robocze / RPO nie dotyczy	zimna	kopia maszyny i bazy SUSDB	zimna	bez zmian, bo stacje działają bez nowych poprawek	WSUS

Bazy danych

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona
Optima (`CDN_Zielona`)	`sql01`	pani Halina	RTO 30 min / RPO 5 min	zimna	backup pełny, różnicowy i logu przez SQL Agent, restart maszyny w klastrze	gorąca	etap pośredni: log shipping do drugiej instancji (ciepła), docelowo grupa dostępności Always On (sql01 stoi na edycji Enterprise), zgodność Optimy sprawdzamy z dostawcą [7]	log shipping, backup
WMS (`WMSPRD`)	`ora01`, fizyczny, poza klastrem	Marek	RTO 30 min / RPO 5 min	zimna	RMAN i archiwalne logi, brak drugiego serwera	ciepła	standby prowadzony skryptem na drugim serwerze Oracle (nazwa do ustalenia): Data Guard wymaga Enterprise Edition, a przykłady w bazie pokazują Standard Edition 2 [4], więc sprawdzamy licencję	RMAN, migracja bazy

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona
PostgreSQL 16 (Gitea, Zabbix, NetBox, TeamCity, aplikacje Oli)	`pg01`	Ola	RTO 15 min / RPO 1 min	zimna	pgBackRest i archiwum WAL	gorąca	etap 2: replika strumieniowa i ręczny awans (ciepła), etap 3: automatyczny awans (Patroni z magazynem uzgadniania na trzech węzłach [9], adres wirtualny z wd3-01-keepalived-i-haproxy.md)	replikacja strumieniowa, pgBackRest
Sklep B2B (`sklep_b2b`)	`my01`	Kasia	RTO 1 h / RPO 5 min	zimna	binlog i kopie bazy	ciepła	replika z GTID i ręczny awans	replikacja MySQL i MariaDB
Katalog produktów (`katalog`)	`mongo01`	Kasia	RTO 15 min / RPO 1 min	ciepła	zestaw replik z dwoma węzłami (`mongo01`, `mongo02` w przykładach), dwa głosy nie wystarczą do wyboru nowego głównego po awarii jednego [8]	gorąca	trzeci głos: arbiter na `bkp01` albo trzeci węzeł danych, z ustawieniem domyślnego write concern [8] (etap 1)	architektura MongoDB

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona
Telemetria (`telemetria`)	`cass01` do `cass03`	Marek	RTO 0 przy awarii jednego węzła / RPO 0	gorąca	współczynnik replikacji 3, poziom QUORUM wymaga dwóch z trzech węzłów	gorąca	rozkład węzłów na hostach i poziom spójności dobrany do wartości danych (etap 1)	architektura Cassandry
Archiwum płacowe (`PLACE_ARCH`)	`syb01`	pani Halina	RTO 5 dni / RPO nie dotyczy (tylko odczyt)	zimna	zrzuty bazy i kopia pliku licencji SySAM	zimna	bez zmian, ze stałym adresem MAC maszyny, bo licencja jest z nim związana	backup i restore, licencje SySAM
Pilotaż SAP (SID `ZHP`)	`hana01`, fizyczny, poza klastrem	pan Zbigniew	RTO 1 dzień / RPO 24 h	zimna	kopia bazy (do potwierdzenia)	zimna	zimna do decyzji o produkcji, potem replikacja systemowa HSR do drugiego serwera	replikacja systemowa HANA

Aplikacje na `docker01`

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona

Reverse proxy (Traefik)	`docker01`	my	RTO 5 min / RPO 15 min	zimna	restic o 02:30 na `bkp01`	ciepła	`docker02`, adres wirtualny `10.20.10.46`, rsync co 15 minut	Przenoszenie kontenerów z docker01 na docker02: zimna i ciepła rezerwa, przełączenie, Traefik
Gitea	`docker01` i baza na `pg01`	Ola	RTO 15 min / RPO 15 min	zimna	zrzut Gitea i `pg_dump`, restic	ciepła	`docker02` z plikami, baza zależy od `pg01`, więc poziom usługi nie przekroczy poziomu `pg01`	kopia Gitea, Przenoszenie kontenerów z docker01 na docker02: zimna i ciepła rezerwa, przełączenie
Vaultwarden	`docker01`	pan Zbigniew, administruje Tomek	RTO 15 min / RPO 15 min	zimna	kopia katalogu z bazą SQLite, restic	ciepła	`docker02`, synchronizacja z krótką pauzą stosu, kopia haseł krytycznych poza Vaultwardenem	kopia Vaultwardena, Przenoszenie kontenerów z docker01 na docker02: zimna i ciepła rezerwa, przełączenie

Poczta (MailCow)	`docker01`	pan Zbigniew	RTO 1 h / RPO 4 h	zimna	kopia nocna rsync na `bkp01`	ciepła	skrypt zimnego standby z dokumentacji MailCow (mariabackup i rsync) na `docker02`, nadawcy ponawiają dostarczanie podczas przerwy	kopia MailCow
NetBox	`docker01`	Tomek	RTO 1 dzień / RPO 24 h	zimna	zrzut bazy i pliki, restic	zimna	bez zmian, baza w wariancie produkcyjnym na `pg01`	NetBox: LDAP i kopia
Graylog	`docker01`, docelowo `log01`	my	RTO 1 dzień / RPO 24 h	zimna	`mongodump` i migawki, kopia na `bkp01`	zimna	bez zmian, po przeprowadzce na `log01`, logi z okna awarii możemy stracić	kopia Graylog, przeprowadzka na log01
Czat AI (Open WebUI)	`docker01`, modele na `gpu01`	pan Zbigniew (pilotaż)	RTO 3 dni / RPO 24 h	zimna	katalog danych w kopii, `gpu01` bez rezerwy	zimna	bez zmian, modele pobieramy ponownie, karty zapasowej nie kupujemy	modele lokalne

Pozostałe serwery linuksowe

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona

Aplikacje Java zespołu	`app01`	Ola	RTO 4 h / RPO 24 h	zimna	kopia maszyny i plików, baza na `pg01`	ciepła	druga instancja za HAProxy, jeśli aplikacje są bezstanowe (sprawdzamy z Olą), opisuje ją Równoważenie i adres wirtualny: keepalived i HAProxy na parze lb01 i lb02	ta strona
Budowanie (Jenkins i TeamCity)	`ci01`	Ola	RTO 1 dzień roboczy / RPO 24 h	zimna	nocna kopia `JENKINS_HOME`, baza TeamCity na `pg01`	zimna	bez zmian, kolejka budowań może poczekać	Jenkins: utrzymanie, TeamCity: kopia
Monitoring (Zabbix)	`mon01`, baza na `pg01`	my	RTO 4 h / RPO 24 h	zimna	kopia maszyny, `wej01` wysyła własny SMS przy czterech zdarzeniach fizycznych	zimna	niezależny alarm „mon01 milczy” z `bkp01` (etap 1), klaster HA Zabbixa z dwoma węzłami serwera tylko, gdy `pg01` będzie miał rezerwę [10]	Zabbix: utrzymanie, mapa czujników

Tożsamość linuksów (FreeIPA)	`ipa01`	my	RTO 4 h / RPO 24 h	zimna	`ipa-backup`	gorąca	replika `ipa02` w układzie wielomasterowym, gdy liczba serwerów linuksowych to uzasadni	instalacja serwera FreeIPA
Home Assistant	`ha01`	Tomek	RTO 1 dzień / RPO 24 h	zimna	kopia z Home Assistanta na udział `bkp01`	zimna	bez zmian, bo projekt nie ma trybu klastrowego [11]	kopia, aktualizacja i dostęp zdalny
Kopie zapasowe i NUT	`bkp01`, fizyczny, szafa R3	my	RTO 1 dzień / RPO nie dotyczy	brak	jedno miejsce kopii, ten sam serwer wyłącza serwerownię przez NUT	zimna	druga kopia poza `bkp01` i poza serwerownią (Swarzędz albo magazyn S3), etap 2	kopia całego docker01, S3

Usługi planowane i laboratorium

Usługa	Serwer	Właściciel	RTO / RPO (propozycja)	Dziś	Mechanizm dziś	Docelowo	Mechanizm docelowy	Strona

Perforce (P4 Server)	`p4d01` (VM, rola klastra Hyper-V)	zespół aplikacji i dział grafiki (właściciel do ustalenia)	założenie: RTO 15 min / RPO 15 min	brak	jeden serwer Windows, kopia do ustalenia	ciepła	VM jako rola klastra (planowe wyłączenie hosta niewidoczne dzięki migracji na żywo), nocny checkpoint i restic na `bkp01`, opcjonalnie standby `p4d02` (.85) z `p4 failover` (osobna licencja); porównanie dróg: Perforce i Lore: porównanie dróg do wysokiej dostępności na Windowsie	Perforce i Lore w klastrze: cztery drogi, rekomendacja dla Zielonej i test przełączenia
Lore	`lore01` (VM, rola klastra Hyper-V)	zespół aplikacji i dział grafiki (właściciel do ustalenia)	założenie: RTO 1 h / RPO 24 h	brak	jeden serwer Windows, kopia do ustalenia	zimna	VM jako rola klastra i kopia na `bkp01`; replikacji aplikacji Lore (przed wersją 1.0) nie ma w dokumentacji	Perforce i Lore w klastrze: cztery drogi, rekomendacja dla Zielonej i test przełączenia

Laboratorium Kubernetesa	`k3s01`	Ola	RTO 1 dzień / RPO 24 h	brak	jeden węzeł, próby przed produkcją	zimna	trzy węzły k3s dopiero wtedy, gdy pojawi się aplikacja produkcyjna, opisuje je k3s z trzema węzłami serwerowymi: etcd, adres wirtualny API i Longhorn	k3s: kolorowy Nginx

Trzy strony księgi nie mają w macierzy własnych wierszy, bo opisują mechanizmy, a nie usługi: keepalived i HAProxy (wd3-01-keepalived-i-haproxy.md), Docker Swarm (wd3-02-docker-swarm.md) i Pacemaker dla własnych usług na Linuksie (wd2-03-pacemaker-linux-wlasne-uslugi.md). Wracają w kolumnie „mechanizm docelowy” tam, gdzie je potrzebujemy, a Swarm nie jest naszym wyborem dla `docker01` i `docker02`.

Ile usług na jakim poziomie

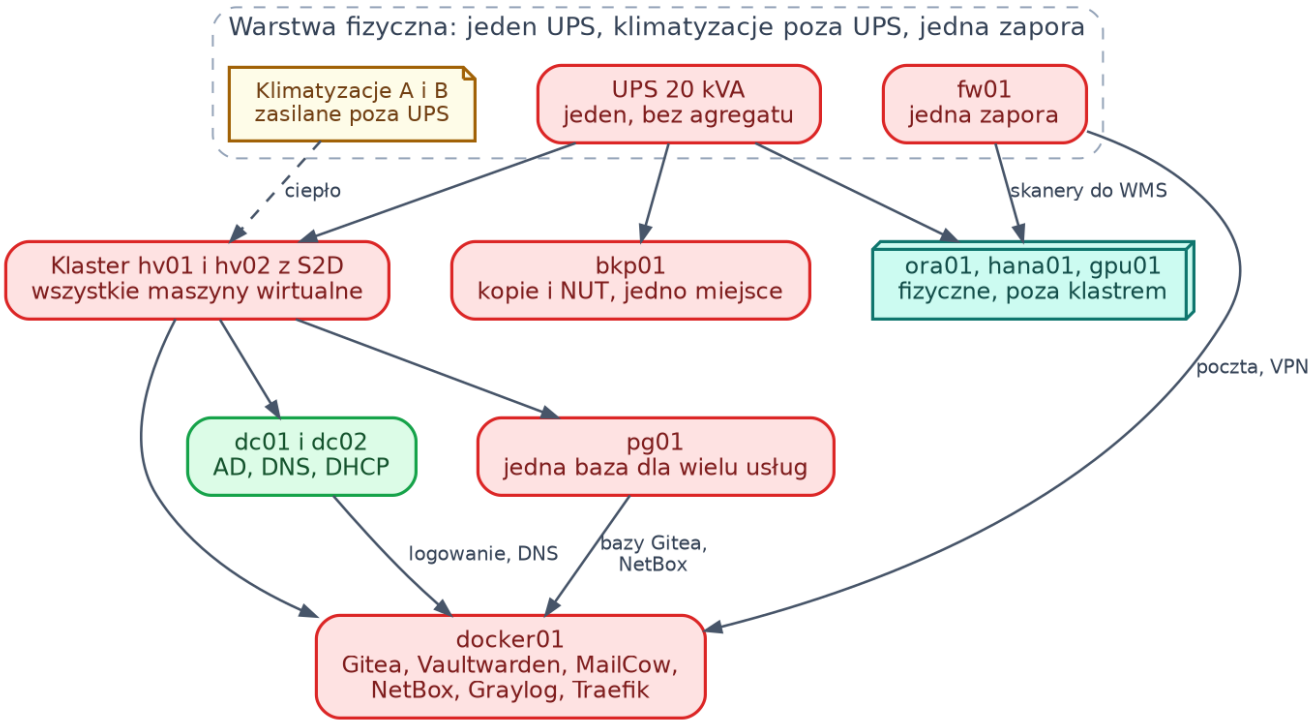
Poniższa tabela liczy wiersze macierzy (33 usługi) według słowa na początku kolumn „dziś” i „docelowo”. AD, DNS i DHCP liczymy jako trzy osobne wiersze, bo mają różne mechanizmy.

Poziom	Dziś	Docelowo
brak	5	0
zimna	21	12
ciepła	1	8
gorąca	6	13

Największa zmiana dotyczy poziomu ciepłego: dziś ma go jedna usługa (MongoDB), a po etapie 2 dostaną go cztery aplikacje z `docker01`, `fs01`, `ora01`, `my01` i `app01`. Gorącą rezerwę dziś mają dwa kontrolery domeny z DNS i DHCP, klaster Hyper-V, Cassandra i chłodzenie. Liczby policzyliśmy z tabel wyżej i po każdej zmianie macierzy trzeba je przeliczyć.

Zależności: co pada razem z czym

Usługa nie działa sama, tylko na ciągu elementów: prądzie, chłodzie, klastrze, domenie, bazie i sieci. Poziom usługi wpisany w macierz mówi o jej własnej rezerwie, ale w dniu awarii liczy się cały ciąg. Dlatego obok macierzy potrzebujemy mapy zależności.



UPS, a `docker01` zależy od klastra, domeny, `pg01` i zapory `fw01`. Czerwone ramki to elementy bez rezerwy.">

Rysunek 1. Zależności w Zielonej. Z jednego UPS zasilane są klaster `hv01` i `hv02`, `bkp01` oraz serwery fizyczne, klimatyzacje stoją poza UPS, a `docker01` zależy od klastra, domeny, `pg01` i zapory `fw01`. Czerwone ramki to elementy bez rezerwy. (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: zależność.** Element, bez którego usługa nie działa, choć sama jest zdrowa. Gitea działa tylko wtedy, gdy działa jej baza, domena, z której loguje się zespół, i maszyna, na której stoi.

Reguła najsłabszego ogniwa

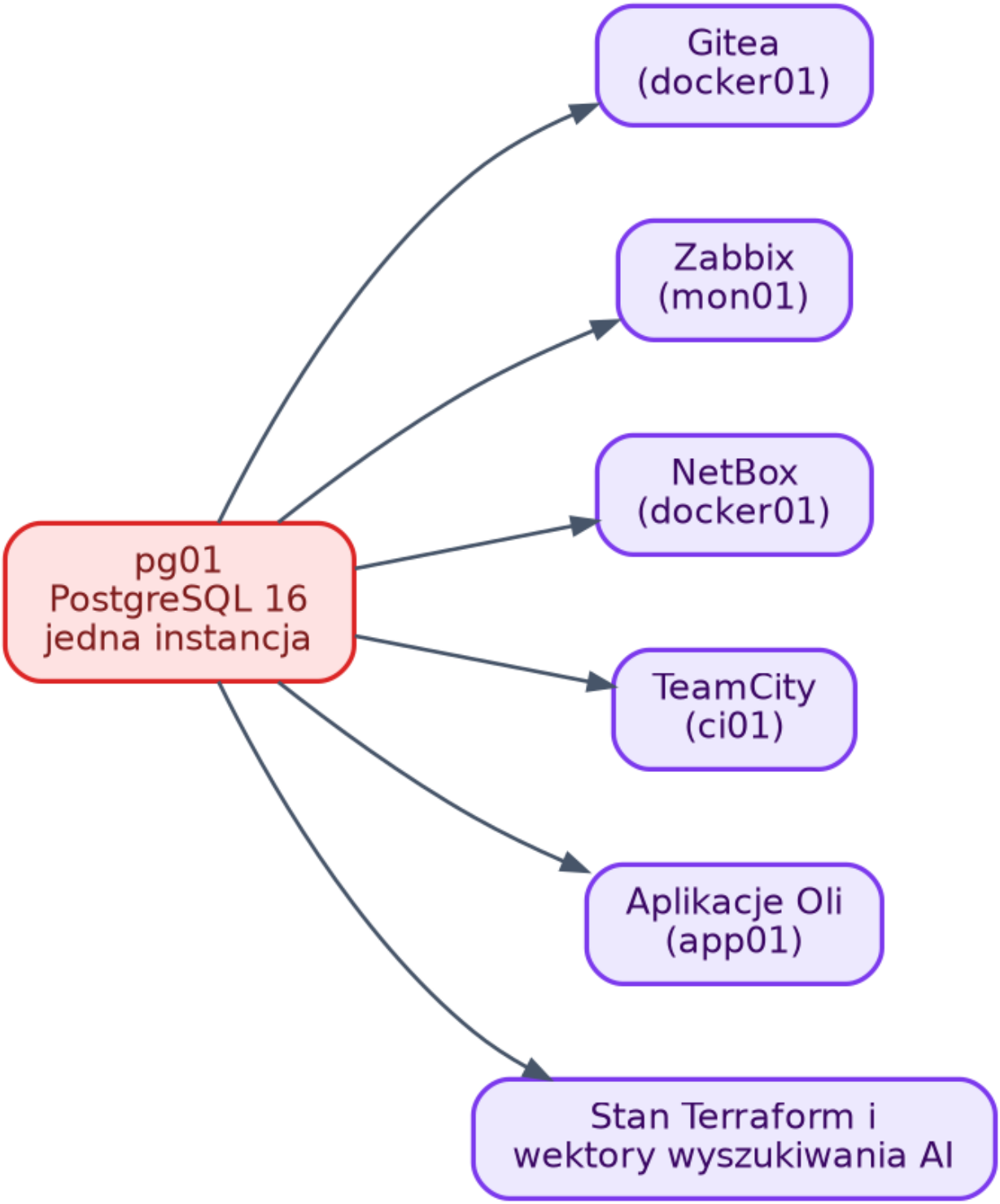
Usługa nie jest bardziej dostępna niż jej najsłabsza zależność. Gdy usługa potrzebuje kilku elementów naraz, ich dostępności mnożymy, więc wynik jest niższy od każdego z nich. To ta sama reguła, którą liczyliśmy na stronie o poziomach rezerwy.

Przykład z założonymi wartościami, a nie z pomiaru: Gitea na `docker01` (99,9 procent), baza na `pg01` (99,5 procent), domena (99,99 procent) i klaster Hyper-V (99,9 procent) dają razem około 99,29 procent, czyli około 62 godziny przestoju w roku. Najwięcej zabiera `pg01`, więc dokładanie drugiego hosta pod Giteę pomaga najmniej ze wszystkich możliwych prac.

Co pada razem z czym

Gdy pada	Przestaje działać	Uwaga
zasilanie (UPS)	wszystko po około 8 minutach na starych bateriach	NUT na `bkp01` wyłącza serwerownię po 3 minutach, ale `bkp01` też stoi na tym UPS
obie klimatyzacje	cała serwerownia, bo wlot dochodzi do 32 °C po 5 do 10 minutach od ich zatrzymania (szacunek)	klimatyzacje są poza UPS, więc zanik prądu zatrzymuje je od razu
klaster `hv01` i `hv02` (kworum albo pula S2D)	wszystkie maszyny wirtualne: `dc01`, `dc02`, `pg01`, `docker01`, `sql01`, `mon01`, `ha01` i reszta	zostają serwery fizyczne `ora01`, `hana01`, `gpu01`, `bkp01` i zapora `fw01`
`dc01` i `dc02` jednocześnie	logowanie do Gitea, Zabbixa, Graylog, MailCow, Vaultwardena, TeamCity, Jenkinsa i NetBoksa, nazwy wewnętrzne, DHCP	oba kontrolery stoją na tym samym klastrze, więc to nie są dwa niezależne elementy
`dc01` (sama)	kolektor FSSO na zaporze, czyli grupy z AD w regułach VPN; wydawanie i odnawianie certyfikatów z `CA-Zielona`	kolektor działa tylko na `dc01`; urząd AD CS stoi dziś na `dc01`, a docelowo na osobnym serwerze `ca01` według strony Projekt PKI Zielonej: dlaczego nie na kontrolerze, hierarchia dwupoziomowa, nazwy, ważność, CRL i AIA; NPS dla Wi-Fi i VPN stoi na `dc02`
`pg01`	Gitea, Zabbix, NetBox, TeamCity, aplikacje Oli, stan Terraform i wektory wyszukiwania AI	patrz rysunek 2, to najgroźniejsza zależność warstwy danych
`docker01`	Traefik, Gitea, Vaultwarden, MailCow, NetBox, Graylog, Open WebUI	Vaultwarden i `docker01` trzymają też hasła do własnych kopii
MailCow	zaproszenia, reset haseł i powiadomienia z Vaultwardena	Vaultwarden wysyła pocztę przez MailCow
`fw01`	internet, VPN handlowców, przekierowania poczty, przekaźnik DHCP dla skanerów z VLAN 30	jedna sztuka, jedno łącze z jednym adresem publicznym `203.0.113.10`
`bkp01`	kopie zapasowe, NUT, udział z kopiami Home Assistanta	jeden serwer, jedna szafa R3

Wynika z tego, że rezerwa ma sens tylko tam, gdzie zależności pod spodem są równie dobre. Dla Gitea najpierw `pg01`, dopiero potem `docker02`.



AI. Jedna instancja bazy trzyma kilka niezależnych zespołów.">

Rysunek 2. Co pada razem z `pg01`: Gitea, Zabbix, NetBox, TeamCity, aplikacje Oli, stan Terraform i wektory wyszukiwania AI. Jedna instancja bazy trzyma kilka niezależnych zespołów. (kliknięcie otwiera pełny rozmiar)

Pojedyncze punkty awarii i kolejność prac

> **Pojęcie: pojedynczy punkt awarii (SPOF).** Element, którego awaria zatrzymuje usługę, bo nie ma dla niego zamiennika: serwer, ale też UPS, zapora albo człowiek, który jako jedyny zna procedurę.

Poniższa lista porządkuje pojedyncze punkty awarii (SPOF) według priorytetu pracy: najpierw wysokie ryzyko i niski koszt usunięcia, na końcu wysokie ryzyko i wysoki koszt. Dlatego zapora `fw01` i `ora01` mają wysokie ryzyko, ale stoją niżej niż świadek klastra, który kosztuje kilka godzin pracy.

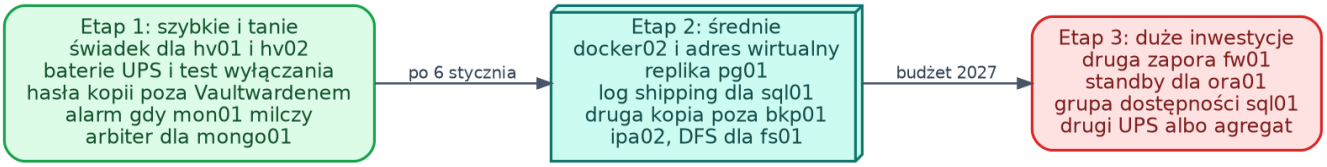
Lp.	Pojedynczy punkt awarii	Co zatrzymuje	Ryzyko	Koszt usunięcia	Etap	Jak usuwamy
1	klaster `hv01` i `hv02` bez świadka (do sprawdzenia)	wszystkie maszyny wirtualne	wysokie	niski	1	świadek: udział SMB na `bkp01` albo Cloud Witness, test wyłączenia jednego węzła
2	baterie UPS sześcioletnie, wyłączanie tylko od baterii	cała serwerownia	wysokie	niski do średni	1	nowe baterie i drugi komplet, wyzwalacz wyłączania od temperatury wlotu, próba ze stoperem
3	kopie tylko na `bkp01`, hasło repozytorium restic tylko w Vaultwardenie na `docker01`	możliwość odtworzenia czegokolwiek	wysokie	niski (hasło), średni (druga kopia)	1 i 2	kopia haseł krytycznych poza `docker01`, potem druga kopia poza `bkp01` i poza serwerownią

Lp.	Pojedynczy punkt awarii	Co zatrzymuje	Ryzyko	Koszt usunięcia	Etap	Jak usuwamy
4	pula S2D prawie pełna (według przykładu z książki o S2D niecałe 0,05 terabajta wolnego)	odbudowa po awarii dysku, czyli bezpieczeństwo danych całego klastra	wysokie	średni	2	odzysk miejsca (punkty kontrolne, zbędne maszyny), potem dyski
5	`pg01` jako jedyna baza dla wielu usług	Gitea, Zabbix, NetBox, TeamCity, aplikacje Oli	wysokie	średni	2, potem 3	replika i ręczny awans, później automat
6	`docker01` jako jedyna maszyna dockerowa	Traefik, Gitea, Vaultwarden, MailCow, NetBox, Graylog	wysokie	średni	2	`docker02`, adres wirtualny i rsync co 15 minut
7	`sql01` bez repliki	Optima, szczególnie w zamknięciu miesiąca	wysokie	średni do wysoki	2, potem 3	log shipping, potem grupa dostępności
8	`ora01` fizyczny, bez drugiego serwera	WMS, start zmiany o 6:00	wysokie	wysoki	3	standby prowadzony skryptem albo Standard Edition High Availability [4][5], decyzja licencyjna
9	`fw01` jedna zapora i jedno łącze	internet, VPN, poczta, DHCP dla skanerów	wysokie	wysoki	3	druga zapora w parze HA [6], drugie łącze do rozważenia
10	jeden UPS i brak agregatu	cała serwerownia przy dłuższym zaniku	wysokie	wysoki	3	drugi UPS albo agregat z SZR
11	`mon01` milczy razem z klastrem	alarmy, jeśli nie ma niezależnego kanału	średnie	niski	1	sprawdzanie `mon01` z `bkp01` i SMS przez ten sam kanał co `wej01`

Lp.	Pojedynczy punkt awarii	Co zatrzymuje	Ryzyko	Koszt usunięcia	Etap	Jak usuwamy
12	`mongo01` i `mongo02` jako dwa głosy	automatyczny wybór głównego po awarii jednego węzła [8]	średnie	niski	1	arbiter albo trzeci węzeł
13	trzy węzły Cassandry na dwóch hostach	operacje na poziomie QUORUM po awarii hosta z dwoma węzłami	średnie	niski	1	rozmieszczenie węzłów i poziom spójności dopasowany do danych
14	kolektor FSSO na `dc01`, AD CS i NPS w jednym miejscu	VPN z grupami z AD	średnie	niski do średni	2	drugi kolektor na `dc02`, jeśli FortiOS to dopuszcza (sprawdzamy w dokumentacji Fortinet), rozmieszczenie ról; urząd AD CS docelowo na `ca01` (strona o projekcie PKI)
15	dwóch administratorów, jeden w drugim tygodniu pracy	każde przełączenie wykonywane ręcznie	średnie	niski	1	instrukcje na stronach usług, przełączenie wykonane z udziałem Tomka
16	przełączniki, okablowanie i łącze internetowe	do inwentaryzacji w NetBoksie	do oceny	niski	2	spis, czy każdy host ma dwa łącza do dwóch przełączników

Trzy etapy prac

Etapy wynikają z kosztu i z kalendarza. Etap 1 mieści się w czasie roboczym i w budżecie, który nie wymaga uchwały zarządu. Etap 2 wymaga nowych maszyn i trochę nowego sprzętu, a etap 3 to zakupy, które pan Zbigniew zatwierdza osobno.



DFS. Etap 3: druga zapora, standby dla `ora01`, grupa dostępności, drugi UPS albo agregat.">

Rysunek 3. Trzy etapy prac. Etap 1: świadek klastra, baterie UPS, hasła kopii poza Vaultwardenem, alarm „mon01 milczy”, arbiter dla `mongo01`. Etap 2: `docker02`, replika `pg01`, log shipping dla `sql01`, druga kopia, `ipa02`, DFS. Etap 3: druga zapora, standby dla `ora01`, grupa dostępności, drugi UPS albo agregat. (kliknięcie otwiera pełny rozmiar)

Etap	Zakres	Kiedy	Czego pilnujemy
1. Szybkie i tanie	świadek dla `hv01` i `hv02`, nowe baterie UPS i próba wyłączania, kopia haseł poza Vaultwardenem, alarm „mon01 milczy”, arbiter dla `mongo01`, rozmieszczenie maszyn, rozmowy o RTO i RPO z właścicielami	od 5 do 27 października i od 2 do 13 listopada 2026	zakaz zmian od 15 listopada do 6 stycznia, trzy ostatnie dni robocze października (28, 29 i 30) są wyłączone
2. Średnie	`docker02` z adresem wirtualnym, replika `pg01`, log shipping dla `sql01`, replika `my01`, druga kopia poza `bkp01`, `ipa02`, DFS dla `fs01`, miejsce w puli S2D, inwentaryzacja sieci	od 7 stycznia 2027, po jednej usłudze na miesiąc	każda usługa wchodzi dopiero po zatwierdzeniu RTO i RPO przez właściciela
3. Duże inwestycje	druga zapora, standby lub SEHA dla `ora01`, grupa dostępności dla `sql01`, drugi UPS albo agregat z SZR, automatyczny awans `pg01`	budżet 2027, decyzje pana Zbigniewa	każda pozycja ma ofertę z ceną i uzasadnieniem w postaci zmierzonego RTO z testu

Świadek dla `hv01` i `hv02` stoi na pierwszym miejscu z dwóch powodów. Microsoft zaleca świadka zawsze, a dla klastra S2D z dwoma serwerami jest on potrzebny do utrzymania kworum [1][3]. Udział plikowy nie może leżeć na maszynie z tego samego klastra, więc `fs01` odpada: to maszyna wirtualna, która gaśnie razem z węzłami.

Dwa warianty świadka mają różne wady, które podajemy do decyzji autora, a nie rozstrzygamy z góry.

Wariant	Zalety	Wady

udział SMB na `bkp01` (Samba)	bez konta w chmurze, działa w sieci lokalnej, Microsoft dopuszcza urządzenia spoza domeny przy Windows Server 2019 i nowszych [2]	`bkp01` stoi na tym samym UPS i jest sam punktem awarii, w tej sesji niczego nie testowaliśmy, więc test jest obowiązkowy
Cloud Witness	niezależny od serwerowni	wymaga subskrypcji Azure, portu 443 z węzłów i działającej zapory `fw01` [1][2]

Jak testujemy

Rezerwa, której nikt nie przełączył, jest przypuszczeniem. Dlatego raz na kwartał robimy test przełączenia jednej grupy usług i porównujemy wynik z liczbami z macierzy.

Kalendarz testów

Test przełączenia wyłącza serwery produkcyjne, a na liście zmian standardowych ze strony Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć go nie ma: lista obejmuje aktualizacje Windows, dodanie do grupy z wniosku, odnowienie certyfikatu, poprawkową aktualizację obrazu kontenera i dopisanie adresu do grupy na `fw01`. Każdy test jest więc zmianą normalną z wpisem w GLPI i robimy go we wtorkowym oknie zmian od 17:00 do 20:00. W piątek od 14:00 i w weekend wolno tylko zmiany standardowe i awaryjne, więc soboty odpadają.

Kwartalny rytm psują zakazy z kalendarza Zielonej: zakaz zmian w infrastrukturze od 15 listopada do 6 stycznia (sezon przed świętami, magazyn na trzy zmiany) i ostatnie trzy dni robocze każdego miesiąca (zamknięcie miesiąca pani Haliny). Omijamy też trzeci wtorek miesiąca, bo to okno aktualizacji Windows, w którym `wsus01` rozdaje poprawki, oraz wtorki zajęte przez kwartalne testy odtwarzania ze strony Testy odtwarzania: plik, maszyna, baza i cała lokalizacja (pierwsze wtorki: 10.11.2026, 2.02, 4.05, 3.08 i 5.10.2027) i przez ćwiczenie awarii klastrów kontenerów (27.10 i 3.11.2026).

Z tych zasad wychodzi stały termin: drugi wtorek miesiąca od 17:00 do 20:00, w miesiącach luty, maj, sierpień i październik. Drugi wtorek to Patch Tuesday: serwery nie są jeszcze zaktualizowane, a do okna aktualizacji zostaje tydzień na wykrycie skutków testu. Przerwa od października do lutego wynika z zamrożenia, a październikowy test kończy czas przed sezonem.

Test tożsamości i sieci z października 2026 (dawniej sobota 17.10) nie ma wolnego wtorku przed zakazem: 6 i 13 października minęły przed przejściem z sobót, 20.10 to okno aktualizacji Windows, 27.10 i 3.11 zajmuje ćwiczenie orkiestracji, 10.11 test odtwarzania. W styczniu 2027 też nie ma miejsca: 12.01 zostawiamy na zmiany przeniesione z grudnia, 19.01 to okno aktualizacji Windows, a 26.01 to rezerwa ćwiczenia orkiestracji. Dlatego test tożsamości wchodzi na luty, a test klastra przesuwamy o miesiąc na marzec.

Termin	Zakres	Zajęte albo wyłączone w tym miesiącu
wtorek 9 lutego 2027, 17:00 do 20:00	tożsamość i sieć: wyłączenie `dc01`, potem `dc02`, obserwacja logowania, DNS i DHCP (test przeniesiony z października 2026)	2.02 test odtwarzania, 16.02 okno aktualizacji Windows, ostatnie dni robocze 24, 25 i 26 lutego
wtorek 9 marca 2027, 17:00 do 20:00	klaster: wyłączenie jednego węzła ze świadkiem	16.03 okno aktualizacji Windows, ostatnie dni robocze 29, 30 i 31 marca
wtorek 11 maja 2027, 17:00 do 20:00	`docker01` na `docker02` (planowo i awaryjnie)	4.05 test odtwarzania, 18.05 okno aktualizacji Windows, ostatnie dni robocze 27, 28 i 31 maja
wtorek 10 sierpnia 2027, 17:00 do 20:00	bazy: awans repliki `pg01`, `sql01` z log shippingu	3.08 test odtwarzania, 17.08 okno aktualizacji Windows, ostatnie dni robocze 27, 30 i 31 sierpnia
wtorek 12 października 2027, 17:00 do 20:00	powtórka tożsamości i sieci oraz wszystko, co po drodze naprawiliśmy	5.10 test odtwarzania i test lokalizacji, 19.10 okno aktualizacji Windows, ostatnie dni robocze 27, 28 i 29 października

Gdy test nie wypada w wyznaczonym terminie, przesuwamy go na następny wolny wtorek w oknie 17:00 do 20:00 (bez trzeciego wtorku, bez terminów testów odtwarzania i bez ostatnich trzech dni roboczych), ale nigdy do okresu zakazu zmian. Odtworzenia z kopii nie łączymy już z testem przełączenia: ma własny kalendarz i protokół na stronie o testach odtwarzania, a zmierzone tam czasy też trafiają do macierzy. Test całkowitego zaniku zasilania opisuje księga o zasilaniu i wykonujemy go raz w roku osobno.

Protokół testu

Każdy test przechodzi przez te same osiem kroków, a przy każdym zapisujemy wynik. Robią go dwie osoby: jedna kieruje, druga mierzy czas i zapisuje.

Krok	Kiedy	Kto	Co robimy	Co zapisujemy
1. Zapowiedź	7 dni wcześniej	my	wysyłamy właścicielowi usługi zakres, datę i godzinę okna, potwierdzamy, że nie wypada w zakazie zmian, i zakładamy zmianę normalną w GLPI	zgodę właściciela i numer zmiany
2. Stan wyjściowy	przed oknem	druga osoba	sprawdzamy wiek ostatniej kopii, wiek ostatniej synchronizacji, stan replik i wolne miejsce	zrzut stanu

Krok	Kiedy	Kto	Co robimy	Co zapisujemy
3. Awaria	początek okna	kierujący	wywołujemy awarię opisaną na stronie usługi: planowe zatrzymanie, wyłączenie maszyny w Hyper-V, nigdy wyłączenie zasilania serwerowni	godzinę zero ze stopera
4. Przełączenie	po godzinie zero	kierujący	wykonujemy procedurę ze strony usługi albo obserwujemy, czy zadziałał automat	czas decyzji i kroki, które wykonaliśmy ręcznie
5. Pomiar RTO	do pierwszej poprawnej odpowiedzi	druga osoba	mierzymy czas od godziny zero do chwili, gdy usługa odpowiada i właściciel (albo skrypt) to potwierdza	RTO zmierzone
6. Pomiar RPO	zaraz po	druga osoba i właściciel	sprawdzamy, czy ostatni zapis testowy sprzed awarii jest widoczny	RPO zmierzone
7. Powrót	po zaliczeniu	my	wracamy do stanu wyjściowego decyzją człowieka, z pilnowaniem kierunku replikacji	czas powrotu
8. Wnioski	w ciągu 3 dni roboczych	my	porównujemy zmierzone RTO i RPO z zatwierdzonymi, poprawiamy macierz i stronę usługi	wpis w macierzy z datą i wynikiem

Test uznajemy za zaliczony, gdy zmierzone RTO i RPO mieszczą się w zatwierdzonych, a całość udała się według instrukcji, bez wiedzy spoza niej. W przeciwnym razie powtarzamy test w następnym oknie po poprawce i do tego czasu nie podnosimy poziomu usługi w kolumnie „dziś”.

Co przyjęliśmy i czego nie wiemy

Poniższe założenia wpływają na wiersze macierzy. Nie znaleźliśmy ich potwierdzenia w istniejących stronach bazy, więc wymagają odpowiedzi autora.

Założenie albo pytanie	Gdzie wpływa

Klaster `hv01` i `hv02` nie ma świadka (strony o klastrze o nim milczą)	wiersz klastra, SPOF 1
Maszyny `ora01`, `hana01` i `gpu01` są fizyczne i stoją poza klastrem, tak jak opisują księgi o zasilaniu i o serwerowni	wiersze baz, SPOF 8
Edycja Oracle na `ora01` to Standard Edition 2, jak w przykładach; edycja `sql01` to Enterprise	wiersze `ora01` i `sql01`
`mongo01` ma replica set z dwoma węzłami, jak w przykładach	wiersz MongoDB, SPOF 12
Dwa węzły Cassandry stoją na jednym hoście Hyper-V	wiersz Cassandry, SPOF 13
Strony o Oracle i tożsamości opisują NetWorker z serwerem jako placeholderem `NazwaSerweraNetWorker`, bo Zielona nie ma serwera NetWorker, a reszta bazy używa `bkp01`	wiersz `bkp01`, wszystkie kopie
Poza oczywistymi przypadkami (Optima, WMS, skanery) właścicieli przypisaliśmy według ról postaci, bez potwierdzenia	kolumna „właściciel”
Perforce i Lore to usługi planowane w klastrze, a ich właściciela i wymagań jeszcze nie znamy	wiersze planowane
Zielona ma jedno łącze z jednym adresem publicznym, jak sugeruje lista adresów	wiersz `fw01`, SPOF 9 i 16

Częste błędy

Objaw	Przyczyna	Co robimy
macierz mówi „gorąca”, a w teście usługa stoi godzinę	zależność o niższym poziomie, na przykład jedna baza `pg01`	liczymy najsłabsze ogniwo i poprawiamy kolumnę „dziś”
dwa kontrolery domeny, a po awarii klastra nikt się nie loguje	oba stoją na tym samym klastrze i tej samej puli S2D	traktujemy je jako jedną zależność od klastra, kontroler poza klastrem planujemy w etapie 3
RTO w macierzy bez nazwiska właściciela	liczba wzięta z głowy zespołu IT	zapisujemy, kto i kiedy zatwierdził, a do tego czasu zostaje „propozycja”
świadek klastra na `fs01` albo innej maszynie z klastra	świadek gaśnie razem z węzłami	świadek poza klastrem: `bkp01` albo chmura
rezerwa „gorąca”, bo są dwa serwery, ale bez kworum	dwa węzły nie wybiorą głównego po awarii jednego	trzeci głos: świadek, arbiter albo trzeci węzeł
test przełączenia w ostatnich dniach miesiąca albo przed świętami	brak kalendarza, zamknięcie miesiąca u pani Haliny	kalendarz z zakazami, terminy z góry
replika zamiast kopii	skasowanie danych dociera do repliki w sekundy	kopia restic, RMAN albo pgBackRest zostaje na każdym poziomie

Objaw	Przyczyna	Co robimy
zmiana poziomu w macierzy bez testu	wpis „ciepła”, bo drugi host istnieje	poziom zmieniamy dopiero po zaliczonym teście

Ćwiczenia

1. Gitea ma ciepłą rezerwę na `docker02`, ale baza leży na `pg01` z zimną rezerwą. Jaki poziom wpisujemy w macierzy dla usługi Gitea?

Odpowiedź

Zimną, bo poziom usługi nie przekracza poziomu jej najsłabszej zależności. Dopiero replika `pg01` z ręcznym awansem podniesie Giteę do ciepłej.

1. Dlaczego Active Directory ma w macierzy gorącą rezerwę, a mimo to po awarii klastra nikt się nie loguje?

Odpowiedź

`dc01` i `dc02` replikują się między sobą, ale oba są maszynami wirtualnymi na tym samym klastrze i tej samej puli S2D. Awaria klastra zabiera oba naraz, więc rezerwa chroni przed utratą jednej maszyny, a nie przed utratą warstwy pod nimi.

1. Dlaczego udział plikowy na `fs01` nie nadaje się na świadka klastra `hv01` i `hv02`?

Odpowiedź

`fs01` to maszyna wirtualna z tego klastra. Gdy klaster traci węzły albo kworum, maszyna z udziałem też przestaje działać, więc świadek znika dokładnie wtedy, gdy jest potrzebny. Świadek musi leżeć poza klastrem, na przykład na `bkp01` albo jako Cloud Witness.

1. Który termin wybieramy dla kwartalnego testu przełączenia w październiku 2027: wtorek 5, wtorek 12, sobota 16 czy wtorek 19?

Odpowiedź

Wtorek 12 października, od 17:00 do 20:00. Test przełączenia jest zmianą normalną, a w sobotę 16 października wolno tylko zmiany standardowe i awaryjne. Wtorek 5 października zajmuje

kwartalny test odtwarzania, a wtorek 19 października to trzeci wtorek miesiąca z oknem aktualizacji Windows.

1. Gitea (99,9 procent), `pg01` (99,5 procent), domena (99,99 procent) i klaster (99,9 procent) tworzą ciąg szeregowy. Ile w przybliżeniu wynosi dostępność całości i która praca poprawi ją najbardziej?

Odpowiedź

Mnożymy: 0,999 razy 0,995 razy 0,9999 razy 0,999 daje około 0,9929, czyli około 99,29 procent, co odpowiada około 62 godzinom przestoju w roku. Najbardziej poprawi wynik praca nad `pg01`, bo to najsłabszy element ciągu.

Powiązane: Wysoka dostępność: usługa, która nie ma jednego serwera · Wysoka dostępność: pojęcia, liczenie dostępności i poziomy rezerwy · Przenoszenie kontenerów z docker01 na docker02: zimna i ciepła rezerwa, przełączenie · Replikacja danych między hostami: DRBD, GlusterFS, Ceph, ZFS i replikacja w aplikacji · RPO i RTO: dwie liczby, od których zaczyna się każdy plan backupu · Zasilanie: wojna prądów, UPS i serwer, który nie może zgasnąć · Planowanie chłodzenia serwerowni: bilans, zapas N+1, awaria klimatyzacji · Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy

Źródła:

1. learn.microsoft.com: Manage the cluster quorum, typy świadka i wymagania udziału plikowego
2. learn.microsoft.com: Deploy a quorum witness, wymagania Cloud Witness (subskrypcja Azure, port 443) i udziału plikowego (Windows Server 2019 i nowszy dla urządzeń spoza domeny)
3. learn.microsoft.com: Storage Spaces Direct overview, dwa serwery i świadek, lustro dwukierunkowe
4. docs.oracle.com: Database Licensing Information User Manual 19c, tabele z Data Guard, RAC i Standard Edition High Availability dla edycji Standard Edition 2 i Enterprise Edition
5. docs.oracle.com: About Standard Edition High Availability, wymagania (Grid Infrastructure, wspólny magazyn, co najmniej dwa węzły)
6. community.fortinet.com: Technical Tip: The HA Cluster license requirements, licencje dla członków klastra HA i współdzielona licencja FortiGuard w 100F od FortiOS 7.2.9
7. learn.microsoft.com: Basic availability groups, ograniczenia grup podstawowych (Standard) wobec pełnych (Enterprise)
8. mongodb.com: Replica Set Deployment Architectures, nieparzysta liczba głosów, arbiter

9. patroni.readthedocs.io: Patroni, wymóg magazynu uzgadniania (etcd, Consul, ZooKeeper) i automatyczny awans
10. blog.zabbix.com: Handy Tips #24: Preventing downtimes with the Zabbix HA cluster, dwa lub więcej węzłów serwera
11. community.home-assistant.io: WTH why is there no Active-Active or Active-Passive high availability setup?, brak klastrowania w Home Assistant
12. Ta baza wiedzy: strony wymienione w kolumnie „Strona”, księgi o zasilaniu, chłodzeniu i serwerowni oraz Świat przykładów: Zielona