Programowanie usług w chmurze komputerowej

Wykład 3

mgr inż. Jarosław Szkoła

Istotność danych

Im większa zależność firm od danych, tym wyższe koszty utraty danych i awarii systemów.

Wzrost ilości danych w tej dekadzie

- Ilość danych: 50 razy.
- Ilość plików: 75 razy.

Globalna ilość danych: 35 ZB (Zetta Bajtów)

$$1\,ZB = 10^{14}\,B$$

wg. European Disaster Recovery

Najważniejsze przyczyny utraty danych i przestojów systemów

- Awaria sprzętu.
- Awaria źródła zasilania.
- Uszkodzenie danych.

wg. European Disaster Recovery

Główne konsekwencje dla firm

- Spadek produktywności.
- Spadek przychodów.
- Opóźnienia w rozwoju produktów.

wg. European Disaster Recovery

Obawy związane z przeniesieniem podstawowych aplikacji do chmury

- Bezpieczeństwo.
- Wydajność.
- Dostępność.
- Problemy z integracją z zasobami wewnętrznymi.
- Ograniczone możliwości konfiguracji.
- Wzrost realnych kosztów wykorzystania zasobów na żądanie.

wg. IDC

Obawy związane z przeniesieniem podstawowych aplikacji do chmury

- Problemy z powrotem do zasobów wewnętrznych.
- Ograniczenia prawne.
- Niewystarczająca liczba dużych dostawców.

wg. IDC

Podstawowe narzędzia zapewniające bezpieczeństwo danych

- Szyfrowanie danych.
- Wirtualne sieci lokalne (VLAN).
- Firewalle i filtry pakietów.

Bezpieczeństwo chmury

- Za bezpieczeństwo fizyczne chmury odpowiada wyłącznie dostawca chmury.
- Za kontrolę dostępu do usług chmury odpowiadają zarówno dostawca chmury jak i jej użytkownicy.

Bezpieczeństwo największych centrów danych w chmurze

- Bezpieczeństwo fizyczne:
  - ufortyfikowane budynki pod ścisłą ochroną oraz otoczone barierami naturalnymi,
  - monitorowanie zarówno obszarów wokół budynków jaki i wstępu do budynków z wykorzystaniem nowoczesnych systemów kamer, systemów wykrywających wtargnięcia., itp.,
  - przynajmniej trzykrotny proces uwierzytelniania oparty o dwie różne cechy,
  - poziom zabezpieczeń przekraczający ten w instytucjach finansowych,

Bezpieczeństwo największych centrów danych w chmurze

- Bezpieczeństwo fizyczne (cd.):
  - zapewnienie dostępu tylko tym pracownikom, którzy mają uzasadniony powód aby go uzyskać,
  - monitorowanie wszelkich form fizycznego i elektronicznego dostępu pracowników centrów do danych.

Bezpieczeństwo największych centrów danych w chmurze

- Środki kontroli dostępu:
  - walidacja adresu posiadacza karty kredytowej,
  - weryfikacja tożsamości przez inny kanał,
  - autentykacja wieloczynnikowa (np. hasło, sprzętowo generowany token o ograniczonym czasie ważności, itp.),
  - klucze dostępowe.

Bezpieczeństwo największych centrów danych w chmurze

- Bezpieczeństwo sieciowe:
  - bezpieczeństwo systemu operacyjnego hosta,
  - bezpieczeństwo systemu operacyjnego instancji wirtualnej,
  - bezpieczeństwo firewalli,
  - bezpieczeństwo podpisanych wywołań API.

Bezpieczeństwo największych centrów danych w chmurze

- Bezpieczeństwo danych:
  - listu kontroli dostępu (ACL - Access Control Lists) definiujące prawa do odczytu i zapisu danych w przeznaczonych do tego kontenerach,
  - udostępnianie API magazynów danych w chmurze przez końcówki stosujące szyfrowanie (SSL),
  - szyfrowanie danych przed ich przesłaniem do chmury.

Dostępność, średni czas naprawy

- Wyznaczanie poziomu dostępności A (Availability):

$$A = \frac{MTBF}{MTBF + MTTR} \cdot 100\,\%$$

  - MTBF (Mean Time Between Failure) - średni czas międzyawaryjnej pracy,
  - MTTR (Mean Time To Repair) - średni czas naprawy.

Standardy i klasyfikacje

- Najbardziej rozpoznawalne standardy dla centrów danych zostały wypracowane przez następujące organizacje:
  - Uptime Institute,
  - Stowarzyszenie Przemysłu Telekomunikacyjnego (Telecommunications Industry Association, TIA)
  - American Institute of Certified Public Accountants: SSAE 16 (dawny SAS 70), ISAE 3402, SOC1 i SOC2 (Statement on Standards for Attestation Engagements no. 16)

Klasyfikacja Tier

- Najczęściej stosowaną klasyfikacją dotyczącą obiektów data center jest klasyfikacja Tier,
- Służy do określenia poziomu bezpieczeństwa (fizycznego i środowiskowego) i niezawodności infrastruktury centrum danych. Im wyższy poziom, tym bardziej niezawodne i bezpieczne data center.

Klasyfikacja Tier

- The Uptime Institute był pierwszą organizacją, która oficjalnie użyła zwrotu „tier” do klasyfikacji poziomu dostępności centrum danych,
- Instytut w roku 2001 opracował wytyczne określające za pomocą wartości procentowej minimalny poziom dostępności systemu dla każdej z klas Tier I, II, III, IV.

Klasyfikacja Tier

- Dwa dokumenty opracowane przez Uptime Institute określają kryteria dla poszczególnych klas.
  - „Industry Standard Tier Classifications Define Site Infrastructure Performance” - opisujący wytyczne konfiguracji infrastruktury technicznej,
  - „Data Center Site Infrastructure Tier Standard: Topology” – określa główne założenia dla poszczególnych klas Tier.

Klasyfikacja Tier

Tier I:

- Podstawowa infrastruktura bez redundancji, systemy podtrzymania zasilania (UPS, agregat prądotwórczy). Planowane prace utrzymaniowe wymagają wyłączenia większości lub wszystkich systemów. Całość systemu posiada wiele punktów awarii mających wpływ na dostępność systemów. Oczekiwana dostępność 99,671%.

Klasyfikacja Tier

Tier II:

- Podstawowa redundancja. Systemy zasilania posiadają redundantne komponenty pracujące równolegle w systemie n+1 oraz instalację chłodniczą pracującą w tym samym systemie. Takie rozwiązanie posiada zamienne urządzenia pozwalające na utrzymanie funkcjonalności w przypadku awarii elementów zasilających posiadających elektronikę. System tak jak poprzedni nie umożliwia wykonywania bezprzerwowych konserwacji, serwisów systemów, jak i posiada wiele punktów awarii. Uszkodzenie jednego z urządzeń nie powoduje zatrzymania pracy Data Center. Oczekiwana dostępność 99,741%.

Klasyfikacja Tier

Tier III:

- Niezależna infrastruktura. Całość infrastruktury jest redundantna. Posiada wiele aktywnych instalacji zasilających. W praktyce oznacza zasilanie układu z podstawowego źródła a zapasowego źródło służy do ewentualnych serwisów i konserwowania. Założeniem tego systemu jest utrzymanie tylko jednej linii zasilania aktywnej, druga może być uruchomiona lub uruchamiana podczas prac konserwacyjnych i serwisowych. W przypadku braku podstawowego źródła zasilania cały układ podtrzymywany jest z zasilaczy UPS i załączany jest agregat.

Klasyfikacja Tier

Tier III (cd):

- Dubluje się instalacje energetyczna przez dodatkowe rozdzielnie lub wyłączniki jak i pozostałą infrastrukturę niezbędna do poprawnego działania systemów IT. Ilość błędów i usterek jest ograniczona do kilku miejsc co znacznie podnosi dostępność całości systemu. Uszkodzenie jednego z urządzeń nie powoduje zatrzymania pracy Data Center. Oczekiwana dostępność 99,982%.

Klasyfikacja Tier

Tier IV:

- Infrastruktura odporna na awarie. Odporność na pojedyncze, nieplanowane zdarzenia, takie jak pożar, wyciek czy eksplozja. Są to dwa systemy zbudowane równolegle i działające równolegle. Cały redundantny układ podstawowy i rezerwowy posiada redundantne elementy, które działają jednocześnie. Możliwe osiągnięcie braku pojedynczego punktu awarii. Uszkodzenie jakiegokolwiek z elementów nie powoduje zatrzymania pracy Data Center. Oczekiwana dostępność 99,995%.

Klasyfikacja Tier

	Tier I	Tier II	Tier III	Tier IV
Źródło zasilania IT	System	System	System	System + system
Zasilanie z sieci energetycznej	niewymagane	niewymagane	niewymagane	niewymagane
Ścieżki zasilania	1	1	1 podst.,1 zapas.	2 równoległe
Redundancja całości infrastruktury	N	N+1	N+1	Min. N+1
Brak ograniczeń w uruchamianiu agregatów prądotwórczych	Nie	Nie	Tak	Tak
Jednoczesność serwisowania / konserwowania	Nie	Nie	Tak	Tak
Ciągłe chłodzenie	Nie	Nie	Nie	Tak
Odporność na pojedyncze zdarzenia	Nie	Nie	Nie	Tak, automatyczna reakcja
Pojedyncze punkty awarii	Liczne + czynnik ludzki	Liczne + czynnik ludzki	Kilka + czynnik ludzki	Brak

Klasyfikacja Tier

- Dodatkowe kryteria dla tej klasyfikacji są opisane w dokumencie „Data Center Site Infrastructure Tier Standard: Operational Sustainability”,
- Dokument określa czynności i procedury jakie należy stosować, aby zapewnić wymagana niezawodność operacyjną centrów danych odpowiedniej klasy Tier

Klasyfikacja Tier

- Procedury i czynności:
  - Zarządzanie i operacje – zatrudnienie, kwalifikacje, organizacja pracy, procedury związane z zarządzaniem i utrzymaniem centrum danych (program prewencyjnego zarządzania, zasady utrzymania czystości, zarządzanie systemami, zasady wsparcia i kontaktu z dostawcami, planowanie czasu życia komponentów itp.), programy szkoleń, planowanie działań (np. zarządzanie dostępną pojemnością centrum danych).

Klasyfikacja Tier

- Procedury i czynności:
  - Charakterystyka budynku – czynności przed uruchomieniem systemu (procedury odbioru testowanie instalacji i urządzeń itp.), przeznaczenie budynku (dedykowany na potrzeby centrum danych czy wydzielona przestrzeń), zabezpieczenie budynku, kontrola dostępu, możliwości rozwoju (przestrzeni, wydajności, pojemności).

Klasyfikacja Tier

- Procedury i czynności:
  - Lokalizacja obiektu – zagrożenia związane z naturalnymi kataklizmami, lokalizacja która mogłaby mieć wpływ na bezpieczeństwo obiektu (odległość portu lotniczego, autostrady itp.).

Norma TIA-942

- W roku 2005 organizacja Telecommunications Industry Association (TIA) opublikowała normę TIA-942 o nazwie „Telecommunications Infrastructure Standard for Data Centers”, która jest najbardziej popularnym standardem wykorzystywanym do projektowania centrów danych.
- Klasyfikacja Tier została zapożyczona od The Uptime Institute i fakt ten jest kilkakrotnie wspominany w treści normy. Klasy nie są tym samym i różnią się od siebie fundamentalnie.

Norma TIA-942

- Dlatego też występują różnice w oznaczaniu i funkcjonowaniu klasyfikacji:
  - The Uptime Institute klasy Tier oznacza rzymskimi cyframi I, II, III, IV (Tier I, Tier II, Tier III, Tier IV)
  - TIA-942 oznacza cyframi arabskimi 1, 2, 3, 4 (Tier 1, Tier 2, Tier 3, Tier 4).

Norma TIA-942

- W celu uniknięcia niejasności 18 marca 2014 roku, podpisano porozumienie, na postawienie którego nastąpiła zmiana normy ANSI/TIA-942 na ANSI/TIA-942:2014,
- Porozumienie uregulowało, że słowo Tier będzie używane tylko i wyłącznie przez Uptime Institute a tym samym w ANSI/TIA-942 pojęcie to zostało usunięte i zastąpione słowami Rated lub Rating.

Norma TIA-942

- TIA-942 definiuje szereg wytycznych dla czterech klas dotyczących m. in.:
  - telekomunikacji,
  - konstrukcji budynku,
  - zadaszenia,
  - elementów budynku,
  - pomieszczeń,
  - dróg transportowych,
  - miejsc magazynowych i przechowywania paliwa,
  - bezpieczeństwa fizycznego budynku,
  - odporności ścian,
  - systemów bezpieczeństwa,
  - instalacji elektrycznych i jej komponentów,
  - instalacji mechanicznych – chłodzenia i wentylacji,
  - systemów przeciwpożarowych

Norma TIA-942

ANSI/TIA-942:2014 definiuje 4 poziomy dla obiektów Data Center

Ocena (rating)	Wymagania	Dostępność / czas naprawy
1	Systemy podstawowej dostępności, brak redundancji zasilania czy dostępu do sieci. Prace naprawcze i awarie powodują niedostępność usług centrum danych	99,671% (ok. 29 godzin przerwy w roku)
2	Dostępność zwiększona z racji na redundancję niektórych krytycznych elementów infrastruktury, np. zasilania. Okna serwisowe w dalszym ciągu są niezbędne	99,741% (ok. 22 godzin przerwy w roku)
3	Podatność dotyczy jedynie nieplanowanych zdarzeń, ponieważ każdy element zasilania i chłodzenia można wymienić bez przerwy w pracy centrum danych. Topologia centrum danych w całości zrealizowana z zachowaniem reguł wysokiej dostępności. Obiekt objęty monitoringiem, a na miejscu stałe są pracownicy serwisowi	99,982% (do. 95 minut przerwy w roku)
4	Centrum danych nie ma pojedynczego punktu awarii. Zarówno prace naprawcze, jak i pojedyncza, nawet poważna awaria, nie wpływają na ciągłość pracy centrum danych. Wynika to z pełnej redundancji systemu.	99,995% (do 26 minut przerwy w roku)

Porównanie norm

- Jak widać oba standardy mają wiele wspólnych założeń m.in:
  - czteropoziomowy podział dostępności wraz z odpowiadającą mu infrastrukturą,
  - systemy bezpieczeństwa,
  - zarządzanie zasilaniem,
  - monitoring,
  - Redundancją
- Jednak wiele je również dzieli m.in. pod względem zakresu wytycznych, co zostało przedstawione tabeli:

Porównanie norm

- Telekomunikacja

	Uptime Institute	ANSI/TIA-942
Główne elementy, technologia		TAK
Struktura, topologia zewnętrzna poza budynkiem	TAK*	TAK
Struktura, topologia wewnętrzna w budynku		TAK
Trasy kablowe, oznakowania		TAK
Uziemienie		TAK

- Architektura

Miejsce lokalizacji	TAK	TAK
Struktura, topologia	TAK**	TAK
Konstrukcja	TAK**	TAK
Ilości pomieszczeń i ich przeznaczenia		TAK
Wymiary i obciążenia		TAK
System CCTV		TAK
System Access Control	TAK	TAK
System bezpieczeństwa fizycznego	TAK	TAK

Porównanie norm

- Energetyka

	Uptime Institute	ANSI/TIA-942
Sposób podłączenia do sieci zawodowej		TAK
Struktura, topologia	TAK	TAK
System zasilania awaryjnego	TAK	TAK

- Mechanika

Systemy chłodzenia	TAK	TAK
Systemy paliwowe	TAK	TAK
Autonomiczne system ppoż.		TAK

źródło http://blog.datacenterworld.pl

* dotyczy doprowadzenie tylko połączeń do DC
** dotyczy Tier IV

Certyfikacja

- W kontekście klasyfikacji Tier certyfikacja centrów danych jest możliwa tylko i wyłącznie przez The Uptime Institute w 3 kategoriach:
  - Certyfikat dokumentacji projektowej (Tier Certification of Design Documents),
  - Certyfikat istniejącego/wybudowanego centrum danych (Tier Certification of Constructed Facility),
  - Certyfikat niezawodności operacyjnej istniejącego obiektu (Operational Sustainability Certification).

Pozostałe standardy

- SAS70 – (Statement on Auditing Standards) był standardem stworzonym przez amerykańskich biegłych rewidentów (Auditing Standards Board of the American Institute of Certified Public Accountants – AICPA), który przez ponad 40 lat stanowił w USA podstawę raportowania wyników badania kontroli w organizacjach usługodawców. Dzięki ustawie Sarbanes-Oxley (SOX), SAS70 stał się standardem stosowanym na skalę międzynarodową. Raport z audytu prezentował ocenę wdrożenia i efektywności operacyjnej mechanizmów kontrolnych badanego usługodawcy. Istniejący SAS 70 został zastąpiony przez SSAE 16 (obecnie SSAE 18) i ISAE3402.
- ISAE3402 – (International Standard on Assurance Engagement) to standard stworzony przez International Auditing and Assurance Standards Board (IAASB), radę do spraw standaryzacji przy Międzynarodowym Stowarzyszeniu Księgowych (IFAC).
- SSAE 16 – Standard dotyczy kontroli wewnętrznych mających wpływ na sprawozdania finansowe odbiorcy usług. Standard opublikowany przez AICPA (American Institute of Certified Public Accountants).

Pozostałe standardy

- Podstawowy podział dokonany przez AICPA (American Institute of Certified Public Accountants) wyróżnia 3 rodzaje audytów (SOC – Service Organization Control):
  - SOC 1: Audyt dotyczy kontroli wewnętrznych mających wpływ na sprawozdania finansowe odbiorcy usług.
  - SOC 2: Audyt dotyczy procesów niefinansowych, które mają kluczowe znaczenie dla jakości dostarczanej usługi. W szczególności brane są pod uwagę kryteria pod względem bezpieczeństwa, dostępności, integralności, poufności, prywatności. Raport z audytu jest dostępny tylko dla obecnych klientów (klienta), zawiera bowiem szereg szczegółowych informacji. Publicznie udostępniona może być informacja o pomyślnej opinii z przebytego audytu, co daje gwarancje jakości usługi potencjalnym klientom.
  - SOC 3: Audyt dotyczy tych samych procesów co SOC 2, jednak raport z audytu jest udostępniany potencjalnym klientom (ponieważ zawiera ograniczony zakres danych wobec raportu wg SOC 2 i może być dostępny publicznie). Zawiera zapewnienie kierownictwa o spełnieniu określonych wymagań oraz opinię audytora.

Pozostałe standardy

- Dodatkowo istnieją 2 typy audytów:
  - Typ I przedstawia opis systemu oraz ocenę adekwatności kontroli wewnętrznych,
  - Typ II zawiera dodatkowo ocenę rzeczywistego funkcjonowania kontroli wewnętrznych. Z oczywistych względów typ II ma znacznie większą wartość dla odbiorców usług.
- Dla standardów SSAE 16 (czy SSAE 18) i ISAE3402 oraz rodzajów audytów SOC1 i SOC2 nie istnieją certyfikaty. Raporty atestacyjne oznaczają, że badania kontroli w organizacjach świadczących usługi zostały przeprowadzone w oparciu o w/w standardy.
- Miejscami, gdzie można sprawdzić informacje o posiadanych przez centra danych zabezpieczeniach i certyfikatach, są:
  - Serwis Data Center Map: https://www.datacentermap.com/
  - CSA Security, Trust & Assurance Registry (STAR), w wyniku którego powstał publicznie dostępny rejestr, w którym udokumentowane są systemy kontroli stosowane przez dostawców usług chmurowych: https://cloudsecurityalliance.org/star/

Dostawcy usług chmurowych i centrów obliczeniowych - certyfikaty

	Uptime Institute	TIA-942	SOC	STAR
AWS			1, 2, 3	Self assessment
Azure			1, 2, 3	Self assessment, certification/attestation
Aruba Global Cloud Data Center		Rating 4		
Aruba.it IT1		Rating 4		
EXEA	Tier III Polska			
Google			2, 3	Self assessment
Beyond.pl Data center 1		Rating 3		
Beyond.pl Data center		Rating 4		
Dropbox			1, 2, 3	Self assessment, certification/attestation
HP	Tier II – Kostaryka		2, 3	Self assessment, certification
Huawei	Tier III China			
OVH			1, 2	Self assessment
Samsung	Tier III Korea Płd			
Vodafone Data center	Tier IV Indie			

Przywracanie infrastruktury - Disaster Recovery

- Disaster Recovery - odtwarzanie po katastrofie
  - w ogólności dotyczy ciągłości działania danego przedsiębiorstwa lub instytucji,
  - w obszarze IT rozwiązania Disaster Recovery skupiają się na przywróceniu po awarii (katastrofie) przetwarzania w infrastrukturze informatycznej używanej w czasie normalnej pracy.
- Disaster Recovery Plan (Plan awaryjny) jest najważniejszym dokumentem w rozwiązaniu Disaster Recovery.

Przywracanie infrastruktury - Disaster Recovery

- Disaster Recovery - podstawowe terminy:
  - RTO (Recovery Time Objective) - czas od katastrofy do odtworzenia normalnego funkcjonowania.
  - RPO (Recovery Point Objective) - aktualność danych odtworzonych po katastrofie.

Przywracanie infrastruktury - Disaster Recovery

- Poziomy rozwiązania Disaster Recovery wg klasyfikacji SHARE:
  - 0: No off-site data (Kopia lokalna składowana lokalnie)
  - 1: Pickup Truck Method PTAM (Kopia lokalna składowana zewnętrznie)
  - 2: PTAM + hot site (Kopia lokalna + Ośrodek zapasowy)
  - 3: Electronic vaulting (Kopia zdalna w ośrodku zapasowym)

Przywracanie infrastruktury - Disaster Recovery

- Poziomy rozwiązania Disaster Recovery wg klasyfikacji SHARE (cd.):
  - 4: Active Secondary Site (Aktywny ośrodek zapasowy)
  - 5: Two-site two-phase commit (Zapis jednoczesny)
  - 6: Zero Data Loss (Bez utraty danych)
  - 7: Automatic site switch (Automatyczne przełączenie)

  Szczegółowy opis poziomów: http://www.vault.pl/datacenter:bcp:klasyfikacja

Dziękuję za uwagę