MOD 1: Azure Cloud Concepts

1. Cloud computing is the delivery of computing services over the internet, enabling faster innovation, flexible resources, economies of scale

2. Public cloud:

- owned by cloud services

- provide services to multiple user

- accessed via network

- Organizations pay only for what they use

Zalety:

* Prosta I szybka do wykorzysatnia
* Pay as you go
* Cost control

Wady:

- znajduje się w rękach providera

- trzeba stosować zabezpieczenia

- to provider decyduje co jest w ofercie

Private cloud:

* Built in organization datacenter
* Organization is responsible for services
* Access only for users from organization
* Single tenant environment

Wady:

* Wysokie koszty utrzymania
* Trzeba mieć swój dział IT

Hybrid cloud:

- Kominacja public i privat e

- Organizations control security, compliance, or legal requirements.

Wady:

- dodatkowy hardware

- dodatkowa konfiguracja

- ciężko utrzymać kompatybilność

- spowolnienie przesyłu danych

3.

- High availability

- Scalability – nie trzeba przewidywać wcześniej jaki mędzie ruch, można dynamicznie sterować zasobami

- Global reach – datacenter na całym świecie

- Agility

- Fault tolerance - metoda na automatyczne rozwiązanie lub obejście problemu

- Elasticity – dynamiczne zwiększanie, zmniejszanie parametrów serwerów dla danego rozwiązania

- Customer latency capabilities

- Predictive cost considerations

4. Scale out – dodawanie nowych maszyn

Scale in – zarządzanie pojedynczą maszyną, zwiększanie liczby procesorów, podłączanie dysków

5. Odpowiada za dystrybucję zadań do maszyn, otrzymuje żądania od klientów i decyduje który komputer ma je obsłużyć. Z jednej strony obsługuje jeden adres IP a z drugiej wiele adresów poszczególnych serwerów. Istnieją różne polityki rozdzielania zadań: losowa, taka sama ilość do wszystkich, w zależności od prędkości odpowiedzi serwera.

6. Określa co ma się dziać w przypadku katastrofy

7. Skalowalność jest zarządzana przez człowieka a elastyczność automatycznie. Przy elstyczności deklarujemy, że przy konkretnych warunkach ma dojść do rozszerzenia parametrów.

8. Capital Expanditure:

- koszty na samym początku, duże, przeznaczone na dłuższy czas – koszty środków trwałuch

- up-front spending of money on physical infrastructure

- reduces over the time

Operational Expanditure:

* pojawiają sie w trakcie działalności, płacisz w miarę jak używasz
* spending on service or product
* expenses deducted over the year

9. End users only pay for the resources that they use

10.

-Better cost prediction

- Prices for individual resources and services are provided

- Billing is based on actual usage

11. Infrastructure as a Service – dostawca zapewnia dostęp do infrastruktury

- hardware

- network connectivity

- physical security

12. Platform as a Service – wszystko od infrastruktury po middleware:

IaaS +

- Operating system

- development tools, database management

- business analytics

13. System as a Service – gotowa funkcjonalność

PaaS +

- Hosted application

14. Żeby wiedzieć w jakim zakresie my jesteśmy odpowiedzialni za usługę a w jakim dostawca

15. Gdy istnieją niezwykłe wymagania co do systemu operacyjnego

16. Shift and lift

17. Brak kontroli nad rozwojem produktu

18. Opcja przy deploymencie apki webowej, streruje śledzeniem apki. Zbiera logi, informuje kiedy obciążenie było wysokie lub kiedy doszło do błędów.

19. Pricing calculator

20. Total cost of ownership calculator

21. Do wykonania określonego działania nie mamy na przydzielonych na stałe i wyłączność zasobów tylko zadanie wykonują akurat wolne tymczasowo zasoby.

22. Azure functions – wykonuje zadania bez dedykowanej infrastruktury

Azure Logic Apps – wspomaga orchiestrację i integrację danych, systemów i usług

23. Logiczny kontener grupujący elementy składające siew jedną całość np. aplikację. Sprawdza się jeśli chodzi o nadawanie uprawnień

24. Z dokładnością do resource grupy

25.Nie, region resource grupy to tylko miejsce przechowywania metadanych opisujących tą resource grupę

26. Na obszary geograficzne, które składają się z regionów

27. Regiony to zbiory centrów danych. W regionie jest min. 1 datacenter

28. Żeby mieć high availability. Każdy region ma region bliźniaczy i w razie problemu dane są szybko replikowane do drugiego z pary. Obydwa regiony są w tym samym obszarze geograficznym.

29. Min 300 km

30. Availability set – ochrona maszyny znajdującej się w jednej domenie

Fault domain – maszyn wirtualne są rozmieszczone w taki sposób, że awaria pojedynczego komponentu nie powoduje uszkodzenia wszystkich maszyn wirtualnych. Maszyny wirtualne są rozmieszczone pomiędzy różne urządzenia sieciowe. Mogą być max 3 fault domains.

Update domain – maszyny z różnych update domain nie będą jednocześnie obsługiwane przez techników w celu maintenancu – max 20 update domain

Availability zone – rozkładamy serwery wchodzące w skład aplikacji na więcej datacenter w ramach regionu. Jeśli używamy Availability Zone to nasze dane znajduja się w kilku miejscach na raz. Każde zone ma niezależne zasilanie, chłodzenie i sieć

31. 3

32. Nie, trzeba ją stawiać na nowo

33. Używając disaster recovery

34.

– Zabezpiecza przed odcięciem usług

- Fizyczna separacja datacenter w ramach jednego regionu

- Każdy datacenter wyposażony w niezależne zasilanie, chłodzenie i sieć

- Połączone przez dedykowany światłowód

35. Komponenty pozwalające na budowanie rozwiązań chmurowych

- maszyny wirtualne

- storage accounts

- sieci wirtualne

- App services

- SQL Databases

- Functions

36.

- dany zasób istnieje tylko w jednej resource grupie

- zasoby resource grupy mogą istnieć w różnych regionach

- zasoby mogą bvyć przenoszone do innych resource grup

- aplikacja może wykorzystywać wiele resource grup

37. Azure Resource Manager – pozwlana na tworzenie, modyfikację i usuwanie zasobów w subskrypcji

38.

- Powershell - install-module az

- Cloud Shell –

- Azure Command Line – az login

39. Rodzaj umowy jaką zawieramy z Microsoftem w zakresie usług z jakich korzystamy w Azure.

40.

Billing boundary – generowanie raportów finansowych i faktur za każdą subskrypcję

Access control boundary – granica wyznaczona przez subskrypcję – zarządzanie dostępem do zasobów dla konkretnych subskrypcji

41. Management grupa zawiera inne management grupy lub subskrypcje. Subskrypcje dziedziczą warunki jakie są narzucone na management grupy.

42. 10000

43. Compute is an on-demand computing service that provides computing resources such as disks, processors, memory, networking, and operating systems

44. Software emulations of physical computers

45. App Services is a fully managed platform to build, deploy, and scale web apps and APIs quickly

46. Light-weight, virtualized environment that does not requireoperating system management.

47. Desktop and app virtualization that runs in the cloud.

Windows Virtual Desktop to technika przeniesienia aplikacji do chmury ale w całości – łącznie z urządzeniami klienckimi. Kolejny krok w wirtualizacji – zwirtualizowaliśmy serwery, bazy danych – teraz pora na aplikacje klienckie. Zalety:

- sprzęt nie musi być już tak często aktualizowany

- nie ma sytuacji, że w aplikacji coś nie działa

- wszystko odbywa się centralnie (aplikacja i virtual desktop w jednym miejscu) – jest bezpieczniej, nie ma problemu, że ktoś nam ukradnie komputer

- rozwiązanie zgodne z certyfikatami – nie trzeba ogarniać tego samodzielnie

Na jednej maszynie moze pracować więcej użytkowników – wtedy mamy multisesyjność.

Windows Virtual Desktop przesuwa punkt ciężkości rozwiązania klienckiego z maszyny użytkownika w stronę centralnej lokalizacji, gdzie tak na prawdę odbywa się całe przetwarzanie aplikacji. W takiej konfiguracji stacja robocza nie musi posiadać zbyt wielu zasobów, bo praktycznie odpowiada tylko za pobieranie danych od użytkownika i wyświetlanie informacji. Taka konfiguracja jest często nazywana "thin client" (cienki klient). Przeciwieństwem jest "fat client" (gruby klient).

48. Azure Virtual Network – enables Azure resources to communicate with each other. Wirtualna sieć łącząca komponenty aplikacji ale też łaczy aplikację ze światem zewnętrznym (ale tylko warstwę presentationawre)

49. Virtual Private Network – send encrypted traffic between Azure virtual network and on-permises location over public internet

50. Connects on-permises network with Azure over private connection facilitated by connectivity provider

51. Blob storage, Queue storage, Disk storage, Azure files

52. Binary large object – storage na pliki które nie mają wewnętrznie zdefiniowanej struktury – zdjęcia, wideo, muzyka, logi, korzysta z nich bardziej aplikacja niż człowiek. Pliki blob porządkuje się w kontenerach

53. Hot (dane pobierane regularnie), cool (dane pobierane nieregularnie, przechowywane min. 30 dni), archive (dane pobierane rzadko, przechowywane min 180 dni)

54. struktura pozwalająca na przechowwanie wiadomości, to nie człowiek generuje wiadomość do kolejki, robi to API. Wiadomość ma wielkość do 64kB

55. Służy do przechowywania obrazów dyskowych dla maszyn wirtualnych.

56.

Zarządzane – to Microsoft stara się o utworzenie storage account gdzie przechowywany jest dysk

Niezarządzane - to ja muszę utworzyć storage account dla takiego dysku. Na tym storage account dysk jest przechowywany jako BLOB.

57. zasoby dostępne z wykorzystaniem SMB (Server Message Block)

58.

Azure Cosmos Database – nierelacyjna baza danych. 4 sposoby przechowywania danych: klucz/wartość, system kolumnowy, dokumentowa baza danych, grafowa baza danych,

Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL.

59. Azure SQL Managed Instance

60. Azure Marketplace

61.

Azure Stack – zestaw hardware I software, który można kupic od Microsoftu i zainstalować on permises.

Azure Express Route – wykorzystanie fizycznego połączenia z twojeje serwerowni do serwerowni Azure. Stabilne rowziązanie o dużych prędkościach przesyłu, bezpieczniejsze, stabilniejsze. Nie da się wyklikać, trzeba się zgłosić do Microsoftu.

Import/Export – dane są nagrywane i odtwarzane bezpośrednio z dysku, bez użycia kabla

62. Azure Application Gateway - dba o to aby raz nawiązane połączenie trafiało do tego samego serwera po stronie aplikacji. Inna funkcja AAG to wyświetlanie informacji o błędzie jeśli klient rząda wyświetlenia nieistniejącej strony.

Inna funkcja to rozpakowywanie pakietów SSL żeby serwery odpowiadające za generowanie strony nie poświęcały swojej mocy obliczeniowej na szyfrowanie danych.

63. Odpowiada na to aby urządzenia znajdujące się na zewnątrz sieci wirtualnej były w stanie do tej sieci się podłączyć. Dzieje się to przez stworzenie dedykowanego tunelu. Istnieją 3 różne sposoby połączenia do VPN Gateway: Site to site, Point to Site, VNet to Vnet

64. Jeśli kolejny raz jest request po te same dane to są one pobierane nie ze źródła a z POP bo trafiły tam po pierwszym requeście. Każdy plik w POP ma time to leave po którym jest usuwany. Celem jest oszczędzanie na transferze danych na dużych odległościach.

65. Ustala do jakich lokalizacji kierować requesty użytkownika. Zasoby są w wielu miejscach a ten manager kieruje tam, gdzie żądane dane mogą być pozyskane jak najszybciej. W tym przypadku nie dochodzi do transferu całego wielkiego pliku a pracujemy na DNSie. User prosi o zasób podając DNS a Manager przekierowuje go do odpowiedniej lokalizacji.

66. Budowanie rozwiązań gdzie dużo czujników raportuje w jedno miejsce. Np. zarządzanie klimatyzacją w wielkim budynku.

67.

Azure IoT Hub – ma odpowiadać za nawiązywanie komunikacji z urządzeniami i odbieranie informacji, które z nich przychodzą. Możemy tu zarejestrować do miliona urządzeń. W Iot Hub można wysyłać komunikaty do urządzeń i takie komunikaty nazywa się Cloud To Device albo CtoD albo od urządzenia do huba (Device to Cloud).

Azure IoT Central – w tym przypadku mniej skupiamy się na komuniakacji. Chodzi o wyciąganie biznesowej wartości z IoT. Chodzi nie tylko o zbieranie komunikatów ale też do wysyłanie ich do aplikacji które z nich korzystają np. do PowerBI. Azure IoT Central to SaaS.

Azure Sphere – dotyczy bezpieczeństwa samych czujników. W przypadku Azure Sphere Microsoft zbudował własny system operacyjny, który może być instalowany na tych urządzeniach. System jest podzielony na warstwy dzięki czemu możliwy jest defence in depth. Nie trzeba kierować się do dostawcy urządzeń po aktualizacje tylko ogarnia to Microsoft. Urządzenia też ogarnia Microsoft.

68. Aktualnie gdy mamy dyski 1 TB to za Big Data uznajemy 1 PB. Big data jest wtedy gdy nie da się przetworzyć przez komputer danych bo jest ich za dużo.

69. Data lake to zbiór danych w postaci nieustrukturyzowanej.

70.

Azure Synapse Analytics – dane są przechowywane w postaci relacyjnej ale są przetwarzane przez wiele serwerów i dsięki temu mamy szybko wyniki. Można nadawać uprawnienia userom, dane są szyfrowane – więc jest bezpiecznie. Żeby uzyskać dane z Azure Synapse trzeba napisać zapytanie SQL. W przypadku Big Data problematyczne jest nie tylko odczytywanie danych ale i ładowanie. Dlatego mamy programy ATF copy albo SSIS albo zapytań kierowanych innych baz przy pomocy których dane są ładowane do Azure Synapse. W Azure Synapse jest cachowane elementów żeby przyspieszyć działanie zapytań. Przetważanie odbywa się na wielu klastrach.

HDInsight – dane mają być przetwarzane w prosty sposób z niewielkim kosztem. Budowane są klastry serwerów i gdy pojawiają się zadania do przetworzenia zarządca kieruje te zadania do nodów w klastrach. Praca rozproszona. Każdy z nodów wykonuje pewien kawałek pracy.

Azure Databricks – pretwarzanie danych w trybie serverless computing. Nie mamy dedykowanych maszyn. Gdy coś potrzebujemy przetworzyć to wtedy jest oddawana do dyspozycji moc obliczeniowa. Azure Databricks to zbiór narzędzi przy pomocy których możemy projektować w jaki sposób dane będą wytwarzane. Budujemy skrypty, programy joby. Nie oczekujemy, że dane zostaną otrzymane natychmiast.

71.



72. Przykład machine learning – wynajmowanie pokoju. Jeśli ktoś zgłosi się z pokojem do wynajęcia to algorytm ML ustali jaka powinna być cena za ten wynajem.

73.

Azure Machine Learning – przy użyciu tego programu mozemy tworzyć własne algorytmy w sposób graficzny.

Przy korzystaniu z Machine Learning Studio mamy do dsypozycji bloki odpowiadające za różne czynności. Bloki przeciąga się an panel skryptów i łączy się ze sobą.

Azure Bot Sevice – pozwala na tworzenie oprogramwania które pozwala na prowadzenie rozmowy z klientem. Np czat wbudowany w stronę webową. Azure Bot Service odpowiada na potrzebę integracji ze środowiskiem interakcji z użytkownikiem, np ze slackiem albo messengerem. Sam bot jest pisany w języku programowania.

Integracja z Microsoftowymi środowiskami takimi jak Teams jest darmowa.

Cognitive Services – np usługa zmiany mowy w tekst.

Cognitive Services ma różne usługi. Np. Wspierające podejmowanie decyzji:

Anomaly detector- wykrywanie anomalii

Content Moderator – szuka w wypowiedziach brzydkie słowa

Personalizer – w oparciu o znajomość danych o użytkowniku próbuje dopasować wrażenia w nowych aplikacjach na takie, które użytkownik lubi

Dotyczące języka:

Immersive Reader – wspiera użytkowników mających problemy ze wzrokiem w czytaniu tekstów

Language Understanding – próbuje zrozumieć sens wypowiedzi

QnA Maker – odnajduje odpowiedź na pytanie z póli najczęściej zadawanych pytań

Text Analytics – szuka w tekście odpowiedzi czy dana wypowiedź jest ozytywna czy negatywna

Translator Text – służy do tłumaczenia tekstu

Speech Recognition – rozpoznawanie użytkownika w oparciu o głos

74.

**Azure Functions**

Można wdrożyć rozwiązania, które będą działały ale nie otrzymają na własność maszyny wirtualnej. W Microsofcie jest dużo wyłączonych maszyn, których potencjał się marnuje

**Logic App**

1 cecha Logic App – tworzenie aplikacji polega na przeciąganiu komponentów i uzupełnianiu ich parametrów

2 cecha – nadaje się do budowania aplikacji które automatyzują pracę administratora Azure. Nadaje się do integracji Azure a częścią aplikacji on permises.

Budujemy mechanizm, który będzie powiadamiał o zmianach w wybranej resource grupie. W tym celu skorzystamy z obiektu, który nazywa się Event Grid.

75.

Coś dla programistów – **Azure DevOps**

Azure Devops to zbiór rozwiązań które mają wspierać pracę programisty. Do dyspozycji są takie produkty jak:

1. Azure Boards – zbiór narzędzi raportujących do śledzenia pracy programisty – dla nadzorujących. Konfigurowalne elementy na których można umieszczać graficzne obiekty.

2. Azure Pipelines – pozwala na wykonywanie CI/CD.

3. Azure Repos – pozwala na przechowywanie i zarządzanie kodem źródłowym aplikacji

4. Azure Test Plans – do zarządzania testami

5. Azure Artifacts – biblioteki z których mogą korzystać programiści. Pobieramy to bliblioteki i z nich korzystamy – na wypadek gdyby zniknęły z internetu

6. Extensions Marketplace – rozszerzenia, które można włączyć podczas tworzenia aplikacji

**Azure Dev Test Labs**

Azure Dev Test Labs pozwala zapanować nad procesem testowania. W ramach środowiska można mieć do dyspozycji przygotowane obrazy maszyn wirtualnych, które wystarczy wdrożyć. Dla firm, które nie chcą się przejmować przygotowywaniem środowisk testowych. Tam gdzie jest wiele komponentów, różnorakie systemy. Środowiska testowe służą nie tylko do weryfikacji poprawności działania ale też do badania wydajności. Jeśli środowisko produkcyjne znajduje się na Azure to środowisko testowe może być wierną kopią danych z produkcji. Możemy też weryfikować jakie koszty niesie za sobą utrzymanie takiego środowiska. Stworzenie samego Dev Test Laba jest za darmo ale trzeba będzie płacić za utworzone tam zasoby – dyki, maszyny wirtualne

76. Azure Advisor zawiera sugestie, które pozwolą poprawić jakość korzystania z chmury. W sekcji overview można sprawdzić co da się w subskrypcji poprawić. Analizie poddane są takie elementy jak:

- cost

- security

- reliability

- operational excellence

- performance

77. Azure Monitoring

78. Azure Service health.

79. Azure Resource Manager (ARM)

80. Służy do monitorowania I zarządzania bepieczeństwem

81. Free – monitorowanie maszyn wirtualnych i aplikacji

Standard - monitorowanie bazy danych, storage i powala na uruchamianie zaawansowane metody wykrywania zagrożeń bezpieczeństwa

82.

• Provides security recommendations

• Detect and block malware

• Analyze and identify potential attacks

• Just in time access control for ports

83.

- Policy compliance

- Continous Assessment

- Tailored Recommendations

- Thread Protection

84. Na stronie Trust Center

85. Strona Service Trust

86. Tam są akty prawne jakie odtyczą mojej firmy. Jeśli muszę wykazać zgodność z tymi normami możemy otworzyć formularz i zapoznać się za co odpowiada microsoft a za co ja.

87. Implementacja Security Information and Event Management. W usłudze tej informacje które ciągle napływają móc przetworzyć w sprytny sposób. Dane, które zostały zebrane są analizowane i wykrywane jest spośród wielu możliwych prób ataku te zdarzenia, które potwierdzają, że rzeczywiście jest atak i w tym przypadku wygenerować incydent i automatycznie rozwiązać problem zamykając port albo blokując konto użytkownika zainfekowanego.

88. SIEM – security information management

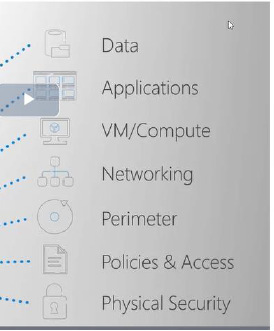
89. SOAR – security automated response

90. Key Vault – pozwala na przechowywanie haseł, kluczy, sekretów, certyfikatów w bezpieczny sposób w Azure. Żeby mieć do nich dostęp trzeba mieć uprawnieia a te przyznaje się w oparciu o Active Directory.

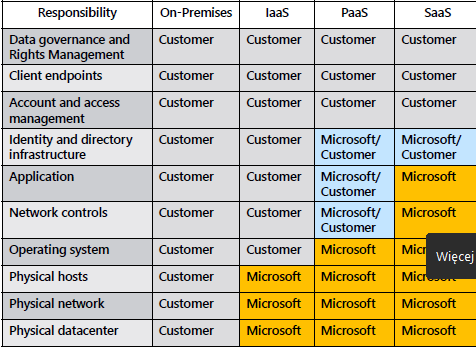
91. Mamy 2 plany Key Vault – standard i premium. Obydwa są płatne. W przypadku premium można korzystać z informacji kodowanej w hardware secret modules.

92. Serwer fizyczny obsługujący jedną lub więcej maszyn wirtualnych pojedynczej organizacji.

93. Warstwowe podejście do bezpieczeństwa systemu komputerowego:



94. Podział odpowiedzialności za bezpieczeństwo:



95. Network Security Group – filtruje ruch sieciowy do i z Azure. Pozwala na ustawienie zasad filtrowania adresu IP, portów i protokołów

96.

- confidentiality – dostęp mają mieć ci którzy naprawdę ich potrzebują – najniższy przywilej

- integrity – zapobieganie nieporządanym zmianom

- availibility – dane powinny być dostępne

97. Azure Firewall – zabezpiecza sieć w Azure. Zadaniem firewalla jest zezwolenie na taki ruch który świadomie dopuszczamy. Określamy źródło ruchu (adres ip i numer portu) i cel ruchu (adres ip i port na który pakiet ma przyjść). Firewall Azure jest statefull – zachowuje w pamięci stan połącen. Pakiety już raz zaakceptowane w ramach połączenia już później będą akceptowane.

Oprócz określenia jaki ruch ma być z zewnątrz dopuszczony firewall określa też jaki ruch ma być dopuszczony z wewnątrz do internetu. Gdyby ktoś włamał się do nas i chciał wyprowadzić dane.

98. Azure DDoS Protection – mamy dwa plany:

Basic – zawsze przypisany do sieci wirtualnej w Azure. Nie loguje ataków i ich nie raportuje, nie tworzy alertów. Darmowy.

Standard – Loguje atak, alertuje o problemi i jest wsparcie od Microsoftu. Automatycznie skaluje w przypadku ataku. Odpłatny.

99.

Uwierzytelnienie – authentication – sprawdzenie kim jesteś

Autoryzacja – authorization – sprawdzenie czy masz dostęp do danego zasobu, czy możesz zrobić to co chcesz zrobić. Autoryzacja wymaga wcześniejszego uwierzytelnienia.

100. Azure Multi-Factor Authentication – user uwierzytelnia się loginem, hasłem oraz jakimś urządzeniem np. telefon, albo keypass. Może też bazować na biometryce.

101. Azure Active Directory

Azure Active Directory B2C – business to customer – zasoby zdefiniowane w Azure będą udostępniane klientom. Uciążliew jest gdy wchodząc na stronę nowego sklepu musimy zakładać konto. Można to załatwić poprzez posiadanie konta na innej platformie np. Facebook czy Google. I to jest właśnie Azure

Active Directory B2C. Nie da się tego po prostu włączyć w ustawieniach AD, potrzebna jest specjalna konfiguracja aplikacji.

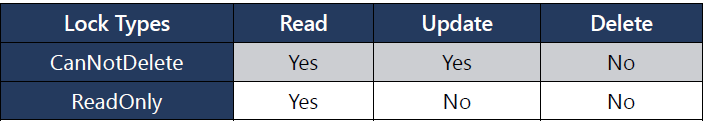
Azure Active Directory B2B – dwa podmioty mogą realizować jeden projekt i potrzebna jest kooperacja. Aby to zrobić przechodzimy do miejsca w AD, gdzie tworzy się nowych użytkowników ale wybieramy invite user:

102. Conditional access – użytkownik loguje się z zewnątrz lub z wewnątrz, korzysta z komputera lub aplikacji itd. Wszystkie czynniki warunkują jak będzie się autentykował. W ten sposób możemy określać jak należy się logować żeby wykjonać określone zadania. Możemy blokować użytkowników którzy nie znajdują się w określonej lokalizacji itd.

103. Role Based Access Control

104. Chroni przed niechcianym usunięciem.

105.



106. Pozwalają logicznie organizować zasoby. Są to pary klucz-wartość.

107. Pozwala wprowadzać standardy. Jedną subskrypcją może administrować wiele osób. Problem jest w tym żeby robili to jednakowo. Odpowiedni opis zasobów, wybór tych samych rodzajów maszyn wirtualnych, tworzenie zasobów takich samych rozmiarów. Do tego służy Azure Policy.

108. Policy jest przypisane do subskrypcji ale można wskazać zasoby, które mają nie podlegać policy. Można różnorako budować definicję polityki ale można też wzorować się na predefiniowanych policy. Np. dostępne lokalizacje dla COsmos DB.

109. Azure Blueprint – ma wspomóc architektów pracujących na rzecz wielkiej organizacji. Wcześniej omawialiśmy szablony ARM – wyklikiwaliśmy obiekt w interfejsie a później eksportowaliśmy template i tworzylismy na tej postawie kolejne obiekty.

Blueprint to pojemnik z wieloma szablonami ARM, definicjami grup zasobów i wiele więcej. Raz powstały blueprint możemy póxniej wdrażać. Dzięki temu kolejne powstałe aplikacje będą podobne.

Architekt albo zespół który wymyśla szablony może zamiast przekazywać zespołowi deweloperów dokument mówiący o tym jak budować aplikacje może przekazać gotowy blueprint. Zespół deweloperów wdroży go na swojej subskrypcji.

110. Cloud Adoption Framework – to proponowane ramy migracji do Azure w postaci kolejnych kroków jakie należy przejść. Na tej stronie znajdują się informacje co może motywować niezdecydowane firmy do migracji do chmury. Są też informacje o narzędziach jakie mają ułatwić proces migracji.

111.

CJIS – Criminal Justice Information Services dostęp do danych FBI

CSA-STAR – zgodność z ISO, spełnienie wymogów dotyczących krytycznych zdarzeń dotyczących bezpieczeństwa

EU Model Clauses – zasady przetwarzania danych z unii europejskiej

HIPAA – dostęp do danych dotyczących zdrowia i ubezpieczeń społecznych

ISO 27018 – zasady prztwarzania informacji personalnych

NIST CSF – national institute of standard and technology cyber security framework

SOC – service organization controls – audyt coroczny, bezpieczeństwo, dostępność, integralność, poufność danych

GDBR – RODO dane osobowe

G-CLOUD – przedtwarzanie danych I przedsiębiorstw obywateli UK

MTCS – w Singapurze, certyfikowana platforma dfo świadczenia usług

112. Miejsce gdzie można sprawdzić raporty z audytów i dowody na spełnienie compliance.

113.

- odseparowana insancja Azure

- fizyczna izolacja od nie-rządowych tenantów

- dostęp tylko dla autoryzowanego personelu

114. W chinach Azure musi współpracować ze spółką 21Vianet. W chinach to włąśnie za pośrednictwem tej firmy można kupić usługi.

115.

- Resource Type

- Services

- Location

- Bandwith – w zależności od tego ile danych wychodzi z Azure

- Reserved Instances – jest taniej gdy rezerwujemy zasoby/usługi na dłuższy okres

- Azure Hybrid Use Benefit – możemy używać licencji z on permises

116. Narzędzie do estymacji kosztów za produkty Azure.

• Region

• Tier

• Billing options

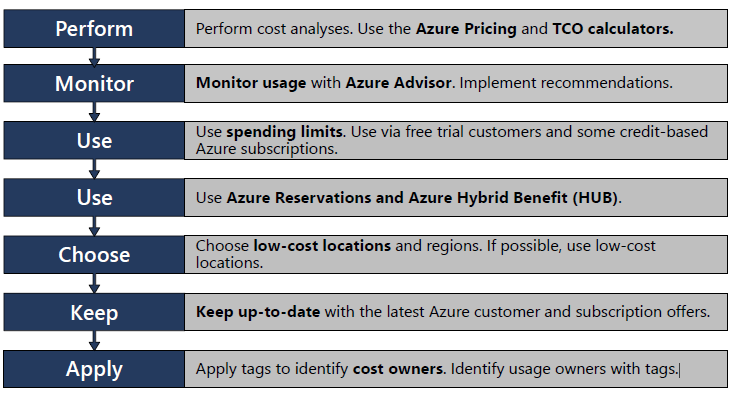
• Support options

• Programs and offers

• Azure dev/test pricing

117. Pozwala porównać koszt budowy rozwiązania on permises vs w Azure.

118.



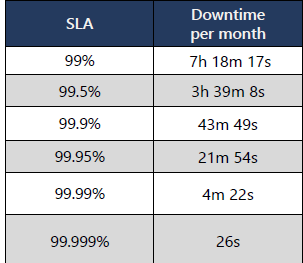
119. Każda z usług jest objęta umową między mną a dostawcą. Ta umowa nazywa się service level agreement (SLA). Właściwie to dla każdego zasobu istnieje osobna umowa, która określa co i jak działa. Każda umowa jest opisana na stronie Microsoftu. SLA nie dotyczy darmowych I demonstracyjnych wersji usług i produktów.

120.

- maszyna z instancjami w więcej niż jednej Availability Zone – 99.99%

- maszyna z instancjami w tym samym Availability Set – 99.95%

- pojedyncza instancja 99.9%



121. Microsoft tworząc nowe rozwiązania daje je do oceny wybranym klientom. Niedokończone rozwiązania są często dostępne i opisywane są w nazwie przez „Preview”.

122. Serwis, który otrzymuje informacje o wszystkich zdarzeniach w Azure.

123.

- Single – użytkownik dostaje endpoint do podłączenia bazy danych, która jest gdzieś w chmurze. Możemy płacić DTU – database transaction unit (płacenie za transakcje) albo zdecydować się na virtual core model – stała opłata.

- Elastic Pool – do dyspozycji jest kilka baz danych na jednym serwerze. Wspólne zasoby mają bazy danych.

- Managed Instance – kompatybilne z implementacją SQL Servera on premises. Głównie po to się to stosuje żeby migrować z on permises do chmury.

124.

Gen 1. – przechowywanie danych w postaci binary large object. Struktura danych jest płaska

Gen. 2 – pozwala na grupowanie blobów. Przetwarzanie moze być łatwiejsze bo możemy przetwarzać dane jednego katalogu. Ten storage jest bardziej wydajny.

125. Centralne miejsce do zarządzania tożsamością. Azure Active Directory to centralne miejsce z którego sterujemy bezpieczeństwem naszego rozwiązania.

126. Czynności jakie można wykonywać na portalu

127. Azure Multi-Factor Authentication – user uwierzytelnia się loginem, hasłem oraz jakimś urządzeniem np. telefon, albo keypass. Może też bazować na biometryce.

128. Azure information Protection – usługa do zabezpieczania danych elektronicznych – np. pilnowanie czy mail nie został wysłany do niewłaściwej osoby albo blokada możliwości wydruku załącznika

129. Azure Advanced Thread Protection – analiza zachoawnia użytkownikow a następnie klasyfikacja na takie które są podejrzane i takie które są zwykłą działalnością użytkownika

130. 

131. Oprócz SLA poszczególnych usług jest jeszcze SLA kompozytowe – jeśli moje rozwiązania składa się z 2-ch komponentów i pierwsza z maszyn jest dostępna przez 99.9% a druga 99.95% to SLA kompozytowe wynosi 0.999 x 0.9995 = 0.9985005.

132. W przypadku maszyn rozmieszczonych w Availability Zones Microsoft zwraca następującą liczbę środków:



W przypadku maszyn rozmieszczonych w Availability Sets Microsoft zwraca następującą liczbę środków:



Maszyna pojedyncza:



133. Vertical – zarządzanie iloscią CPU i RAM

Horizontal – zarządzanie ilością virtual machines i kontenerów

134. Ability of a system to recover from failures and continue to function

135. Predictability can be focused on performance predictability or cost predictability. Performance predictability focuses on predicting the resources needed to deliver a positive experience for your customers. Cost predictability is focused on predicting or forecasting the cost of the cloud spend.

136. Management of the cloud - managing your cloud resources:

* Automatically scale resource deployment based on need.
* Deploy resources based on a preconfigured template, removing the need for manual configuration.
* Monitor the health of resources and automatically replace failing resources.
* Receive automatic alerts based on configured metrics, so you’re aware of performance in real time.

Management in the cloud - manage your cloud environment and resources:

* Through a web portal.
* Using a command line interface.
* Using APIs.
* Using PowerShell