5 lipca wziąłem udział w zorganizowanym w Microsoft, technicznym warsztacie dotyczącym usług oferowanych (obecnie jest ich ponad 600!) na platformie chmury obliczeniowej Microsoft Azure oraz sposobu ich implementacji. Postaram się w skrócie podzielić zdobytą wiedzą i korzystając z okazji napisać więcej o możliwościach jakie niesie ta konkretnie chmura.

Warsztaty dotyczące usług Azure obejmowały techniczne wprowadzenie do produktów oraz omówienie przykładowych rozwiązań w powiązaniu z narzędziami potrzebnymi do pracy i kontrolą dostępu. Przedstawiona została globalna infrastruktura Azure, typowe usługi IaaS oraz usługi PaaS i SaaS. Relację z warsztatów podzieliłem na trzy części, w tym artykule przybliżę wstępne zagadnienia dotyczące Microsoft Azure oraz Azure Management Tools. Każda z części relacji z warsztatów dostarczy solidną dawkę sprawdzonej i niezbędnej wiedzy dotyczącej platformy chmurowej Azure. Zapraszam do lektury!

Wstęp do Azure

Zacznijmy do wyjaśnienia czym jest Azure i chmura jako taka. Mówiąc o platformie chmurowej, jaką jest np. Azure (model przetwarzania w chmurze pozwolę sobie pominąć) powinniśmy wiedzieć, że w uproszczeniu jest to nic innego jak infrastruktura centrum danych wyposażona w narzędzia do wirtualizacji (dla chmury prywatnej mówilibyśmy o Hyper-V), zarządzania (chmura prywatna – System Center), ale również mechanizmy skalowania i automatyzacji (Azure Stack), w odróżnieniu od np. kolokacji (która de facto również jest chmurą obliczeniową).

Do tego dochodzi mnóstwo zabezpieczeń, zaczynając od tych fizycznego i wirtualnego dostępu, przez systemy ppoż, nadmiarowe zasilanie, separację danych, a na szyfrowaniu tych danych w locie i spoczynku kończąc. Są to najwyższej klasy rozwiązania bezpieczeństwa wypracowywane przez pionierów branży w ciągu kilku dekad. Mówimy tu w sumie o „Security as a Service”, czyli Bezpieczeństwie jako Usłudze.

Warto dodać, że Azure to chmura publiczna, ale w żadnym wypadku nie oznacza to, że nasze dane są publicznie dostępne, a jedynie, że możemy korzystać z niej wspólnie, w odróżnieniu od chmury prywatnej, która jest dostępna tylko w ramach posiadającej ją organizacji. Obie chmury są dobre, tyle, że na tę drugą nie każdy może sobie pozwolić. Oczywiście mamy też chmurę hybrydową, np. dla potrzeb mocy obliczeniowej lub jako DRC (Disaster Recovery Center), co w praktyce oznacza, że nasza infrastruktura jest zreplikowana w chmurze publicznej, dzięki czemu w wypadku awarii kilka minut zajmie „przepięcie się” między ośrodkami i możemy być spokojni o business continuity, czyli ciągłość naszego biznesu.

Regiony

Microsoft może pochwalić się jednym z największych doświadczeń budowy i utrzymania centrum danych. Cała infrastruktura Azure podzielona jest obecnie pomiędzy 36 ośrodków regionalnych (6 w Europie), a w planach są kolejne 4 (po 2 we Francji i południowej Afryce). Daje to ciekawy obraz nie tylko skali, ale również nadmiarowości, którą możemy osiągnąć, oczywiście za odpowiednią ceną. Należy jednak pamiętać, że (przynajmniej na razie) każda usługa jest dostępna w każdym regionie, oznacza to, że planując nasze rozwiązania oparte na Azure lub ich nadmiarowość, musimy wziąć pod uwagę dostępność poszczególnych usług. Inne, jak np. CDN (Content Delivery Network) czy DNS są globalne. Warto dodać, że niektóre centra danych powstały specjalnie by świadczyć usługi dla lokalnej administracji państwowej lub Departamentu Obrony, w przypadku USA.

Microsoft Azure Management Tools, czyli Centrum Dowodzenia i nie tylko…

Portal / ARM / CLI / PowerShell

Przechodząc do kwestii zarządzania naszymi zasobami w chmurze, należy zacząć od podstawowego narzędzia jakim jest portal. W wielkim skrócie jest to miejsce, gdzie możemy „wyklikać” swoją infrastrukturę wirtualną i nią administrować. Nasze ulubione zasoby z łatwością znajdziemy w dostępnych Pulpitach Nawigacyjnych, które dodatkowo możemy współdzielić i mnożyć, by podzielić dzierżawione usługi na związane z np. konkretną aplikacją. Znajdziemy tu również galerie predefiniowanych maszyn wirtualnych, wyszukiwarkę zasobów, czy Marketplace, który jest centralnym miejscem przeszukiwania dostępnych usług i aplikacji. Pod maską wszystkim zarządza Azure Resource Manager, który oczywiście sami kontrolujemy. Dzięki niemu możemy definiować szablony infrastruktury i innych zależności dla naszych aplikacji, a potem wykorzystać je dla dowolnego środowiska; ARM umożliwia również wygodne zarządzanie zasobami aplikacji, organizowanie je w grupy zasobów by przyspieszyć wdrożenia, definiować poziomy dostępu czy nawet zwiększyć przejrzystość naszych rozliczeń.

Co ciekawe, z poziomu portalu możemy też od niedawna uruchomić Powłokę Chmurową Azure (Cloud Shell), by z poziomu linii poleceń (mamy tu na wyposażeniu powszechnie używane narzędzia CLI) kompilować nasze aplikacji i zarządzać nimi. Jest ona zintegrowana z edytorami tekstu, wspiera kilka popularnych języków programowania (m.in. Java, Python) i kontrolę źródeł git. Na poziomie użytkowym Portalu warto dodać, że potrafi dostosować się

do prędkości połączenia lub naszego urządzenia, choć w tym drugim przypadku użyjemy raczej dedykowanej aplikacji mobilnej, zatem co by się nie działo – mamy wszystko pod kontrolą będąc w ciągłym ruchu.
Podobnie działa to z drugiej strony, Azure możemy też zarządzać, jak się domyślacie przez PowerShell i napisane dla niego moduły, jednakże specjalnie dla użytkowników systemów Linux i OS X powstało narzędzie Azure CLI, której do używanej przez nas powłoki (np. bash) dodaje funkcjonalność administrowania Microsoft Azure.
Azure Active Directory
To prawdopodobnie pierwsza usługa Azure z której będziemy korzystać, choćby i zwłaszcza dlatego, że jest niejako „w pakiecie" z Office 365, jeśli już go mamy lub rejestrujemy się na Portalu Azure. Jest to bowiem (choć nie do końca) usługa katalogowa w chmurze, a jednym z jej plusów jest to, że w zasadzie jest darmowa, choć to zależy w jakim zakresie planujemy jej używać. Nie jest to pełnoprawny kontroler domeny (tutaj powinniśmy skorzystać z wirtualnej maszyny w Azure i na niej zainstalować rolę ADDS lub skorzystać z usługi Azure Active Directory Domain Services, jeśli chcemy przyłączać do domeny w chmurze wirtualne maszyny Azure), gdyż służy ona przede wszystkim do zarządzania tożsamością i dostępem w chmurze. Integruje się jednakże z lokalną domeną poprzez agenta Azure AD Connect, w celu uproszczenia zarządzania i logowania, gdyż dzięki takiej integracji można ustawić synchronizację hash-y haseł, w wyniku czego użytkownicy przy pomocy tylko jednego hasła zalogują się do wszystkich aplikacji w chmurze zarządzanych przez nasze AAD.
Bardziej zaawansowane funkcje, takie jak Multi-Factor Authentication (MFA, wieloskładnikowe uwierzytelnianie), MDM czy prawdziwe jednokrotne logowanie (true Single Sign-On, dzięki integracji z Active Directory Federation Services) są dostępne, ale wymagają płatnych wyższych edycji. Uważam, że o ile SSO głównie upraszcza pracę użytkownika, to MFA jest bardzo istotnym elementem, który stanowi drugą warstwę ochrony przed dostępem do naszych danych.
Powinniśmy go używać wszędzie tam, gdzie to możliwe, nawet w portalach społecznościowych takich jak np. Facebook, który również daje taką możliwość. Nawet jeżeli ktoś pozna nasze hasło i spróbuje wykorzystać je do zalogowania się na nasze konto, zostaniemy powiadomieni o próbie logowania z nieautoryzowanego urządzenia, a usługa będzie żądać podania kodu, który otrzymamy np. na nasz telefon komórkowy lub skrzynkę e-mail.
IAM – RBAC
Kolejną ważną funkcją jest Zarządzanie tożsamością i dostępem (IAM – Identity and Access

Management), która jest świadczona również przez AAD. Tu właściwie od razu przejdę do mechanizmu Kontroli Dostępu Opartej na Rolach, czyli RBAC (Role-Based Access Control), który zastąpił klasycznych administratorów subskrypcji. Mieli oni pełny dostęp. Jeśli już mówimy o bezpieczeństwie i efektywności pracy (nie tylko w chmurze), trzeba pamiętać, że pracownicy nie mogą mieć dostępu do rzeczy, za które nie odpowiadają, gdyż to zwiększa ryzyko nieuprawnionego dostępu i utraty kontroli nad naszym środowiskiem w wypadku ataku. Z drugiej strony nie powinniśmy tego dostępu zbytnio ograniczać, ponieważ może to sparaliżować przepływ pracy lub przynajmniej ograniczyć sprawność jej wykonywania.
Chcąc chronić się przed oboma scenariuszami mamy właśnie do dyspozycji RBAC, który daje możliwość bardzo precyzyjnej kontroli nad dostępem do zasobów. Same role to temat na oddzielne wypracowanie, dlatego przybliżę najważniejsze z nich oraz działania jakie wspierają. Możemy zatem wyróżnić 3 podstawowe role:
właściciel mający pełny dostęp do wszystkich zasobów i prawo nadawania dostępu innym;
moderator, który tak jak właściciel ma dostęp do wszystkich zasobów, ale nie może zarządzać dostępem do zasobów;
czytelnik z prawem jedynie do wyświetlania zasobów.
Poza tym, dostępnych jest ponad 40 predefiniowanych ról, jak np. Monitoring Contributor, która pozwala na odczyt i edycję ustawień monitorowania. Jeżeli dla kogoś okaże się to niewystarczające, to może zdefiniować nawet 2000 własnych ról (w ramach jednej dzierżawy) dla zapewnienia niemalże granularnej kontroli nad zasobami w Azure. Przy definiowaniu ról należy pamiętać, że relacja między subskrypcjami działa na zasadzie jeden do wielu. Każda jedna subskrypcja jest przypisana do jednego katalogu AAD, ale pojedynczy katalog może zawierać wiele subskrypcji. Ponadto trzeba zwrócić uwagę, iż RBAC pozwala na zarządzanie zasobami, jak np. magazyn danych, ale tabelami już nie, gdyż nie odpowiada on za operacje na danych.
To by było na tyle jeśli chodzi o pierwszą część serii poświęconej możliwościom jakie daje platforma Microsoft Azure. Następna odsłona będzie poświęcona Magazynom danych oraz Wirtualnym sieciom.
W międzyczasie jeżeli chcesz wiedzieć więcej zapraszamy do kontaktu z naszymi przedstawicielami.