Kluczowe technologie wspomagające dla wirtualnych chmur prywatnych

Koncepcja wirtualnej chmury prywatnej (VPC) pojawiła się jako sposób zarządzania zasobami technologii informacyjnej, tak że z logicznego punktu widzenia wydają się one obsługiwane przez pojedynczą organizację, ale mogą być zbudowane z podstawowych zasobów fizycznych, które należą do organizacji, zewnętrznego usługodawcy lub kombinacji obu. Kilka technologii ma kluczowe znaczenie dla skutecznego wdrożenia VPC. Wirtualne centra danych zapewniają izolację, która oddziela wirtualne zasoby jednej organizacji od zasobów innych organizacji oraz od podstawowej infrastruktury fizycznej. Aplikacje wirtualne gromadzą te zasoby w oddzielnie zarządzanych jednostkach. Wdrażanie oparte na zasadach i zgodność z zasadami oferują środki kontroli i weryfikacji działania aplikacji wirtualnych w wirtualnych centrach danych. Wreszcie integracja zarządzania usługami łączy podstawowe zasoby, zapewniając ogólny, logiczny i praktyczny widok. Te kluczowe technologie umożliwiają dostawcom usług w chmurze oferowanie organizacjom korzyści w zakresie kosztów i wydajności przetwarzania w chmurze, a także autonomii operacyjnej i elastyczności, do której są przyzwyczajeni.

Wstęp

Stosunkowo często zdarza się, że organizacje zlecają część lub całość swoich operacji IT zewnętrznemu dostawcy usług „chmury", który oferuje specjalistyczne usługi przez Internet po konkurencyjnych cenach. Model ten obiecuje wyższy całkowity koszt posiadania (TCO) dzięki wykorzystaniu wielkoskalowych zasobów towarowych, które są dynamicznie przydzielane i udostępniane wielu klientom. Dotychczasowy problem z tym modelem polega na tym, że organizacje musiały zrezygnować z kontroli nad zlecanymi na zewnątrz zasobami i funkcjami IT. Mogą zyskać na efektywności kosztowej usług oferowanych przez zewnętrznego dostawcę, ale tracą autonomię i elastyczność w zarządzaniu zlecaną na zewnątrz infrastrukturą IT w sposób spójny ze sposobem zarządzania wewnętrznymi operacjami IT. Koncepcja wirtualnej chmury prywatnej (VPC) pojawiła się niedawno jako odpowiedź na ten pozorny dylemat między kosztami a kontrolą. W typowym podejściu VPC łączy zasoby technologii informacyjnej (IT) organizacji z dynamicznie przydzielanym podzbiorem zasobów dostawcy chmury za pośrednictwem wirtualnej sieci prywatnej (VPN). Organizacyjne kontrole IT są następnie stosowane do zbiorowych zasobów w celu spełnienia wymaganych poziomów usług. W rezultacie, oprócz zwiększonego TCO, model zapewnia organizacjom bezpośrednią kontrolę nad bezpieczeństwem, niezawodnością i innymi atrybutami, do których są przyzwyczajone w konwencjonalnych, wewnętrznych centrach danych. Koncepcja VPC jest zarówno fundamentalna, jak i transformacyjna. Po pierwsze, proponuje odrębną abstrakcję zasobów publicznych w połączeniu z zasobami wewnętrznymi, która zapewnia funkcjonalność i pewność równoważną fizycznemu zbiorowi zasobów eksploatowanemu dla jednej organizacji, przy czym zasoby publiczne mogą być współdzielone z wieloma innymi organizacjami, które jednocześnie otrzymują swoje własne VPC. Po drugie, koncepcja zapewnia organizacji praktyczną ścieżkę do włączenia przetwarzania w chmurze do swojej infrastruktury IT. Gdy organizacja zarządza swoimi istniejącymi zasobami jako chmurą prywatną (tj. z wirtualizacją i standardowymi interfejsami do zarządzania zasobami), może bezproblemowo rozszerzyć swoją domenę zarządzania, aby obejmowała zasoby zewnętrzne hostowane przez dostawcę chmury i połączone przez VPN. Z punktu widzenia organizacji droga do modelu VPC jest stosunkowo prosta. W zasadzie nie powinno to być bardziej skomplikowane, powiedzmy, niż wprowadzenie VPN lub maszyn wirtualnych do infrastruktury IT organizacji, ponieważ abstrakcja zachowuje istniejące interfejsy i poziomy usług oraz izoluje nowe szczegóły implementacji. Jednak, podobnie jak w przypadku wprowadzania wszelkiego rodzaju abstrakcji, punkt widzenia dostawcy jest tam, gdzie pojawiają się zawiłości. Rzeczywiście, prawdziwym wyzwaniem VPC nie jest to, czy organizacje przyjmą je po spełnieniu wymagań IT organizacji, ale jak spełnić te wymagania – zwłaszcza autonomię

operacyjną i elastyczność – bez poświęcania wydajności, która motywowała zainteresowanie chmurą. Wraz z pojawieniem się VPC jako sposobu na udostępnienie przetwarzania w chmurze organizacjom, kolejnym pytaniem, które należy zadać, jest: Jakie są kluczowe technologie, które dostawcy usług w chmurze i organizacje potrzebują do realizacji VPC?

Wirtualne chmury prywatne

Chmura, zgodnie z definicją NIST, która stała się standardowym punktem odniesienia, to pula konfigurowalnych zasobów obliczeniowych (serwery, sieci, pamięć masowa itp.). Taka pula może być wykorzystana na kilka sposobów, jak opisano dalej w Mell and Grance:

• Prywatna chmura obsługiwana dla jednej organizacji;

• Chmura społecznościowa współdzielona przez grupę organizacji;

• chmura publiczna dostępna dla dowolnych organizacji; lub

• Chmura hybrydowa, która łączy dwie lub więcej chmur.

Pełna definicja chmury prywatnej podana w Mell and Grance to Chmura prywatna. Infrastruktura chmury jest obsługiwana wyłącznie dla organizacji. Może być zarządzany przez organizację lub stronę trzecią i może istnieć w lokalu lub poza lokalem. Definicja sugeruje trzy kluczowe pytania dotyczące wdrożenia w chmurze:

1. Kto korzysta z infrastruktury chmury?

2. Kto zarządza infrastrukturą?

3. Gdzie jest infrastruktura?

Rozróżnienie między chmurami prywatnymi, społecznościowymi, publicznymi i hybrydowymi opiera się przede wszystkim na odpowiedzi na pierwsze pytanie. Drugie i trzecie pytanie to opcje implementacji, które mogą dotyczyć więcej niż jednego modelu wdrażania. W szczególności dostawca chmury może obsługiwać i/lub hostować infrastrukturę we wszystkich czterech przypadkach. Chociaż definicja NIST nie określa tego wyraźnie, istnieje wniosek, że infrastruktura chmury odnosi się do zasobów fizycznych. Innymi słowy, zasoby obliczeniowe w chmurze prywatnej są fizycznie dedykowane organizacji; są używane tylko (tj. „wyłącznie") przez tę organizację przez stosunkowo długi czas. W przeciwieństwie do tego, zasoby obliczeniowe w chmurze publicznej lub społecznościowej są potencjalnie wykorzystywane przez wiele organizacji nawet przez krótki czas. Fizyczne ukierunkowanie definicji przyświeca koncepcji wirtualnej chmury prywatnej, która zgodnie ze zwykłym paradygmatem daje wrażenie fizycznej separacji, czyli rozszerzania:

Wirtualna chmura prywatna (VPC). Infrastruktura chmury wygląda tak, jakby była obsługiwana wyłącznie dla organizacji. Może być zarządzany przez organizację lub stronę trzecią i może istnieć w lokalu lub poza lokalem - lub może być kombinacją tych opcji.

Innymi słowy, VPC oferuje funkcję chmury prywatnej, choć niekoniecznie jej formę. Fizyczne zasoby obliczeniowe VPC mogą być obsługiwane przez wiele organizacji jednocześnie. Niemniej jednak, wirtualne zasoby prezentowane danej organizacji - serwery, sieci, pamięć masowa itp. - spełnią te same wymagania, jakby były fizycznie dedykowane.

Możliwość, że podstawowe zasoby fizyczne mogą być obsługiwane i/lub hostowane przez kombinację organizacji i strony trzeciej, jest ważnym aspektem definicji, jak po raz pierwszy sformułował R. Cohen w wpisie na blogu z maja 2008 r., który wprowadził VPC pojęcie:

VPC to metoda partycjonowania publicznego narzędzia komputerowego, takiego jak EC2, do infrastruktury wirtualnej poddanej kwarantannie. VPC może hermetyzować wiele lokalnych i zdalnych zasobów, aby wyglądały jako jedno jednorodne środowisko obliczeniowe, łączące możliwość bezpiecznego korzystania z zasobów zdalnych w ramach [a] płynnej globalnej infrastruktury obliczeniowej.

Kolejne prace skupiły się na konkretnym profilu wdrożeniowym, w którym VPC obejmuje tylko zasoby z chmury publicznej. Wood i inni w artykule z czerwca 2009 piszą:

VPC to połączenie zasobów przetwarzania w chmurze z infrastrukturą VPN, aby zapewnić użytkownikom abstrakcję z prywatnego zestawu zasobów w chmurze, które są przejrzyście i bezpiecznie połączone z ich własną infrastrukturą.

Podobnie Amazon opisuje swoją wirtualną chmurę prywatną w białej księdze ze stycznia 2010 r. ‚jako „odizolowaną część chmury AWS". połączony z zasobami wewnętrznymi przez VPN.

W obu Amazon, VPC ma wygląd chmury prywatnej, więc spełnia bardziej ogólną definicję podaną powyżej. Jednak profil wdrożenia nakłada ograniczenie na to, że zasoby fizyczne leżące u podstaw VPC są hostowane i obsługiwane przez dostawcę chmury. Innymi słowy, odpowiedź na drugie i trzecie pytanie powyżej jest „zewnętrzna". Chociaż zasoby wewnętrzne, np. „witryna przedsiębiorstwa" Wooda i in., są połączone z VPC przez VPN, nie są one częścią właściwego VPC. Ten artykuł utrzymuje szerszą definicję R. Cohena, ponieważ chmura, za którą organizacja będzie odpowiedzialna, ostatecznie obejmie większość lub wszystkie jej zasoby, a nie tylko części zewnętrzne. Rozważany tutaj podstawowy profil implementacji VPC to zatem taki, w którym podstawowe zasoby są pobierane z chmury publicznej i wewnętrznej chmury prywatnej lub, innymi słowy, z chmury hybrydowej, która łączy te dwa elementy. W kolejnych rozdziałach skoncentrowano się na sposobie zarządzania tymi zasobami w celu spełnienia wymagań informatycznych organizacji.

Uwaga: Profil wdrożenia jest najbardziej odpowiedni dla średnich i dużych przedsiębiorstw, które już poczyniły znaczne wewnętrzne inwestycje w IT i prawdopodobnie utrzymają niektóre z tych zasobów, włączając usługi IT od zewnętrznego dostawcy chmury. W przypadku przedsiębiorstw, które zlecają całość IT dostawcy chmury, profil wdrożenia obejmowałby tylko zasoby zewnętrzne. W obu przypadkach istotne są kluczowe technologie wspomagające VPC.

Wirtualne centra danych i aplikacje

Ogólnym celem organizacji w zakresie korzystania z IT jest realizacja określonych procesów biznesowych opartych na informacjach, przy jednoczesnym zachowaniu zgodności z obowiązującymi przepisami i regulacjami oraz optymalizacja stosunku kosztów do korzyści. Niezależnie od tego, czy jest wdrażany za pomocą przetwarzania w chmurze, czy z konwencjonalnym IT, wysokopoziomowe cele IT organizacji są takie same. Obietnica przetwarzania w chmurze polega na tym, że z biegiem czasu organizacje mogą osiągnąć te cele przy coraz lepszym stosunku kosztów do korzyści

Wirtualne centra danych

W konwencjonalnym IT centra danych zapewniają wygodny sposób organizowania zasobów w lokalnie połączone pule. Lokalizacja zapewnia możliwość wspólnego nadzoru fizycznego i poprawy wydajności sieci pomiędzy zasobami w centrum danych. W efekcie centrum danych może być postrzegane jako lokalny kontener zasobów IT, którymi można zarządzać razem z perspektywy zasobów, bezpieczeństwa i/lub informacji. Wirtualizacja, jako ogólny paradygmat, izoluje zasoby i funkcje od podstawowej implementacji fizycznej, co w konsekwencji daje korzyść polegającą na tym, że zasoby wirtualne mogą być dynamicznie przydzielane do organizacji bez obaw (przez organizację) o podstawowe implikacje

fizyczne. Co więcej, wirtualne zasoby można łatwo migrować z jednego środowiska fizycznego do drugiego – na przykład między centrami danych organizacji a centrami danych obsługiwanymi przez dostawcę chmury. Z tej perspektywy zasoby wirtualne „w chmurze" są w zasadzie niezależne od lokalizacji i kontenera. Jednak z tych samych powodów, co w konwencjonalnym IT, kontenery i atrybuty typu lokalizacji mogą odgrywać ważną rolę w praktyce, ponieważ organizacje będą nadal wymagać korzyści w zakresie wydajności, jakie niesie ze sobą lokalizacja, i wygodnie będzie zarządzać zasobami jako zestawami. W związku z tym, tak jak centra danych są podstawową jednostką zarządzania wysokiego poziomu w konwencjonalnym IT, można oczekiwać, że wirtualne centra danych – pierwsza kluczowa technologia umożliwiająca VPC - będą podstawową jednostką zarządzania zasobami na wysokim poziomie.

Wirtualne centrum danych (VDC). Pula zasobów wirtualnych, które pojawiają się pod względem wydajności, są połączone lokalnie i mogą być zarządzane jako zestaw.

Ze względów praktycznych VDC będzie zazwyczaj wdrażany w oparciu o pojedyncze fizyczne centrum danych; w przeciwnym razie pozorna łączność lokalna byłaby trudna do osiągnięcia (chociaż istnieją najnowsze technologie sieciowe o wysokiej wydajności, które obejmują fizyczne centra danych). Ograniczenie jest oczywiście tylko w jednym kierunku: dane fizyczne centrum danych może obsługiwać więcej niż jeden VDC. Ponadto centrum danych obsługiwane przez dostawcę chmury publicznej może oferować centra wirtualne wielu organizacjom lub odtąd dzierżawcom, więc bazowe środowisko obliczeniowe jest wielodostępne. Oprócz łączności lokalnej umieszczenie zasobów w określonej lokalizacji może oferować korzyści geograficzne, takie jak bliskość niektórych użytkowników lub zasobów energetycznych, lub różnorodność obowiązujących przepisów i regulacji. Umieszczenie zasobów w wielu niezależnych lokalizacjach może również pomóc w poprawie odporności. Takie aspekty geograficzne mogą zostać „zwirtualizowane" przez zarządzanie oparte na polityce (patrz sekcja 3.4 poniżej). VDC (i/lub jego zasoby) zostałyby wybrane tak, aby osiągnęły pożądane właściwości, z rzeczywistą lokalizacją pozostawioną do wdrożenia (chociaż niektóre właściwości mogą być osiągalne tylko w określonej lokalizacji geograficznej). Ponadto centra danych, podobnie jak fizyczne centra danych, mogą różnić się pod względem oferowanych możliwości, takich jak:

1. Rodzaje obsługiwanych zasobów wirtualnych;

2. Koszt, wydajność, bezpieczeństwo i inne atrybuty tych zasobów (i ogólnie VDC), w tym rodzaje wykorzystywanej energii; oraz

3. Konkretne zasoby, które już są obecne i których uzyskanie w innym miejscu może być niewygodne, takie jak duże zbiory danych lub wyspecjalizowane funkcje obliczeniowe.

Zamiast przedstawiać wygląd fizycznego centrum danych takim, jakim jest w rzeczywistości, abstrakcja VDC może pokazać centrum danych takim, jakie powinno być. W efekcie VDC daje możliwość uproszczonego, ujednoliconego zarządzania z punktu widzenia korzystającej z niego organizacji. Biorąc pod uwagę VDC jako podstawową jednostkę zarządzania, podstawowy profil implementacji VPC może być dalej dopracowany jako taki, w którym zasoby wirtualne są zorganizowane w kombinację

• Jeden lub więcej prywatnych VDC hostowanych przez dostawcę chmury; oraz

• Jeden lub więcej wewnętrznych, prywatnych VDC hostowanych przez organizację

VDC dostawcy chmury opierałyby się na skalowalnych partycjach publicznych centrów danych dostawcy chmury; wewnętrzne wirtualne dyski twarde mogą być po prostu wirtualizacją istniejących centrów danych organizacji lub być może ponownie skalowalnymi partycjami. W obu przypadkach modyfikator prywatny jest niezbędny: aby wynikowy VPC wyglądał tak, jakby był obsługiwany

wyłącznie przez organizację, komponenty VDC również muszą być takie. W ten sposób budowanie VPC rozkłada się na problem budowy prywatnego VDC lub, rozszerzając definicję, puli wirtualnych zasobów, które wydają się być lokalnie połączone i obsługiwane przez pojedynczą organizację. Konkretne tłumaczenie między prywatnym VDC a podstawowymi zasobami fizycznymi jest oczywiście kwestią implementacji, ale kilka technologii z pewnością będzie odgrywać kluczową rolę, w tym oczywiście wirtualizacja i zarządzanie zasobami, a także, być może, szyfrowanie w jakiejś formie (Uwaga 3). Dzięki tej pierwszej technologii wspomagającej organizacja korzystająca z VPC będzie miała do dyspozycji pewną liczbę prywatnych VDC lub kontenerów, w których może wdrażać zasoby, a także możliwość uzyskania dodatkowych VDC w razie potrzeby. Sposób wykorzystania tych pojemników jest przedmiotem następnej technologii wspomagającej.

Uwagi

1. Przetwarzanie w chmurze można realizować bez metafory centrum danych, na przykład w miejscach, w których łączność lokalna nie jest istotna, takich jak aplikacje o wysokim stopniu dystrybucji lub peer-to-peer. Skupiamy się tutaj na typowych przypadkach użycia w przedsiębiorstwie, które są oparte na centrach danych.

2. Wirtualizacja, co do zasady, daje wrażenie prywatności w tym sensie, że jeśli wszyscy najemcy wchodzą w interakcję tylko poprzez abstrakcję VDC, to z definicji nie mają dostępu do swoich zasobów (zakładając oczywiście, że w fizycznym odpowiedniku, którego wygląd jest przedstawione, nie mogą tego zrobić). Tak więc sama wirtualizacja serwerów, sieci, pamięci masowej itp. jest prawdopodobnie wystarczająca do zbudowania VDC (o ile wydaje się, zarządzanie zasobami jest również potrzebne do obsługi harmonogramów itp.).

Z tą pozycją wiążą się dwa główne problemy. Po pierwsze, mogą istnieć ścieżki poza abstrakcją, za pomocą których strony mogą wchodzić w interakcje z bazowymi zasobami. Przynajmniej operator infrastruktury będzie miał taki dostęp, zarówno fizyczny, jak i administracyjny. Po drugie, w abstrakcji mogą istnieć ścieżki, które przypadkowo umożliwiają taką interakcję, czy to z powodu błędów, czy też kanałów bocznych, które nie są całkowicie ukryte. Wprowadza to możliwość złośliwych aplikacji lub złośliwych aplikacji, które są skierowane do innych dzierżawców korzystających z tego samego publicznego środowiska komputerowego. Kartografia w chmurze i techniki wycieku informacji między maszynami wirtualnymi Ristenpart, Tromer, Shacham i Savage (2009) to najnowsze przykłady. Warto zauważyć, że konwencjonalne centra danych radzą sobie już z podobnymi lukami w zabezpieczeniach, stosując szereg kontroli bezpieczeństwa, od szyfrowania po analizę behawioralną. Różnica w przetwarzaniu w chmurze polega nie tyle na charakterze luk, ile na liczbie potencjalnych przeciwników „w obozie". Podstawowy i adaptacyjny zestaw kontroli bezpieczeństwa będzie niezbędny dla abstrakcji, niezawodnie, aby zachować swoje gwarancje, podczas gdy aplikacje implementują dodatkowe kontrole ponad abstrakcją, tak jak gdyby działały bezpośrednio w infrastrukturze fizycznej. Dobrym przykładem takiej dodatkowej kontroli jest VPN (widoczny dla aplikacji w modelu private VDC). Zaufane przetwarzanie może również odgrywać rolę w prywatnych wirtualnych centrach danych, zapewniając podstawę zaufania, w odniesieniu do której dzierżawcy mogą weryfikować integralność swoich zasobów. Integracja zaufanego przetwarzania i wirtualizacji jest bardziej szczegółowo badana w projektach takich jak Terra autorstwa Garfinkel, Pfaff, Chow, Rosenblum oraz Boneh and Daonity (obecnie kontynuowane jako Daoli).

Aplikacje wirtualne

Procesy oparte na informacjach w konwencjonalnym IT są realizowane przez różne aplikacje wymagające interakcji między zbiorami zasobów. Zasoby obsługujące daną aplikację mogą działać w jednym centrum danych lub w wielu centrach danych, w zależności od wymagań aplikacji. Kontynuując

analogię z konwencjonalnym IT, można oczekiwać, że aplikacje wirtualne - druga kluczowa technologia wspomagająca - będą podstawową, wysokopoziomową jednostką rozmieszczania zasobów:

Aplikacja wirtualna. Zbiór połączonych zasobów wirtualnych wdrożonych w jednym lub kilku wirtualnych centrach danych, które wdrażają konkretną usługę IT.

Aplikacja wirtualna składa się nie tylko z maszyn wirtualnych, które implementują funkcjonalność oprogramowania aplikacji, ale także z innych zasobów wirtualnych potrzebnych do realizacji aplikacji, takich jak sieci wirtualne i wirtualna pamięć masowa. W tym sensie aplikacja wirtualna rozszerza koncepcję urządzenia wirtualnego, która obejmuje kompletny stos oprogramowania (maszyny wirtualne i system operacyjny z interfejsami sieciowymi) realizujący pojedynczą usługę, obejmując zestaw usług obsługujących aplikację. Tak jak VDC może pokazać centrum danych w bardziej idealnej formie, wirtualna aplikacja może prezentować wygląd aplikacji tak, jak powinna być. Obecnie zabezpieczenia, zarządzanie zasobami i zarządzanie informacjami są zazwyczaj wymuszane przez system operacyjny i stos aplikacji, co czyni je skomplikowanymi i kosztownymi we wdrażaniu i utrzymaniu. Dzięki uproszczonemu, ujednoliconemu zarządzaniu zapewnianemu przez abstrakcję aplikacji wirtualnych i enkapsulację komponentów aplikacji w kontenerach maszyn wirtualnych, kontener aplikacji wirtualnej staje się nowym punktem kontrolnym dla spójnego zarządzania aplikacjami. Zamiast organizować każdy zasób z osobna, organizacja może działać wspólnie na pełnym zestawie, osiągając ekwiwalent udostępniania „jednym kliknięciem", włączania zasilania, tworzenia migawek, tworzenia kopii zapasowych i tak dalej. Główny profil implementacji VPC może być teraz ponownie dopracowany jako taki, w którym aplikacje wirtualne składające się z zasobów wirtualnych działają na jednym lub większej liczbie wirtualnych centrów danych. Open Virtualization Format (OVF, 2009) niedawno ustandaryzowany przez grupę zadaniową ds. zarządzania danymi oferuje wygodny sposób określania kolekcji maszyn wirtualnych. Za pomocą metadanych można również wyrazić połączenia między tymi maszynami i ich zależności od innych zasobów, takich jak sieci i pamięć masowa, obsługując pełne aplikacje wirtualne, jak zdefiniowano tutaj. Oprócz kilku produktów komercyjnych, specyfikacja jest również obsługiwana w projekcie open source Open-OVF (open-ovf.sourceforge.net). Organizacja korzystająca z VPC z dwoma pierwszymi wprowadzonymi obecnie technologiami prorozwojowymi będzie mogła wykorzystywać swoje prywatne wirtualne centra danych do wdrażania aplikacji wirtualnych. Kolejne technologie wspomagające dotyczą umowy między tymi aplikacjami a VPC, która umożliwia automatyczny montaż komponentów w celu spełnienia celów informatycznych organizacji przy jednoczesnym zachowaniu elastyczności optymalizacji.

Notatka

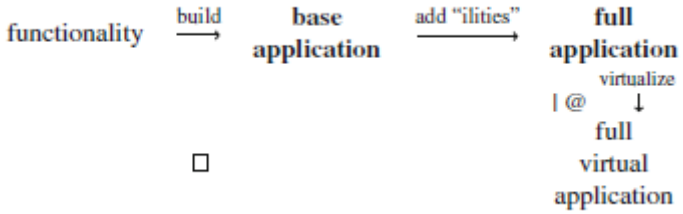
1. Wzajemne oddziaływanie między wirtualnymi centrami danych i aplikacjami wirtualnymi jest ważnym aspektem spełniania wymagań informatycznych organizacji w przypadku VPC, które w niektórych przypadkach zależą od (prawdopodobnie względnej). Tak więc, oprócz podstawowej roli aplikacji wirtualnych w umożliwianiu przenoszenia między chmurami, aplikacje wirtualne mogą być również postrzegane jako sposób na umożliwienie efektywnego wdrożenia w chmurze poprzez opisanie pożądanych relacji między zasobami wirtualnymi.

Zarządzanie oparte na zasadach

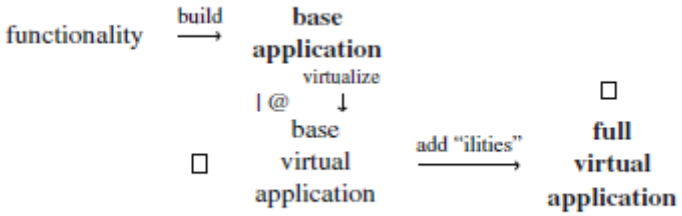
Z biegiem czasu VPC zostanie zapełniony zasobami obsługującymi aplikacje wirtualne działające na różnych VDC. Zasoby te zostaną wdrożone i zgromadzone z ostatecznym zamiarem spełnienia wymagań informatycznych organizacji. To jest istota „umowy", formalnej lub innej, pomiędzy organizacją a VPC. Rolę takiej umowy można rozpatrywać w dwóch częściach: ujęcie jej warunków aby ćwiczyć i sprawdzać, czy praktyka jest poprawna

Wdrażanie oparte na zasadach

Rozważ organizację, która chce wdrożyć aplikację e-commerce z określonymi celami dotyczącymi bezpieczeństwa, wydajności i ciągłości biznesowej. W konwencjonalnym centrum danych ta aplikacja może być zaimplementowana jako połączenie zasobów, zaczynając od serwera WWW i bazy danych. Zapora ogniowa zostałaby dodana, aby spełnić cele bezpieczeństwa, oraz moduł równoważenia obciążenia, aby przypisać transakcje do dodatkowych serwerów internetowych w razie potrzeby, aby spełnić cele wydajnościowe. Aby zrealizować cele związane z ciągłością działania, druga instancja tych komponentów może zostać umieszczona w innym centrum danych, skoordynowana z pierwszą przez menedżera ciągłości działania. Załóżmy dalej, że organizacja chce również wdrożyć aplikację do zarządzania relacjami z klientami (CRM) o podobnych celach usługowych. Ta aplikacja może być również zaimplementowana jako połączenie serwerów internetowych, baz danych, zapór ogniowych, systemów równoważenia obciążenia itd. w dwóch centrach danych. Teraz zastanów się, co się stanie, gdy organizacja zdecyduje się wdrożyć te aplikacje w VPC (w ramach jakiejś „umowy", zgodnie z powyższymi komentarzami). Zgodnie z modelem w sekcji 3.3.2, każda aplikacja zostanie wdrożona jako zbiór zasobów wirtualnych. W ten sposób VPC hostowałby kombinację zestawów zasobów dla dwóch aplikacji: dwa zestawy wirtualnych serwerów WWW, dwie wirtualne bazy danych, dwie zapory ogniowe, dwa systemy równoważenia obciążenia itd., a ta kolekcja byłaby powtarzana w dwóch centrach wirtualnych. Wdrażanie aplikacji w VPC, jak właśnie opisano, ma pewne zalety, takie jak dynamiczna alokacja zasobów i ekonomia skali. Jednak taki proces to tak naprawdę tylko migracja komponentów z jednego środowiska do drugiego lub coś, co można by nazwać dosłowną wirtualizacją. Rozrost infrastruktury w centrum danych przekłada się bezpośrednio na rozrost wirtualny, z taką samą liczbą komponentów do zarządzania jak wcześniej, po prostu skonsolidowanych na mniejszej liczbie serwerów i zorganizowanych w bardziej elastyczny sposób. Środowiska przetwarzania w chmurze mogą poprawić tę sytuację, organizując komponenty i możliwości w przeszukiwalne listy wirtualnych aplikacji i zasobów, które można łatwo wdrożyć. Wybierając usługi z katalogu ofert i inwentarza, zamiast narzucać całkowicie unikalne wybory, organizacja może skorzystać z optymalizacji, które dostawca chmury mógł już wprowadzić. Dobrym przykładem może być system równoważenia obciążenia. Zamiast każdej aplikacji wnoszącej swój własny system równoważenia obciążenia, VPC oferowałby jeden z nich do użytku przez wiele aplikacji. Gdy projektant aplikacji wie, że równoważenie obciążenia będzie dostępne, nie musi już określać aplikacji wirtualnej jako kombinacji, powiedzmy, dwóch serwerów WWW i modułu równoważenia obciążenia. Zamiast tego wirtualna aplikacja może być wyrażona jako połączenie pojedynczego serwera WWW (i innych komponentów funkcjonalnych) oraz zasady, zgodnie z którą VPC powinien tworzyć dodatkowe instancje serwera WWW i równoważyć transakcje między nimi, aby utrzymać określony poziom wydajności. Ta zasada ma dodatkową zaletę, że aplikacja może być automatycznie skalowana poza dwa wystąpienia pierwotnie określone w dosłownym odpowiedniku wersji centrum danych. Równoważenie obciążenia jest jednym z przykładów ogólnego wzorca: aplikacje są projektowane jako połączenie funkcjonalności i cech związanych z umowami o poziomie usług (SLA). Te cechy, czasami nazywane również „ilities" (od wspólnego przyrostka skalowalności, dostępności itp.), są generalnie implementowane z dość podobnymi komponentami w różnych aplikacjach, takich jak systemy równoważenia obciążenia, zapory ogniowe, menedżery ciągłości biznesowej i tak dalej. Są więc naturalnymi kandydatami do usług obsługujących wiele aplikacji w VPC. Prosta formuła ilustruje zarówno wzór, jak i problem. Typową aplikację konstruuje się najpierw poprzez zbudowanie aplikacji bazowej, która spełnia pewne wymagania funkcjonalne, a następnie dodanie „uprawnień" dotyczących tych niefunkcjonalnych. Powstała pełna aplikacja jest następnie zwirtualizowana i wdrażana w VPC. Ten wzór można podsumować w następujący sposób:



Biorąc pod uwagę tylko pełną aplikację wirtualną, VPC prawdopodobnie będzie miał problem z rozpoznaniem „uwarunkowań", a tym samym z zarządzaniem nimi lub optymalizacją ich dostarczania, tak samo jak trudno jest zoptymalizować kod obiektowy bez oryginalnego źródła. Jednak biorąc pod uwagę część tego oryginalnego źródła, VPC będzie miał znacznie więcej okazji do dodania wartości. W związku z tym preferowanym modelem wdrażania aplikacji w VPC jest dodawanie przez środowisko komputerowe „ilities" w ramach wdrażania. Wzór wygląda teraz następująco:



„Usługi" można dodać, konfigurując podstawową aplikację wirtualną lub wdrażając dodatkowe usługi. Zgodnie z modelem VDC w sekcji 3.3.2, polityka może być również realizowana zgodnie z rozmieszczeniem zasobów wirtualnych w określonych VDC, np. tam, gdzie wymagana jest łączność lokalna, bliskość niektórych użytkowników, niezależność itp. Paradygmat można podsumować jako trzecią kluczową technologię wspomagającą, wdrożenie oparte na zasadach:

Wdrożenie oparte na zasadach. Montaż komponentów aplikacji w środowisku komputerowym zgodnie z predefiniowanymi celami polityki. Chociaż wdrażanie oparte na zasadach może być również stosowane w innych typach chmur (a także w centrach danych), technologia ta jest szczególnie ważna dla VPC ze względu na ich główny cel użycia: organizacje, które muszą spełniać dobrze zdefiniowane cele IT. Przesunięcie wprowadzania niektórych funkcji zasad z programowania do wdrażania niekoniecznie ułatwia wdrażanie, a w rzeczywistości może je utrudnić, jak zauważają Matthews, Garfinkel, Hoff i Wheeler, ze względu na liczbę potencjalnie zaangażowanych interesariuszy i administratorów. Automatyzacja jest niezbędna do uproszczenia wdrażania, a dobrze zdefiniowany język do wyrażania zasad jest niezbędny do automatyzacji. Oddzielenie „ilities" od funkcjonalności jest zatem konieczne, ale niewystarczające. Ponadto „ilities" muszą być wyrażone jako zasady odczytywalne maszynowo, które może wdrożyć środowisko obliczeniowe. W Matthews et al. takie zasady mają formę Umowy na Maszynę Wirtualną, zdefiniowanej jako:

Umowa na maszynę wirtualną to złożona deklaratywna specyfikacja prostego pytania, czy ta maszyna wirtualna powinna być dopuszczona do działania, a jeśli tak, to czy obecnie działa z akceptowalnymi parametrami?

Specyfikację taką jak OVF można wykorzystać do przenoszenia umów i innych informacji dotyczących zasad, tak aby podróżowały one wraz z maszynami wirtualnymi i, bardziej ogólnie, aplikacjami

wirtualnymi, do których mają zastosowanie warunki. Dzięki zautomatyzowanemu wdrożeniu opartemu na zasadach, organizacja jest w stanie określić w VPC swoje oczekiwania w zakresie bezpieczeństwa, wydajności i innych umów SLA, a VPC może następnie automatycznie zoptymalizować swoje operacje pod kątem tych celów. Wyrażenie wojskowe „Dostajesz to, co sprawdzasz, a nie to, czego oczekujesz", motywuje wyzwanie, na które zmierzy się następna technologia wspomagająca: jak sprawdzić, czy warunki umowy z VPC są rzeczywiście spełnione.

Zgodność z zasadami

W dowolnym środowisku komputerowym, które organizacja zdecyduje się wdrożyć aplikację, organizacja będzie potrzebować dowodów, że aplikacja działa zgodnie z przeznaczeniem. Dowody te służą zarówno zapewnieniom własnym organizacji, jak i audytorom lub klientom. Nawet jeśli nie jest to złośliwe, optymalizacje środowiska mogą jedynie przybliżać zamierzony wynik. Cele polityki są szczególnie trudne do osiągnięcia w środowisku wielu aplikacji ze względu na możliwość rywalizacji o zasoby. Na przykład fizyczny zasób obliczeniowy może niezawodnie spełniać cele wydajności obliczeniowej dla jednej obsługiwanej aplikacji, ale gdy ten zasób wchodzi w interakcję z innym zasobem, obecność ruchu sieciowego z innych aplikacji może sprawić, że wydajność komunikacji będzie nieprzewidywalna. Z tego powodu schematy rezerwacji sieci i podobne podejścia do pamięci masowej odgrywają ważną rolę w spełnianiu umów SLA. Mogą również istnieć możliwości dla różnych zastosowań, zgodnie z projektem, do działania w sposób uzupełniający, który zmniejsza rywalizację. Środowisko obliczeniowe dla wielu dzierżawców, takie jak chmura publiczna hostująca VPC dla wielu organizacji, wprowadza kolejne komplikacje. Podobnie jak w przypadku każdej usługi internetowej, najemcy mają wpływ na siebie nawzajem, co może być nieprzewidywalne. Ponieważ nie ma bezpośredniej możliwości negocjacji między różnymi najemcami w odniesieniu do bazowego środowiska obliczeniowego (w zasadzie nie mogą się nawet wykryć), wszelkie spory muszą być rozstrzygane przez samego dostawcę chmury. Cele różnych najemców niekoniecznie są ze sobą zbieżne, więc oprócz podstawowej rywalizacji o zasoby, może wystąpić również rywalizacja między strategiami optymalizacji. Potencjał zakłóceń jest kolejną silną motywacją do umieszczania usług zasad w środowisku komputerowym, a nie w poszczególnych aplikacjach. Wreszcie cele najemców niekoniecznie są zgodne z celami dostawcy chmury publicznej. Chociaż obsługa klientów będzie prawdopodobnie pierwszym priorytetem odnoszącego sukcesy dostawcy chmury, pozostawanie w biznesie to kolejna rzecz i istnieje wyraźna motywacja do wdrażania dalszych optymalizacji, które obniżają koszty dostawcy niekoniecznie zwiększając świadczenia dla któregokolwiek z lokatorów (Uwaga 1). Biorąc pod uwagę trudność w doskonałym spełnieniu wymagań zasad w wielu aplikacjach i dzierżawcach, szczególnie ważne staje się, aby VPC dostarczał, a dzierżawca otrzymywał pewne informacje o stopniu spełnienia tych wymagań lub nie, w różnych momentach . Prowadzi to do czwartej kluczowej technologii wspomagającej, zgodności z polityką.

Zgodność z polityką. Weryfikacja, czy aplikacja lub inny zasób IT działa zgodnie z predefiniowanymi celami polityki

Ze względu na oddzielenie „ilities" od opartej funkcjonalności, uzasadnione jest oczekiwanie, że sama zgodność z zasadami zostanie ostatecznie uznana za po prostu kolejną usługę dodaną do aplikacji po wdrożeniu w VPC (Uwaga 2). Taka zdolność idzie w parze z wdrażaniem opartym na zasadach: VPC będzie znacznie łatwiej zebrać odpowiednie dowody z zasobów, które już zgromadził, mając na uwadze cele polityki, niż odkrycie celów, zasobów i dowodów po fakcie. Jeśli chodzi o same dowody, dokładnie w celu oceny wydajności, wiele zasobów IT jest wyposażonych w dzienniki aktywności, które rejestrują transakcje i inne zdarzenia. Na przykład fizyczny router sieciowy może śledzić źródło, miejsce docelowe, rozmiar, znacznik czasu i inne metadane przesyłanych pakietów (lub nie może przesłać); fizyczna macierz pamięci może rejestrować podobne informacje o blokach, które odczytuje i zapisuje.

Dzięki odpowiednim interfejsom środowisko wirtualne może wykorzystać te funkcje w celu zebrania dowodów zgodności z zasadami. Na przykład tagowanie we/wy osadza wirtualne identyfikatory aplikacji jako metadane w żądaniach fizycznych, z tą korzyścią, że identyfikatory są następnie automatycznie dołączane do dzienników aktywności w celu późniejszej analizy przez środowisko wirtualne z minimalnym wpływem na wydajność (Uwaga 3). Zbiór dzienników systemowych z fizycznych zasobów obliczeniowych, sieciowych i pamięciowych, zawierających informacje o wirtualnych aplikacjach i zasobach oraz ich działaniach, stanowi zbiór informacji, z którego można uzyskać dowody zgodności z zasadami. Ten zestaw informacji, kluczowany identyfikatorami aplikacji wirtualnych i powiązanymi ilościami, umożliwia rozproszony kontekst aplikacji i korelację — w efekcie wirtualny widok aktywności aplikacji wirtualnej w całym VPC. Konstruowanie takiego widoku, zwłaszcza z heterogenicznych, nieustrukturyzowanych dzienników systemowych, które zostały zaprojektowane tylko dla lokalnej widoczności, oraz interfejsów zarządzania, które były przeznaczone tylko do lokalnego sterowania, zależy od piątej i ostatniej technologii umożliwiającej, takiej, która odpowiada na pytanie: Jak zapewnić wszystkie te informacje razem inteligentnie?

Integracja zarządzania usługami

Wirtualne centra danych, pierwsza z technologii wspomagających, mogą być postrzegane jako zapewniające izolację, która oddziela wirtualne zasoby jednej organizacji od zasobów innych organizacji oraz od leżących u ich podstaw zasobów fizycznych. Drugie aplikacje wirtualne gromadzą te zasoby w oddzielnie zarządzanych jednostkach. Wdrażanie oparte na zasadach i zgodność z zasadami, trzecia i czwarta, oferują środki kontroli i weryfikacji działania aplikacji wirtualnych w centrach VDC. Wszystkie cztery opierają się na piątej technologii: bardziej podstawowym fundamencie, który łączy podstawowe granice, zorientowanym na bezproblemową integrację. Przypomnijmy pierwotny profil wdrożenia dla VPC: hybryda wewnętrznej chmury prywatnej i chmury publicznej. VPC zapewnia wygląd pewnej liczby VDC, niektóre pobierane z chmury wewnętrznej, niektóre z chmury publicznej. Ta VPC jest zasadniczo postrzegana jako bezproblemowa, tak jak wygląda (ekspozycja wielu VDC jest cechą architektoniczną). W związku z tym możemy mówić o wdrożeniu aplikacji w VPC, zbieraniu dowodów z VPC i tak dalej, bez względu na fakt, że wdrożenie i zbieranie ostatecznie obejmuje interakcje z zasobami fizycznymi, a co ważniejsze, że te zasoby fizyczne są w wielu centrach danych obsługiwanych przez co najmniej dwa różne podmioty. Podstawowym wyzwaniem dla zadowolenia z zarządzania opartego na zasadach w VPC jest umożliwienie takiej bezproblemowej interakcji między komponentami zarządzania zasobami, usługami i zasadami: ponad granicami infrastruktury centrum danych, a następnie ponad granicami sfederowanych dostawców usług. Takie mosty nie są łatwe do zbudowania, ponieważ różne interfejsy zarządzania - takie jak lokalne dzienniki - zostały zaprojektowane do oddzielnych celów. W warstwie fizycznej mogą używać różnych nazw dla tej samej jednostki lub funkcji, stosować niekompatybilne systemy uwierzytelniania i kontroli dostępu oraz wyrażać te same warunki na różne sposoby. Informacje, których potrzebuje organizacja i VPC, są dostępne, ale nie są od razu przydatne bez tłumaczenia. Ponadto translacja ta nie polega po prostu na konwersji między formatami, ale w rzeczywistości na wirtualizacji interfejsów do metadanych zarządzania ponad granicami podstawowego elementu zarządzania. Piąty i ostatni klucz umożliwiający technologię, integrację zarządzania usługami, rozwiązuje to ostatnie wyzwanie:

Integracja zarządzania usługami. Tłumaczenie heterogenicznych informacji zarządczych z oddzielnych domen na ogólny, logiczny i praktyczny widok

Integracja usługowo-zarządzająca jest szczególnym przypadkiem szerszej technologii integracji informacji, która podobnie dotyczy tłumaczenia federacji ogólnych informacji z wielu dziedzin. Szczególny przypadek VPC dotyczy w szczególności federacji trzech rzeczy: (1) podstawowej infrastruktury w jednym wirtualnym środowisku obliczeniowym, (2) tożsamości współdziałających z

zasobami w środowisku oraz (3) informacji o zasobach. Ze swej natury integracja zarządzania usługami dla VPC jest podatna na paradygmat zdarzeń, w którym podstawową jednostką informacji jest zdarzenie opublikowane przez jeden podmiot w systemie i wykorzystane przez inny. Ten paradygmat jest dobrym rozwiązaniem dla menedżera ds. zgodności z zasadami, który jest zainteresowany zawartością wielu dzienników fizycznych w miarę gromadzenia dowodów. Zapewnia również menedżerowi wdrażania bieżący widok zasobów bazowych w miarę ich ciągłych zmian. Co więcej, separacja architektoniczna między wydawcą a subskrybentem umożliwia fizyczne oddzielenie i dystrybucję uczestniczących elementów w granicach centrum danych i federacji chmury. Pośrednictwo między wydawcą a konsumentem można osiągnąć za pomocą systemu przesyłania wiadomości. Jako dedykowana warstwa komunikacyjna dla zdarzeń, taki system zapewnia sfederowaną „płytę bazową" dostarczania informacji, która łączy wiele domen zarządzania (np. wewnętrzne centra danych, centra danych dostawców chmury) w jedną architekturę zorientowaną na usługi, przekładającą się tam i z powrotem między języki bezpieczeństwa i zarządzania z różnych dziedzin. Zdarzenia opublikowane w jednej domenie można wykorzystać w innej zgodnie z różnymi regułami subskrypcji lub filtrami; Menedżer ds. zgodności z zasadami dla konkretnego dzierżawcy, na przykład, będzie zainteresowany (i powinien wiedzieć tylko o) wydarzeniach związanych z wirtualnymi aplikacjami tego dzierżawcy. System przesyłania wiadomości może implementować swoje tłumaczenia za pomocą zestawu adapterów, dzięki zrozumieniu powiązań między tożsamościami i zdarzeniami w różnych domenach. Uczenie się tych połączeń przez system może nastąpić automatycznie lub może wymagać ręcznej interwencji, a w niektórych przypadkach może wymagać uzupełnienia o znaczną ilość obliczeń, na przykład w celu wyszukania skorelowanych zdarzeń w różnych domenach. W środowisku chmury obliczeniowej zasoby do takich obliczeń nie będą trudne do znalezienia. (Jak zrównoważyć wykorzystanie zasobów w celu zwiększenia efektywności całego środowiska w porównaniu z przydzielaniem ich bezpośrednio do najemców, to kolejne dobre pytanie do dalszej eksploracji.)

Wnioski

Ten artykuł rozpoczął się od prostego założenia, że przetwarzanie w chmurze staje się coraz ważniejsze dla organizacji, jednak, jak w przypadku każdego nowego paradygmatu, stoi przed pewnymi wyzwaniami. Jednym z wyzwań jest zdefiniowanie najbardziej odpowiedniego do przyjęcia typu przetwarzania w chmurze. Jako preferowany profil wdrożenia oferowana jest wirtualna chmura prywatna zbudowana z zasobów IT zarówno z własnych wewnętrznych centrów danych organizacji, jak i publicznych centrów danych dostawcy chmury. Aby zapewnić prywatność, czyli sprawiać wrażenie, że chmura jest obsługiwana wyłącznie dla organizacji, potrzebne są również pewne dodatkowe zabezpieczenia. Kolejnym wyzwaniem jest dobre wykorzystanie zbiorowych zasobów. Dosłowny rodzaj wirtualizacji, w którym aplikacje są w zasadzie przenoszone z centrum danych do VPC, przyniósłby pewne korzyści, ale większy potencjał wynika z umożliwienia samej VPC optymalizacji montażu aplikacji. Punktem wyjścia do tego postępu jest oddzielenie funkcjonalności od polityki w ramach specyfikacji aplikacji wirtualnej, tak aby wymagania polityki mogły być spełnione w sposób wspólny, a zatem zoptymalizowany przez VPC. Wspólne zarządzanie zasadami umożliwia również VPC weryfikację przestrzegania zasad. Wreszcie, infrastruktura informacyjna stanowi podstawę realizacji VPC. Rzeczywiście, wirtualizacja polega na przekształcaniu zasobów w informacje. Im lepiej VPC może komunikować się z tymi informacjami, wyłaniającymi się z cienia przeszłości prywatnych centrów danych i teraźniejszości chmury publicznej, tym skuteczniej organizacje mogą realizować obietnicę przyszłości wirtualnej chmury prywatnej.