Rola sieci w przetwarzaniu w chmurze

Wstęp

Zbieg postępu technologicznego i rozwoju biznesu w szerokopasmowym Internecie, usługach sieci Web, systemach komputerowych i oprogramowaniu aplikacyjnym w ciągu ostatniej dekady stworzył idealną burzę dla przetwarzania w chmurze. „Model chmury" dostarczania i wykorzystywania funkcji IT jako usług ma na celu fundamentalną transformację branży IT i zrównoważenie wzajemnych relacji między użytkownikami końcowymi, IT dla przedsiębiorstw, firmami programistycznymi i dostawcami usług w ekosystemie IT. W centrum modelu dostarczania i konsumpcji w chmurze znajduje się sieć. Sieć służy jako łącznik pomiędzy użytkownikami końcowymi korzystającymi z usług w chmurze a centrami danych dostawcy świadczącymi usługi w chmurze. Ponadto w dużych centrach danych w chmurze dziesiątki tysięcy węzłów obliczeniowych i pamięci masowej są połączone siecią centrum danych, aby zapewnić jednofunkcyjną usługę w chmurze. Jak architektury sieciowe wpływają na przetwarzanie w chmurze? Jak rozwinie się architektura sieciowa, aby lepiej wspierać przetwarzanie w chmurze i dostarczanie usług w chmurze? Jaka jest rola sieci w bezpieczeństwie, niezawodności, wydajności i skalowalności przetwarzania w chmurze? Czy sieć powinna być głupim potokiem transportowym, czy inteligentnym stosem, który uwzględnia obciążenie chmury? Ta część koncentruje się na aspekcie sieciowym w chmurze obliczeniowej i zapewnia wgląd w te pytania. Rozdział jest zorganizowany w następujący sposób. Omawiamy różne modele wdrażania usług w chmurze - chmury prywatne, chmury publiczne i chmury hybrydowe - oraz ich unikalne wymagania architektoniczne w sieci. Skupiamy się na modelu chmury hybrydowej i omawiamy możliwości biznesowe związane z chmurami hybrydowymi oraz architekturą sieciową umożliwiającą chmury hybrydowe. Pod wieloma względami architektura sieci chmury hybrydowej obejmuje cechy sieci zarówno dla chmur publicznych, jak i prywatnych. Omawiamy nasze wnioski i wskazujemy kierunki przyszłych prac nad architekturami sieciowymi obsługującymi chmurę.

Modele wdrażania w chmurze i sieć

Branżę IT przyciąga prostota i opłacalność reprezentowana przez koncepcję przetwarzania w chmurze, zgodnie z którą możliwości IT są dostarczane jako usługi w skalowalny sposób przez Internet ogromnej liczbie zdalnych użytkowników. Podczas gdy puryści wciąż debatują nad dokładną definicją przetwarzania w chmurze, branża IT postrzega przetwarzanie w chmurze - nowy model biznesowy - jako nowy sposób rozwiązywania dzisiejszych wyzwań biznesowych. Ankieta przeprowadzona przez Olivera Wymana w listopadzie 2008 roku z udziałem kadry kierowniczej z różnych przedsiębiorstw określiła „redukcja kosztów kapitałowych", „redukcja kosztów zarządzania IT", „przyspieszenie wdrażania technologii" i „przyspieszenie innowacji biznesowych" jako główne korzyści biznesowe związane z przetwarzaniem w chmurze. Pomimo korzyści obiecanych przez przetwarzanie w chmurze, branża IT dostrzega również, że potrzebne są znaczące innowacje i ulepszenia w zakresie technologii i zarządzania operacjami, aby umożliwić szerokie zastosowanie usług w chmurze. Głównymi problemami są kwestie bezpieczeństwa i wydajności. Weźmy na przykład bezpieczeństwo, podczas gdy indywidualni konsumenci mogą zwracać się do Amazon Elastic Compute Cloud (EC2) i Simple Storage Services (S3) w celu uzyskania zasobów obliczeniowych na żądanie i pojemności pamięci masowej, bank ma inną sprawę do przechowywania informacje o swoich klientach w chmurze innej firmy. W oparciu o różnice w modelu wdrożenia usługi w chmurze można dostarczać na trzy główne sposoby: chmura publiczna, chmura prywatna i chmura hybrydowa.

Chmura publiczna

Chmura publiczna odnosi się do modelu dostarczania usług w chmurze, w którym usługodawca udostępnia powszechnie skalowalne zasoby IT, takie jak moce procesora i pamięci masowej lub

aplikacje oprogramowania, za pośrednictwem Internetu. Usługi chmury publicznej są zazwyczaj oferowane w modelu opartym na użytkowaniu. Chmura publiczna to pierwszy model wdrażania usług w chmurze, który weszło do słownika branży IT. Koncepcja chmur publicznych jasno pokazała długoterminowy potencjał modelu przetwarzania w chmurze i rozpaliła wyobraźnię przemysłu i społeczności naukowej. Obecnie istnieje wielu dostawców usług chmury publicznej, oferujących usługi od infrastruktury jako usługi, przez platformę programistyczną jako usługę, po aplikacje jako usługi specjalnego przeznaczenia. Amazon EC2, Force.com i Google App Engine to jedne z najbardziej znanych przykładów chmur publicznych, ale rynek jest teraz najeżony konkurencją. Zobacz ankietę firmy InformationWeek dotyczącą głównych dostawców usług chmury publicznej, aby uzyskać szczegółową analizę ich usług, modeli cenowych, obsługiwanych platform itp. Podczas gdy chmura publiczna oferuje czysty, pozbawiony infrastruktury model dla użytkowników końcowych do korzystania z usług IT i intryg społeczność naukową z jej destrukcyjnym charakterem, migrująca większość dzisiejszych usług IT, takich jak różne aplikacje biznesowe w środowisku korporacyjnym (np. aplikacje ubezpieczeniowe, administracja opieki zdrowotnej, zarządzanie kontami klientów bankowych, lista jest długa), do model chmury publicznej jest niewykonalny. Bezpieczeństwo danych, ład korporacyjny, zgodność z przepisami oraz obawy dotyczące wydajności i niezawodności zabraniają przenoszenia takich aplikacji informatycznych poza „domeny kontrolowane" (tj. w ramach zapór korporacyjnych), podczas gdy infrastruktura chmury publicznej, regulacje rządowe i akceptacja publiczna nadal poprawić.

Prywatna chmura

Z kolei chmura prywatna reprezentuje model wdrażania, w którym przedsiębiorstwa (zwykle duże korporacje działające w wielu lokalizacjach) oferują usługi w chmurze za pośrednictwem sieci korporacyjnej (może to być wirtualna sieć prywatna) swoim wewnętrznym użytkownikom za środowiskiem chronionym zaporą ogniową. Ostatnie postępy w wirtualizacji i konsolidacji centrów danych pozwoliły administratorom sieci firmowych i centrów danych skutecznie stać się dostawcami usług spełniających potrzeby ich klientów w tych korporacjach. Chmury prywatne pozwalają dużym korporacjom czerpać korzyści z koncepcji „łączenia zasobów" związanej z przetwarzaniem w chmurze i ich własnym rozmiarem, jednocześnie rozwiązując obawy dotyczące bezpieczeństwa danych, ładu korporacyjnego, regulacji rządowych, wydajności i problemów związanych z niezawodnością. chmury dzisiaj. Krytycy chmur prywatnych wskazują, że te korporacje „nadal muszą kupować, budować i zarządzać chmurami" i jako takie nie odnoszą korzyści z niższych początkowych kosztów kapitałowych i mniej praktycznego zarządzania, zasadniczo „brakuje modelu ekonomicznego, który sprawia, że chmura obliczenie tak intrygującej koncepcji." Chociaż te krytyki są prawdziwe z punktu widzenia purystów, chmury prywatne są opłacalnym i niezbędnym modelem wdrażania w ogólnym przyjęciu przetwarzania w chmurze jako nowego modelu IT. Wierzymy, że bez wielkich korporacji przetwarzanie w chmurze nigdy nie stanie się głównym nurtem obliczeniowym i paradygmatem IT (do tego można się odwołać do poprzedniego przykładu Grid Computing). Chmura prywatna stanowi krok umożliwiający, a także przejściowy w kierunku szerszego przyjęcia usług IT w chmurach publicznych. Ponieważ infrastruktura chmury publicznej, regulacje rządowe i akceptacja społeczna wciąż się poprawiają, coraz więcej aplikacji IT będzie najpierw oferowanych jako usługi w środowisku chmury prywatnej, a następnie migrowanych do chmury publicznej. Ścieżka migracji usługi poczty e-mail w środowisku korporacyjnym - od początkowo wielu wydziałowych serwerów poczty e-mail, przez dzisiejszą pojedynczą „chmurę poczty e-mail" na poziomie korporacyjnym do publicznej chmury poczty e-mail - oferuje przykładową reprezentację. Chociaż puryści mogą argumentować w kategoriach czarno-białych, uważamy, że chmura prywatna jako realny model wdrażania przetwarzania w chmurze będzie istniała przez długi czas i zasługuje na uwagę zarówno środowisk biznesowych, jak i naukowych.

Chmura hybrydowa

Podczas gdy chmury publiczne i prywatne reprezentują dwa krańce spektrum przetwarzania w chmurze pod względem własności i wydajności współdzielonych zasobów - a każda z nich znajduje akceptację zgodnie z oferowanymi usługami i docelowymi segmentami klientów – trzeci model wdrażania chmury obliczeniowej, hybryda Pojawia się model chmury, który łączy cechy chmur publicznych i prywatnych. Chmura hybrydowa to model wdrażania usług w chmurze, w którym organizacja dostarcza usługi w chmurze i zarządza niektórymi zasobami pomocniczymi we własnym zakresie, a inne zleca na zewnątrz. Na przykład organizacja może przechowywać dane klientów we własnym centrum danych i mieć usługę chmury publicznej, taką jak EC2 firmy Amazon, aby zapewnić moc obliczeniową na żądanie, gdy potrzebne jest przetwarzanie danych. Innym przykładem jest koncepcja „chmury publicznej jako przepełnienia chmury prywatnej", w której menedżer IT nie musi udostępniać swojej korporacyjnej chmury prywatnej na wypadek najgorszego scenariusza obciążenia (tak z pewnością pokona ekonomię chmury prywatnej), ale wykorzystać chmurę publiczną do przepełnienia, aby dynamicznie i przejrzyście przenosić obciążenia o mniej krytycznym znaczeniu dla działalności w celu dostosowania do rozwoju firmy lub sezonowych szczytowych obciążeń. Można znaleźć różne warianty scenariusza „przepełnienia", takie jak operacje „podążania za słońcem" w globalnej organizacji, w której obciążenia są przenoszone na całym świecie w oparciu o strefy czasowe zespołów roboczych. Pod względem architektonicznym chmurę hybrydową można uznać za chmurę prywatną rozszerzającą swoje granice na środowisko chmury innej firmy (np. chmurę publiczną) w celu uzyskania dodatkowych (lub niekrytycznych) zasobów w sposób bezpieczny i na żądanie. Wdrażanie usług w chmurze jest procesem stopniowym: IT przedsiębiorstwa (które stanowi większość wydatków branży IT i zużycia usług) potrzebuje ścieżki migracji, aby przenieść dzisiejsze lokalne aplikacje IT do usług oferowanych przez dostawców chmury publicznej za pomocą modelu użytkowego. W związku z tym chmura hybrydowa reprezentuje dominujący model wdrażania. Duże przedsiębiorstwa często już poczyniły znaczne inwestycje w infrastrukturę informatyczną niezbędną do zapewnienia własnych zasobów. Tymczasem organizacje muszą zachować wrażliwe dane pod własną kontrolą, aby zapewnić bezpieczeństwo i zgodność z przepisami rządowymi. Kusząca możliwość oferowana przez model chmury hybrydowej – korporacyjne organizacje IT zarządzające chmurą wewnętrzną, która płynnie łączy się z chmurą publiczną, która pobiera opłaty na zasadzie płatności zgodnie z rzeczywistym użyciem – urzeczywistnia obietnicę amorficznego terminu cloud computing. Aby umożliwić chmurę hybrydową, wirtualizacja, bezproblemowa mobilność obciążeń, dynamiczne udostępnianie zasobów w chmurze i przejrzyste środowisko użytkownika należą do krytycznych wyzwań technicznych, które należy rozwiązać.

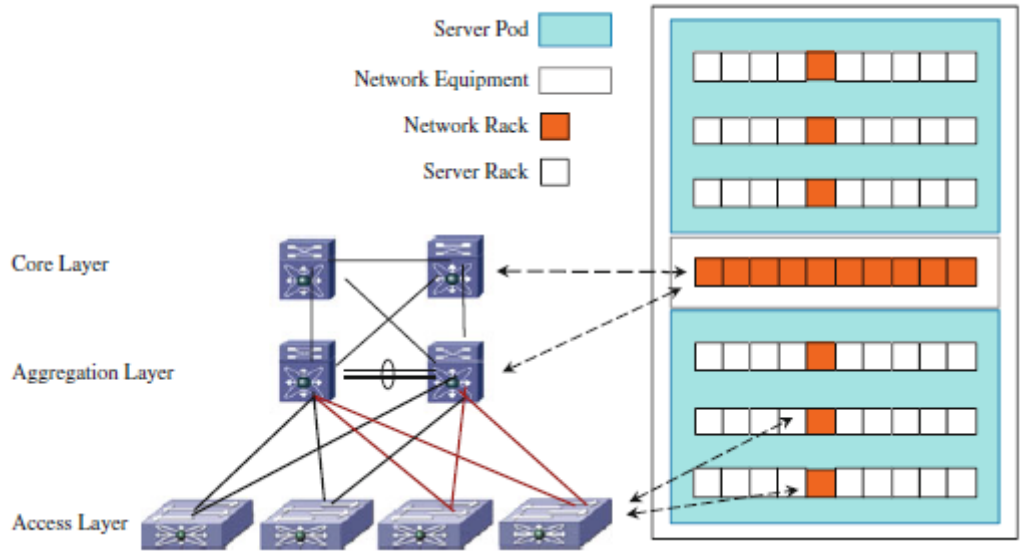
Przegląd architektur sieciowych dla chmur

Istnieją trzy główne obszary, w których architektura sieci ma znaczenie dla przetwarzania w chmurze: (1) sieć centrum danych, która łączy zasoby infrastruktury (np. serwery i urządzenia pamięci masowej) w ramach centrum danych usługi w chmurze, (2) połączenie centrum danych sieć łącząca wiele centrów danych w chmurze prywatnej, publicznej lub hybrydowej w celu obsługi usług w chmurze, (3) publiczny Internet, który łączy użytkowników końcowych z centrami danych dostawcy chmury publicznej. Ostatni obszar dotyczy głównie dzisiejszej infrastruktury sieci telekomunikacyjnej i sam w sobie jest złożonym tematem z perspektywy architektonicznej, regulacyjnej, operacyjnej i regionalnej. W tej części skupimy się tylko na dwóch pierwszych obszarach (sieć centrów danych i sieć połączeń centrów danych).

Sieć centrów danych

Dostawcy usług w chmurze oferują skalowalne usługi w chmurze za pośrednictwem ogromnych centrów danych. W takich centrach danych na dużą skalę sieć centrów danych (DCN) jest skonstruowana tak, aby łączyć dziesiątki, a czasem setki tysięcy serwerów w celu dostarczania

publicznie skalowalnych usług w chmurze. Hierarchiczne projektowanie sieci to najpowszechniejsza architektura stosowana w sieciach centrów danych. Rysunek przedstawia koncepcyjny widok hierarchicznej sieci centrum danych oraz przykład mapowania architektury referencyjnej do fizycznego wdrożenia centrum danych.



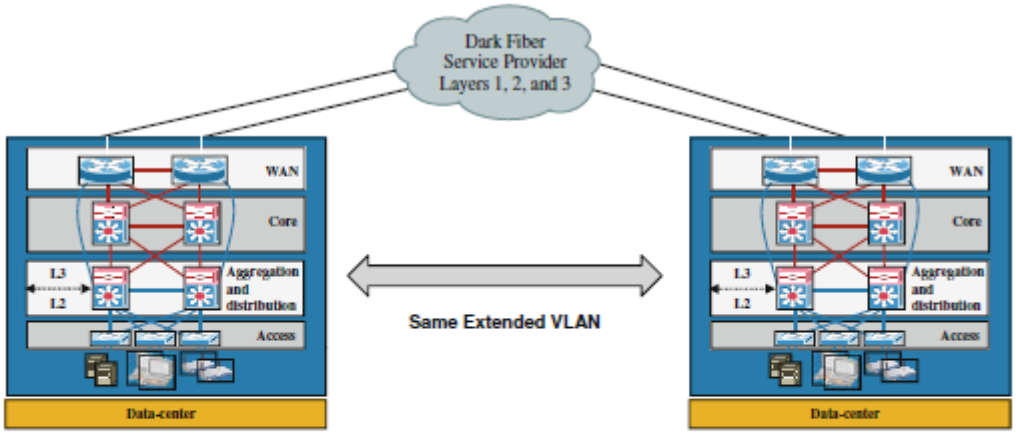
Warstwa dostępu sieci centrum danych zapewnia łączność dla puli zasobów serwerów znajdujących się w centrum danych. Na projekt warstwy dostępu duży wpływ mają kryteria decyzyjne, takie jak gęstość serwera, współczynnik kształtu i wirtualizacja serwera, które mogą skutkować wyższymi wymaganiami dotyczącymi liczby interfejsów. Powszechnie stosowane podejścia do łączności w warstwie dostępu do centrum danych to przełącznik końca rzędu (EoR), przełącznik na górze szafy (ToR) oraz przełącznik zintegrowany (zwykle w postaci przełączników kasetowych wewnątrz modułowej obudowy serwera kasetowego). Inną formą zintegrowanego przełącznika jest wbudowany przełącznik programowy w punkcie końcowym serwera. Każde podejście projektowe ma swoje wady i zalety i jest podyktowane wymaganiami sprzętowymi i aplikacyjnymi serwera. Warstwa agregacji centrum danych stanowi punkt konsolidacji, w którym połączone są przełączniki warstwy dostępu, zapewniając łączność między serwerami dla aplikacji wielowarstwowych, a także łączność w rdzeniu sieci z klientami rezydującymi w obrębie kampusu, sieci WAN lub Internetu. Warstwa agregacji zazwyczaj stanowi granicę między łączami routowanymi warstwy 3 a domenami rozgłoszeniowymi sieci Ethernet warstwy 2 w centrum danych. Przełączniki dostępowe są połączone z warstwą agregacji za pomocą łączy trunkingowych VLAN 802.1Q, aby zapewnić możliwość łączenia serwerów należących do różnych sieci VLAN i podsieci IP do tego samego przełącznika fizycznego. Podstawową funkcją warstwy szkieletowej w sieci centrum danych jest zapewnienie wysoce dostępnego i wydajnego przełączania w warstwie 3 dla ruchu IP między centrum danych a brzegiem Internetu i szkieletem sieci telekomunikacyjnej. W niektórych sytuacjach wiele rozproszonych geograficznie centrów danych należących do dostawcy usług w chmurze może być połączonych za pośrednictwem prywatnej sieci WAN lub sieci metropolitalnej (MAN). W takich środowiskach rozszerzenie sieci warstwy 2 w wielu centrach danych jest lepszym projektem architektury. W innych sytuacjach ruch musi być przenoszony przez publiczny Internet. Typową topologią sieci dla tego rodzaju geograficznie rozproszonych centrów danych jest routing równorzędny warstwy 3 między głównymi przełącznikami centrum danych. Skonfigurowanie wszystkich łączy łączących się z rdzeniem sieci jako połączeń typu punkt-punkt w warstwie 3 zapewnia szybką konwergencję wokół awarii łącza, a płaszczyzna sterowania przełączników rdzeniowych nie jest narażona na ruch rozgłoszeniowy z urządzeń węzłów końcowych ani nie jest wymagana do udziału w protokole STP w celu zapobiegania pętlom sieci warstwy 2. Ewolucja

technologii sieciowych do obsługi centrów danych o dużej skali jest najbardziej widoczna w warstwie dostępowej ze względu na szybki wzrost liczby serwerów w centrum danych. Niektóre prace badawcze wymagają dużej domeny warstwy 2 z bardziej płaską architekturą sieci centrum danych (2 warstwy vs 3 warstwy). Chociaż podejście to może pasować do jednorodnego, jednofunkcyjnego środowiska centrum danych, bardziej rozpowszechnione podejście opiera się na koncepcji wirtualizacji przełącznika, która umożliwia działanie logicznej warstwy dostępu warstwy 2 na wiele urządzeń fizycznych. Istnieje kilka odmian architektury implementacji wirtualizacji przełącznika w warstwie dostępu. Obejmują one technologie Virtual Blade Switch (VBS), Fabric Extender i Virtual Ethernet Switch. Podejście VBS pozwala wielu fizycznym przełącznikom kasetowym współużytkować wspólną płaszczyznę zarządzania i kontroli, wyświetlając się jako pojedynczy węzeł przełączający. Podejście Fabric Extender umożliwia wielointerfejsowemu przełącznikowi dostępowemu o dużej gęstości i dużej przepustowości współpracę z zestawem przedłużaczy sieci szkieletowej służących jako „zdalne moduły we/wy", rozszerzając wewnętrzną strukturę przełączników dostępowych na większą liczbę portów dostępu do serwerów o niskiej przepustowości. Przełącznik wirtualnej sieci Ethernet jest zazwyczaj przełącznikiem dostępowym opartym na oprogramowaniu, zintegrowanym w hipernadzorcy po stronie serwera. Te technologie wirtualizacji przełączników umożliwiają centrum danych obsługę usług w chmurze dla wielu dzierżawców i zapewniają elastyczne konfiguracje w celu skalowania w górę i w dół możliwości wdrażania w zależności od poziomu obciążenia. Chociaż omówiliśmy ogólne zasady projektowania sieci centrum danych w masowo skalowalnym centrum danych, niektórzy dostawcy usług w chmurze, zwłaszcza niektórzy dostawcy chmury publicznej, przyjęli dwuwarstwową architekturę centrum danych w celu optymalizacji kosztów centrum danych i świadczenia usług. W tej architekturze tworzenie i dostarczanie usługi w chmurze jest zwykle realizowane przez dwie warstwy centrów danych - warstwę frontonu i warstwę zaplecza — o znacznej różnicy w ich rozmiarach. Weźmy na przykład usługę wyszukiwania w sieci Web, aplikacje do masowej analizy danych (np. obliczające indeks wyszukiwania w sieci) są naturalnym rozwiązaniem dla scentralizowanych megacentrów danych (mierzonych przez setki tysięcy serwerów), podczas gdy wysoce interaktywny interfejs użytkownika aplikacje (np. proces zapytania/odpowiedzi) są naturalnym rozwiązaniem dla rozproszonych geograficznie mikrocentrów danych (mierzonych przez setki lub tysiące serwerów), z których każde znajduje się w pobliżu głównych skupisk ludności, aby zminimalizować opóźnienia sieci i koszty dostawy. Hierarchiczna architektura sieci centrów danych jest wystarczająco skalowalna, aby obsługiwać zarówno megacentra danych, jak i mikrocentra danych, stosując te same zasady projektowania omówione w tej sekcji.

Sieć połączeń w centrum danych

Sieci połączeń centrów danych (DCIN) służą do łączenia wielu centrów danych w celu zapewnienia bezproblemowej obsługi klientów usług w chmurze. Podczas gdy konwencjonalna, statycznie aprowizowana wirtualna sieć prywatna może łączyć wiele centrów danych i zapewniać bezpieczną komunikację, aby spełnić wymagania bezproblemowego korzystania z usług w chmurze (wysoka dostępność, dynamiczna migracja serwerów, mobilność aplikacji), pojawił się DCIN dla usług w chmurze jako specjalna klasa sieci w oparciu o zasadę projektowania rozszerzenia sieci warstwy 2 w wielu centrach danych (Cisco Systems, 2009b). Na przykład w przypadku migracji serwerów (w planowanym scenariuszu konserwacji centrum danych lub w scenariuszu nieplanowanego dynamicznego równoważenia obciążenia aplikacji), gdy tylko część puli serwerów jest przenoszona w danym momencie, zachowując sąsiedztwo warstwy 2 całej pula serwerów w wielu centrach danych w przeciwieństwie do renumeracji adresów IP serwerów jest znacznie lepszym rozwiązaniem. Z jednej strony podejście do rozbudowy sieci warstwy 2 jest koniecznością z punktu widzenia ciągłości biznesowej; z drugiej strony jest opłacalny z punktu widzenia operacji, ponieważ zachowuje tę samą konfigurację serwera i zasady operacyjne. Wśród głównych wymagań technicznych i przypadków

użycia sieci łączących centra danych znajdują się unikanie awarii centrum danych (w tym konserwacja centrum danych bez przestojów), dynamiczna migracja serwerów wirtualnych, klastry o wysokiej dostępności oraz dynamiczne równoważenie obciążenia i mobilność aplikacji w wielu lokalizacjach. Są to krytyczne wymagania dotyczące przetwarzania w chmurze. Weźmy na przykład mobilność aplikacji. Zapewnia podstawę niezbędną do zapewnienia elastyczności obliczeniowej — kluczowej cechy przetwarzania w chmurze — poprzez zapewnienie elastyczności przenoszenia maszyn wirtualnych między różnymi centrami danych. Rysunek przedstawia architekturę wysokiego poziomu dla sieci połączeń centrum danych opartą na podejściu do rozszerzania sieci warstwy 2.



WAN Transport	Description	LNA Extension Encapsulation Options
Dark Fiber and Service Provider Layer1	Customer Owned or Service Provider Leased	Native Ethernet, IP, MPLS
Service Provider Layer 2	Service Provider Layer 2 Service, Ethernet Private Line L (EPL)	Native Ethernet,IP, MPLS
Service Provider Layer 3	IP Leased-Line Service	IP, MPLS

Ponieważ konwencjonalna zasada projektowania sieci warstwy 2 polega na zmniejszeniu jej średnicy w celu zwiększenia wydajności i możliwości zarządzania (zwykle ograniczenie jej do warstwy dostępu, tym samym zalecając konsolidację serwerów w jednym megacentrum danych i ograniczenie łączności warstwy 2 do komunikacji wewnątrz centrum danych). , istnieje wiele obszarów wymagających ulepszeń i dalszych badań, aby sprostać potrzebom sieci połączeń w centrach danych. Poniżej wymieniono niektóre z kluczowych wymagań dotyczących rozszerzenia sieci warstwy 2 w wielu centrach danych.

Zapobieganie pętli od końca do końca

Aby poprawić wysoką dostępność sieci VLAN warstwy 2, gdy rozciąga się ona między centrami danych, to połączenie musi zostać zduplikowane. Dlatego algorytm musi być włączony, aby kontrolować wszelkie ryzyko wystąpienia pętli warstwy 2 i chronić przed wszelkiego rodzaju globalnymi zakłóceniami, które mogą być generowane przez zdalną awarię. Natychmiastową opcją do rozważenia jest wykorzystanie protokołu Spanning Tree (STP), ale należy go odizolować między zdalnymi lokalizacjami, aby zmniejszyć ryzyko propagowania niepożądanych zachowań, takich jak zmiana topologii lub przenoszenie mostu głównego z jednego centrum danych do drugiego.

Równoważenie obciążenia sieci WAN

Zazwyczaj łącza WAN są drogie, więc łącza nadrzędne muszą być w pełni wykorzystane, przy równoważeniu obciążenia ruchu we wszystkich dostępnych łączach nadrzędnych. Obszarem badań jest mechanizm dynamicznego równoważenia obciążeń na poziomie maszyny wirtualnej.

Przejrzystość podstawowa

Rozwiązanie rozszerzające sieć LAN musi być niewidoczne dla istniejącej sieci szkieletowej przedsiębiorstwa, jeśli jest dostępna, aby ograniczyć jakikolwiek wpływ na operacje. Jest to bardziej powszechne w środowiskach chmury prywatnej lub hybrydowej niż w chmurze publicznej.

Szyfrowanie

Wymóg dotyczący kryptografii rozszerzenia sieci LAN jest coraz bardziej powszechny, na przykład w celu zaspokojenia potrzeb usług w chmurze oraz wymagań federalnych i regulacyjnych.

Unikalne możliwości i wymagania dotyczące sieci w chmurze hybrydowej

Branża IT przechodzi transformację. Globalizacja, eksplozja informacji biznesowych, bezprecedensowe poziomy wzajemnych powiązań i dynamiczna współpraca między różnymi aktywami biznesowymi zarówno w ramach korporacji, jak i między wieloma korporacjami (na przykład łańcuch dostaw na żądanie) wymagają od dzisiejszych przedsiębiorstw przejścia na naprawdę ekonomiczną infrastrukturę IT , wysoce zintegrowany, zwinny i responsywny. Jak omówiono w poprzedniej sekcji, model chmury hybrydowej zapewnia bezproblemowe rozszerzenie prywatnej infrastruktury IT przedsiębiorstwa poprzez zapewnienie elastycznych usług obliczeniowych, pamięci masowej i usług sieciowych w opłacalny sposób. To bezproblemowe rozszerzenie może umożliwić przedsiębiorstwom usprawnienie procesów biznesowych, szybsze reagowanie na zmiany, elastyczną współpracę z partnerami biznesowymi, szybsze wykorzystanie pojawiających się technologii, które odpowiadają na rosnące wyzwania biznesowe i zwiększenie konkurencyjności poprzez dostarczanie większej liczby usług klientom. Aby osiągnąć tę wizję sprawności biznesowej, którą obiecują chmury hybrydowe, stoją przed nami poważne wyzwania. Należy zająć się trudnymi wymaganiami dotyczącymi wdrożeń chmury hybrydowej pod względem kosztów wdrożenia i operacyjnych, jakości świadczenia usług, odporności biznesowej i bezpieczeństwa. Chmury hybrydowe będą musiały obsługiwać dużą liczbę obciążeń związanych z „inteligentnymi rozwiązaniami branżowymi” — aplikacje biznesowe w postaci inteligentnych rozwiązań transportowych, inteligentnych rozwiązań energetycznych, inteligentnych rozwiązań w zakresie łańcucha dostaw itp. W tych „inteligentnych rozwiązaniach branżowych” duża część biznesu informacje i dane kontrolne będą gromadzone, analizowane i poddawane reakcji w ograniczonym czasie na wielu poziomach centrów chmury; obciążenia i dane będą dynamicznie przenoszone w środowisku chmury hybrydowej. Będzie to wymagało znacznych ulepszeń w dzisiejszej sieci. Używając metafory projektu mostu, możemy opisać te wymagania w trzech kategoriach - fundament, przęsło i nadbudówka.

Wirtualizacja, automatyzacja i standardy – podstawa

Wirtualizacja, automatyzacja i standardy to filary, na których opiera się każda dobra infrastruktura przetwarzania w chmurze. Bez solidnego umocowania tego fundamentu w warstwach serwerów, pamięci masowej i sieci możliwe jest wprowadzenie jedynie minimalnych ulepszeń w zakresie wdrażania usług w chmurze; z drugiej strony, mając ten fundament, można uzyskać radykalne ulepszenia poprzez „oddzielenie” aplikacji i usług od podstawowej infrastruktury w celu poprawy przenośności aplikacji, zwiększenia wykorzystania zasobów, zwiększenia niezawodności usług i znacznej poprawy podstawowych struktur kosztów. Jednak to „oddzielenie” musi być wykonane harmonijnie, tak aby sieć była „świadoma aplikacji” i aplikacja była „świadoma sieci”. W szczególności

sieci - zarówno sieć centrum danych, jak i sieć połączeń centrów danych (a na dłuższą metę publiczna sieć szkieletowa) - muszą uwzględniać wirtualizację i usługi automatyzacji. Sieć musi koordynować się z wyższymi warstwami chmury (tj. obciążeniami aplikacji - zarówno fizycznymi, jak i wirtualnymi), aby zapewnić wymagany poziom wydajności operacyjnej, aby przełamać blokadę między zasobami IT w dzisiejszym modelu klient-serwer. Ta transformacja w dynamiczną infrastrukturę, która jest „skoncentrowana" na świadczeniu usług, wymaga nie tylko, aby dział IT przedsiębiorstwa przekroczył codzienną rutynę informowania o awariach i naprawach, ale także stworzył zmianę paradygmatu w społeczności użytkowników w kierunku współdzielonego środowiska z powtarzalnymi, ustandaryzowanymi procesami. Scentralizowanemu dostarczaniu znormalizowanego zestawu usług zamiast rozproszonego dostarczania wysoce zindywidualizowanego zestawu usług musi towarzyszyć nowy poziom elastyczności dzięki mechanizmom samoobsługi. Innymi słowy, łatwiejszy i szybszy dostęp do usług sprawia, że standaryzacja jest akceptowalna, a nawet atrakcyjna dla użytkowników, ponieważ poświęcają oni możliwość dostosowywania, ale zyskują wygodę i czas. Istnieje również silna potrzeba otwartych standardów umożliwiających interoperacyjność i federację nie tylko poszczególnych warstw chmury prywatnej za zaporą sieciową przedsiębiorstwa, ale także w przypadku korzystania z usług opartych na chmurze publicznej. Ten typ hybrydowego środowiska chmury umożliwia skalowalną i elastyczną współpracę oraz globalną integrację w celu wsparcia ewoluujących zmian modelu biznesowego z klientami (np. zarządzanie relacjami z klientami) i partnerami (np. partnerzy łańcucha dostaw).

Opóźnienie, przepustowość i skala - rozpiętość

Zakres wymagań sieciowych dotyczących opóźnień, przepustowości i skali, które są potrzebne do obsługi tradycyjnych aplikacji biznesowych dla przedsiębiorstw, oraz tych potrzebnych do obsługi aplikacji opartych na chmurze, może być bardzo szeroki. Dokładne prognozowanie jakości doświadczenia użytkownika i potencjalnego wpływu biznesowego na awarię sieci jest już poważnym wyzwaniem dla menedżerów i planistów IT, nawet w przypadku dzisiejszych tradycyjnych aplikacji biznesowych dla przedsiębiorstw. Wyzwanie to stanie się jeszcze trudniejsze, ponieważ firmy będą w coraz większym stopniu polegać na bardziej wydajnych aplikacjach opartych na chmurze, które często charakteryzują się większą zmiennością niż tradycyjne aplikacje biznesowe dla przedsiębiorstw. Sprostanie temu wyzwaniu ma zasadnicze znaczenie dla „jakości doświadczenia" wymaganej, aby społeczność użytkowników zaakceptowała wspólny zestaw standardowych usług dostarczanych w chmurze. Bez tej akceptacji transformacja dzisiejszego centrum danych do środowiska chmury prywatnej lub hybrydowej z dynamiczną i współdzieloną infrastrukturą potrzebną do obniżenia całkowitego kosztu posiadania będzie znacznie trudniejsza. Niektórzy użytkownicy mogą zdecydować się na „obejście" IT, próbując wykorzystać usługi z chmury publicznej bez odpowiedniej integracji z istniejącymi procesami IT i biznesowymi, co może mieć znaczący negatywny wpływ na ich firmy. „Jakość doświadczenia" w przypadku dostępu do niektórych aplikacji i usług opartych na chmurze może wymagać wydajności zbliżonej do sieci LAN, aby umożliwić części społeczności użytkowników korzystanie z informacji w czasie rzeczywistym w celu natychmiastowego reagowania na nowe potrzeby biznesowe i spełniania wymagań klientów. W takich przypadkach znaczenie mają opóźnienia i przepustowość. Co więcej, nie muszą występować problemy na jednym przeskoku, aby wpłynąć na wydajność od końca do końca. Niewielkie przeciążenie na wielu przeskokach może powodować problemy z opóźnieniami i utratą pakietów. Dlatego dystrybucja treści, zoptymalizowane usługi routingu i akceleracji aplikacji są zwykle wymagane, zwłaszcza w przypadku wdrożeń chmury hybrydowej z regionalną i globalną łącznością sieciową. Inni użytkownicy mogą tylko chcieć po prostu zażądać nowej usługi bez konieczności wiedzy, jak lub gdzie jest ona tworzona i dostarczana. Nie chodzi o to, że wydajność nie jest ważna dla tych użytkowników. W rzeczywistości optymalizacja komunikacji i dostarczania aplikacji może nadal być wymagana w celu zwiększenia wydajności aplikacji i danych,

które muszą przenosić się przez chmurę. Po prostu ich główne kryterium jakości ma więcej wspólnego z możliwością łatwego świadczenia tylu usług, ile potrzeba, niż zależy to od optymalizacji opóźnień i przepustowości. W takich przypadkach niezbędna jest możliwość łatwego udostępniania zasobów systemowych, w tym zasobów sieciowych (fizycznych lub wirtualnych). Należy również zauważyć, że dwie najpopularniejsze techniki pomagające w skalowaniu po stronie serwera, tj. gęstość fizyczna i wirtualizacja, zwiększają zależność od integracji sieci. W przypadku każdej grupy użytkowników i odpowiadających im przypadków użycia ewolucję w kierunku świadczenia usług na skalę globalną najlepiej przeprowadzić za pośrednictwem środowiska chmury hybrydowej. Chmura hybrydowa może zapewnić widoczność, kontrolę i automatyzację niezbędną do świadczenia wysokiej jakości usług na niemal każdą skalę, wykorzystując nie tylko sieć prywatną, ale także publiczny Internet za pośrednictwem zarządzanych dostawców usług sieciowych. Chmury publiczne mogą służyć do odciążania niektórych obciążeń. To odciążenie może polegać na tym, że infrastruktura sieci prywatnej może być dostępna i zoptymalizowana pod kątem innych obciążeń wrażliwych na opóźnienia i przepustowość i/lub w celu świadczenia dodatkowych usług ze względu na brak dostępnej infrastruktury na miejscu. Platformy aplikacji i narzędzia dostępne w chmurze publicznej mogą być również wykorzystywane do zapewnienia jeszcze większej elastyczności w środowiskach deweloperskich i testowych, które często są najlepszymi obciążeniami dla tego typu odciążania. Aplikacje SaaS mogą być również wykorzystywane przez społeczność użytkowników w środowisku chmury hybrydowej. W modelu chmury hybrydowej korzystanie z usług chmury publicznej można w pełni zintegrować z istniejącymi lokalnymi procesami IT i biznesowymi, aby zmaksymalizować zwrot z inwestycji, a także zapewnić zgodność z przepisami.

Zarządzanie bezpieczeństwem, odpornością i usługami - nadbudowa

Podobnie jak nadbudowa, która zapewnia integralność projektu mostu, elementy środowiska przetwarzania w chmurze – bezpieczeństwo, odporność i zarządzanie usługami – zapewniają integralność jego projektu. Bez tych elementów „nadbudowy" propozycja wartości związana z przetwarzaniem w chmurze upadnie, a korzyści ekonomiczne obiecane przez przetwarzanie w chmurze będą tylko złudzeniami. W przypadku niektórych obciążeń zgodność z przepisami branżowymi, takimi jak HIPAA (ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych) i SOX (Sarbanes Oxley), wymaga od firm zachowania pełnej kontroli nad bezpieczeństwem swoich danych. Chociaż dzieje się wiele innowacji w zakresie bezpieczeństwa w chmurach publicznych, poziom dojrzałości tych technologii może nie być jeszcze na poziomie, na którym można zagwarantować bezpieczeństwo i zgodność z przepisami. Jednak nawet w takich przypadkach przedsiębiorstwo może nadal przenosić niewrażliwe/krytyczne obciążenia do chmury publicznej, korzystając z chmury prywatnej, aby zapewnić wymagane umowy SLA dla wrażliwych/krytycznych obciążeń. Sieć odgrywa kluczową rolę w tworzeniu tych chmur zgodnych z przepisami. Prywatne usługi WAN muszą być włączone, aby zapewnić bezpieczeństwo wymagane dla prywatnej części chmury. Jeśli wykorzystywane jest środowisko chmury hybrydowej, sieć musi być również w stanie zapewnić wymaganą sfederowaną łączność i izolację oraz obsługiwać odpowiedni poziom szyfrowania tuneli VPN, które będą wykorzystywane przez chmury publiczne w celu uzyskania dostępu do danych pozostających za korporacyjną zaporą ogniową . Chociaż dostępne są inne opcje wdrażania w chmurze dla obciążeń, które nie wymagają tego samego poziomu zgodności, łączność sieciowa i funkcje bezpieczeństwa są nadal kluczowe dla pomyślnego wdrożenia tych usług w chmurze.

Zarządzanie usługami i automatyzacja również odgrywają kluczową rolę w chmurach hybrydowych. W miarę postępu usług w chmurze jest bardziej prawdopodobne, że w przyszłości usługi sieciowe dla aplikacji w chmurze będą oferowane za pośrednictwem zorientowanych na aplikacje interfejsów API warstwy abstrakcji, a nie określonych technologii sieciowych. W ramach tego paradygmatu

architektury sieci modyfikacja i udostępnianie zasobów sieciowych mogą być dokonywane w bardziej zautomatyzowany i zoptymalizowany sposób poprzez zarządzanie usługami lub samoregulację sieci. W szczególności modyfikacje te mogą być dokonywane poprzez inicjowane przez operatora dostarczanie poprzez systemy zarządzania usługami w celu zapewnienia bezpośredniej kontroli nad usługami sieciowymi lub poprzez „inteligentne" technologie sieciowe, które mogą również dostosowywać usługi w sposób autonomiczny lub samoregulujący. Co więcej, bardzo ważne jest, aby zarządzanie usługami sieciowymi i inteligentne technologie sieciowe były ściśle zintegrowane z ogólnym zarządzaniem dostarczaniem usług w chmurze, tak aby zmiany wymagane przez górne warstwy „stosu" chmury w zasobach sieciowych można było przeprowadzić przez zarządzanie usługami sieciowymi lub autoadaptacje w sposób zautomatyzowany. Wiele z tych „inteligentnych" technologii sieciowych koncentruje się na maksymalizacji odporności wdrożeń w chmurze pod względem dostępności, wydajności i mobilności obciążenia. Na przykład usługi sieciowe dostarczania aplikacji optymalizują przepływ informacji i zapewniają przyspieszenie aplikacji poprzez klasyfikację i priorytetyzację aplikacji, treści i dostępu użytkownika; technologia przełączania wirtualnego zapewnia „abstrakcję" struktury przełączania i umożliwia mobilność maszyny wirtualnej. W miarę dojrzewania tych „inteligentnych" technologii sieciowych, ich możliwości wykroczą poza obecne możliwości pojedynczej chmury, do „chmury wewnętrznej", a także „intercloud". Wraz z takim dojrzewaniem chmura hybrydowa zapewni bezprecedensowy poziom globalnego wzajemne powiązania zapewniające dostęp do informacji w czasie rzeczywistym lub prawie w czasie rzeczywistym, integracja i współpraca między aplikacjami.

Architektura sieciowa do wdrożeń chmury hybrydowej

Chmury hybrydowe odgrywają kluczową rolę w przyjęciu chmury obliczeniowej jako paradygmatu IT nowej generacji. Podczas gdy branża IT i społeczność naukowa są wciąż na wczesnym etapie zrozumienia technologii wdrożeniowych dla chmur hybrydowych, zidentyfikowano szereg głównych komponentów funkcjonalnych w architekturze sieci chmury hybrydowej. Rysunek przedstawia funkcjonalny widok architektury sieci dla chmur hybrydowych.

Chmura w pudełku

Ponieważ duże przedsiębiorstwa zaczynają budować własne chmury prywatne i dalej rozszerzać je na chmury hybrydowe, istotną potrzebą jest uproszczenie projektowania, wdrażania i zarządzania chmurami. Tradycyjny model wdrażania centrum danych, w którym oddzielne urządzenia fizyczne koncentrują się na jednostkach serwerowych, jednostkach sieciowych i jednostkach pamięci masowej, stanowi poważne wyzwanie. Nowym trendem w projektowaniu i wdrażaniu chmur prywatnych i hybrydowych jest koncepcja „chmury w pudełku". Chmura w pudełku, czasami nazywana także komórką w chmurze, to wstępnie zintegrowana, wstępnie zapakowana i samodzielna platforma dostarczania usług, którą można łatwo i szybko wykorzystać do wdrożenia prywatnych centrów chmury. Fizycznie jest zwykle dostarczany w jednej obudowie zawierającej wiele serwerów kasetowych; niektóre kasety to jednostki obliczeniowe, niektóre jednostki przełączające, a niektóre jednostki pamięci. Są one połączone za pomocą połączenia wspólnej płyty montażowej (np. płyty montażowej typu PCI) i szybkich konwergentnych połączeń Ethernet (np. 10G FCoE). Z punktu widzenia sieci przełączniki, które są wstępnie zintegrowane z chmurą w urządzeniu, to zazwyczaj przełączniki warstwy dostępu. Jeśli chodzi o oprogramowanie, wspólne środowisko hiperwizora zazwyczaj rozszerza się na jednostki obliczeniowe, jednostki sieciowe i jednostki pamięci masowej w urządzeniu typu „chmura w pudełku". Z punktu widzenia sieci wymaga to wbudowania w hipernadzorcę przełącznika wirtualnej sieci Ethernet. W środowisku VMware, przełącznik vNetwork Distributed firmy VMware i przełącznik wirtualny Cisco Nexus 1000v to dwa dobrze znane przykłady wirtualnych przełączników Ethernet z wbudowanym hiperwizorem. Oprócz wspólnej warstwy wirtualizacji zazwyczaj dołączona jest aplikacja do zarządzania usługami, która umożliwia zarządzanie i

automatyzację dostarczania usług w chmurze, rozliczania i rozliczania, bezpieczeństwa, dynamicznej realokacji zasobów i mobilności obciążeń. Co więcej, niektóre z dzisiejszych specjalnie zaprojektowanych platform cloud-in-a-box zawierają również aplikację usług w chmurze, aby oferować konkretną usługę w chmurze. Na przykład platforma cloud-in-a-box zorientowana na programowanie i testowanie może wstępnie zintegrować i wstępnie spakować zintegrowane środowisko programistyczne (IDE) gotowe do pracy w chmurze jako część produktu. W chwili pisania tego rozdziału w branży dostępnych jest wiele produktów typu „chmura w pudełku".

Węzeł usług sieciowych

Usługi sieciowe warstwy 4 odgrywają ważną rolę w architekturze sieciowej chmur hybrydowych. Zapory aplikacyjne zapewniają bezpieczny transport danych użytkowników i obciążeń aplikacji między centrami danych w chmurze hybrydowej; Systemy równoważenia obciążenia serwerów zapewniają równomierne rozłożenie obciążeń lub zgodnie z polityką operacyjną zarówno w ramach jednego centrum danych, jak i wielu centrów danych; Akceleratory sieci WAN zapewniają optymalizację sieci WAN, która przyspiesza docelowe obciążenia chmury w sieci WAN i zapewniają przejrzysty interfejs użytkownika niezależnie od tego, gdzie znajdują się aplikacje. Chociaż te usługi warstwy 4 istnieją w dzisiejszych środowiskach centrów danych, rozpowszechnienie wirtualizacji serwerów w modelu dostarczania w chmurze stworzyło poważne wyzwanie dla tradycyjnej architektury usług sieciowych, ponieważ usługi warstwy 4 muszą być teraz świadome wirtualizacji. Widoczność aktywności maszyn wirtualnych i izolacja ruchu na serwerze staje się trudniejsza, gdy ruch generowany przez maszynę wirtualną może dotrzeć do innych maszyn wirtualnych zarówno w obrębie tego samego serwera, jak i poprzez sieć centrum danych oraz sieć połączeń centrum danych. W tradycyjnym modelu dostępu każdy serwer fizyczny jest podłączony do portu dostępowego. Wszelka komunikacja do iz określonego serwera lub między serwerami przechodzi przez fizyczny przełącznik dostępu i wszelkie powiązane usługi, takie jak zapora ogniowa lub system równoważenia obciążenia. Ale co się dzieje, gdy aplikacje znajdują się teraz na maszynach wirtualnych, a wiele maszyn wirtualnych znajduje się na tym samym serwerze fizycznym? Może nie być konieczne, aby ruch opuszczał fizyczny serwer i przechodził przez fizyczny przełącznik dostępu, aby jedna maszyna wirtualna mogła komunikować się z inną. Z drugiej strony aplikację znajdującą się na maszynie wirtualnej można „przenieść" na inne centrum danych do równoważenia obciążenia. Jak zapewnić akceleratorowi sieci WAN rozpoznawanie aplikacji znajdującej się w maszynie wirtualnej i optymalizację działania sieci WAN dla maszyny wirtualnej? Egzekwowanie polityki sieciowej w tego typu środowisku może być poważnym wyzwaniem. Węzeł usług sieciowych to jednostka logiczna lub fizyczna 80 G. Lin i M. Devine, która zapewnia usługi sieciowe warstwy 4 w celu wsparcia wdrażania usług w chmurze. Celem pozostaje zapewnienie wielu takich samych usług sieciowych i funkcji używanych w tradycyjnej warstwie dostępu w nowej warstwie dostępu uwzględniającej wirtualizację. Wierzymy, że będzie to żyzny obszar dla przyszłych badań.

Sieć centrum danych i sieć połączeń centrum danych

Sieć centrów danych i sieć połączeń centrów danych zostały opisane wcześniej. Ze względu na ograniczenia długości tego rozdziału, nie będziemy wykraczać poza to, co zostało opisane wcześniej.

Zarządzanie Architekturą Sieci

Zarządzanie architekturą sieci w chmurze hybrydowej jest częścią ogólnego systemu zarządzania chmurą. Kluczowe tematy obejmują „fizyczne" zarządzanie systemowe infrastrukturą sieciową w chmurze hybrydowej oraz aspekt zarządzania „wirtualizacją", który obejmuje całą ścieżkę sieciową, począwszy od przełącznika wirtualnej sieci Ethernet wbudowanego w Hypervisor, poprzez przełączniki dostępowe i rdzeniowe w sieć centrum danych oraz w całej sieci połączeń centrum danych, a także moduły usług sieciowych na ścieżce sieciowej. Wirtualizacja nadaje nowy wymiar architekturze

zarządzania. Podobnie jak w przypadku tradycyjnego „fizycznego” zarządzania systemem, zarządzanie wirtualizacją sieci musi dynamicznie udostępniać, monitorować i zarządzać siecią typu end-to-end i usługi między maszynami wirtualnymi w środowisku chmury. W tym kontekście pierwszym krokiem jest sposób wyrażania obciążeń, zasobów sieciowych i zasad operacyjnych w sposób uwzględniający wirtualizację, ale niezależny od hiperwizora. Czytelnicy zainteresowani większą ilością szczegółów w tym zakresie mogą zacząć od DMTFb. Po osiągnięciu tego można opracować algorytmy i systemy w celu uzyskania konfiguracji sieci i alokacji zasobów w oparciu o wymagania obciążeń maszyn wirtualnych. Podobnie jak w przypadku „fizycznego” zarządzania systemem, interoperacyjność między systemami (np. między systemem zarządzania a siecią oraz między systemami zarządzania) jest ważnym wymogiem. W tym celu kluczowe są wspólne standardy, otwarte interfejsy, wspólny model danych (model informacji zarządczej). Obecnie jest to wciąż mniej skoordynowany obszar, w którym wiele organów normalizacyjnych, w tym Distributed Management Task Force (DMTF), Object Management Group (OMG), Open Grid Forum (OGF) itp., pracuje nad różnymi „standardami ” do zarządzania chmurą. Jest to obszar, który wymaga większych wysiłków, aby dojrzeć. Zainteresowani czytelnicy mogą zacząć od DMTFa i Cloud Standards Coordination

Wnioski i przyszłe kierunki

Jako kolejna zmiana paradygmatu dla branży IT, przetwarzanie w chmurze jest wciąż na wczesnym etapie. Tak jak poprzednia poważna zmiana paradygmatu IT - od przetwarzania scentralizowanego do przetwarzania rozproszonego – miała ogromny wpływ na sieci IP (i odwrotnie), widzimy podobny wpływ w odniesieniu do przetwarzania w chmurze i sieci nowej generacji. Pod wieloma względami wspieranie przetwarzania w chmurze stanowi naturalną ewolucję sieci IP; widzimy, że domena warstwy 2 w sieci centrum danych staje się szersza, bardziej płaska i świadoma wirtualizacji; widzimy, że sieć łącząca centrum danych i usługi sieciowe warstwy 4 stają się świadome wirtualizacji i samodostosowujące się do ograniczeń bezpieczeństwa, wydajności i SLA; widzimy mobilność maszyn wirtualnych i elastyczność usług w chmurze nie tylko w ramach jednego centrum danych, ale także w sieciach metropolitalnych lub sieci WAN w wielu centrach danych. W miarę jak branża IT tworzy i wdraża coraz więcej usług w chmurze, sieciom będzie stawiane więcej wymagań, a sieć obsługująca chmurę będzie wdrażać więcej inteligencji. Jesteśmy przekonani, że chmura hybrydowa stanie się idealnym modelem wdrażania chmury dla większości przedsiębiorstw, ponieważ łączy w sobie najlepsze cechy chmur prywatnych i publicznych. Sieci odgrywają niezwykle istotną rolę w umożliwianiu wdrożeń chmury hybrydowej. W przypadku usług podstawowych z krytycznymi danymi biznesowymi sieć prywatna w chmurze hybrydowej może zapewnić pełną kontrolę nad bezpieczeństwem sieci, wydajnością, zarządzaniem itp. Publiczna strona chmury hybrydowej zapewnia możliwość rozszerzenia zasięgu przedsiębiorstwa na aplikacje i usługi wdrożone w Internecie które można następnie zintegrować z zasobami lokalnymi i procesami biznesowymi. Wierzymy, że więcej innowacji umożliwiających chmurę pojawi się zarówno w sieciach centrów danych, jak i sieciach połączeń centrów danych. Ponadto wierzymy, że publiczny Internet obejmie wiele możliwości prezentowanych w dzisiejszych sieciach połączeń centrów danych (i rozszerzy się dalej). Nieco w przeciwieństwie do dzisiejszej luźno powiązanej architektury sieci IP (w odniesieniu do innych zasobów IT - serwerów, pamięci masowej i aplikacji), która była wynikiem rozproszonego modelu obliczeniowego klient-serwer, wierzymy, że model cloud computing będzie napędzał ściślej zintegrowaną architekturę sieci z innymi zasobami IT Mell & Grance.