Wirtualizacja

Cel ogólny lekcji: Zrozumienie koncepcji wirtualizacji oraz zdolność do identyfikacji różnych rodzajów wirtualizacji i ich zastosowań.

Cele szczegółowe:

I. Podstawy wirtualizacji:

a. Wyjaśnienie pojęcia wirtualizacji i jej znaczenia.
b. Zrozumienie abstrakcji tworzonej przez wirtualizację na sprzęcie komputerowym.
c. Rozpoznanie pojęcia maszyn wirtualnych (VM) i ich roli w procesie wirtualizacji.
d. Przedstawienie korzyści organizacji wynikających z wirtualizacji.

II. Hypervisory:

e. Definicja hiperwizora i jego roli w wirtualizacji.
f. Wyjaśnienie różnicy między hiperwizorami pierwszego i drugiego typu.
g. Przedstawienie funkcji hiperwizora typu 1 (nativ) i typu 2 (hosted).
h. Wskazanie przykładów popularnych hiperwizorów.

III. Zwirtualizowana sieć:

i. Definicja zwirtualizowanej sieci.
j. Wyjaśnienie zalet wirtualizowanych komponentów sieciowych.
k. Zrozumienie pojęcia wirtualnych sieci i ich roli w izolacji ruchu oraz segmentacji sieci.
l. Przedstawienie elastyczności, skalowalności i testowania w kontekście zwirtualizowanych sieci.
m. Omówienie technologii umożliwiających zwirtualizowaną sieć.

IV. Przypadki użycia:

n. Wyjaśnienie, jak wirtualizacja może być stosowana w praktyce,
o. Przedstawienie migracji fizycznej do wirtualnej i korzyści wynikających z tego procesu.

V. Kluczowe punkty:

p. Wyjaśnienie roli kluczowych elementów wirtualizacji.

VI. Korzyści z wirtualizacji:

q. Przedstawienie różnych korzyści operatorów centrów danych i dostawców usług wynikających z wirtualizacji.

VII. Hipernadzorca:

r. Wyjaśnienie roli hipernadzorcy w zarządzaniu procesami wirtualizacji.
s. Przedstawienie różnicy między hipernadzorcą typu 1 i typu 2 oraz przykładami popularnych hipernadzorców.

VIII. Wybrane rodzaje wirtualizacji:

t. Wyjaśnienie pełnej wirtualizacji, pełnej wirtualizacji wspieranej sprzętowo oraz parawirtualizacji, wraz z różnicami między nimi.

IX. Podsumowanie:

u. Podsumowanie różnic w podejściu do wirtualizacji i zrozumienie, jakie korzyści i wyzwania wiążą się z poszczególnymi rodzajami wirtualizacji.

Lekcja będzie miała na celu dostarczenie uczniom wiedzy na temat wirtualizacji, jej różnych aspektów i zastosowań, a także zrozumienia kluczowych pojęć i technologii związanych z tym zagadnieniem.

I.Podstawy wirtualizacji

Wirtualizacja to proces, który pozwala na bardziej efektywne wykorzystanie fizycznego sprzętu komputerowego i jest podstawą przetwarzania w chmurze.

Wirtualizacja wykorzystuje oprogramowanie do tworzenia warstwy abstrakcji na sprzęcie komputerowym, która umożliwia podzielenie elementów sprzętowych pojedynczego komputera - procesorów, pamięci, pamięci masowej i innych - na wiele komputerów wirtualnych, powszechnie nazywanych maszynami wirtualnymi (VM). Każda maszyna wirtualna ma własny system operacyjny (OS) i zachowuje się jak niezależny komputer, mimo że działa tylko na części rzeczywistego sprzętu komputerowego.

Wynika z tego, że wirtualizacja umożliwia bardziej efektywne wykorzystanie fizycznego sprzętu komputerowego i umożliwia większy zwrot z inwestycji w sprzęt organizacji.

Obecnie wirtualizacja jest standardową praktyką w architekturze IT przedsiębiorstwa. Jest to również technologia, która napędza ekonomię przetwarzania w chmurze. Wirtualizacja umożliwia dostawcom chmury obsługę użytkowników przy użyciu istniejącego fizycznego sprzętu komputerowego; umożliwia użytkownikom chmury zakup tylko potrzebnych zasobów obliczeniowych wtedy, gdy ich potrzebują oraz efektywne kosztowo skalowanie tych zasobów w miarę wzrostu ich obciążeń.

II.Hypervisory

Czym są hiperwizory?

Zanim hiperwizory trafiły do głównego nurtu, na większości komputerów fizycznych można było uruchamiać tylko jeden system operacyjny (OS) na raz. Dzięki temu były stabilne, ponieważ sprzęt komputerowy musiał obsługiwać tylko żądania z tego jednego systemu operacyjnego. Wadą tego podejścia było marnowanie zasobów, ponieważ system operacyjny nie zawsze mógł wykorzystać całą moc komputera.

Hiperwizor rozwiązuje ten problem. Jest to niewielka warstwa oprogramowania, która umożliwia jednoczesne działanie wielu instancji systemów operacyjnych przy współudziale tych samych fizycznych zasobów obliczeniowych. Ten proces nazywa się wirtualizacją, a instancje systemu operacyjnego nazywane są maszynami wirtualnymi (VM) - programowymi emulacjami fizycznych komputerów.

Hiperwizor, znany również jako monitor maszyny wirtualnej (VMM), zarządza tymi maszynami wirtualnymi, gdy działają one obok siebie. Oddziela od siebie maszyny wirtualne w sposób logiczny, przypisując każdej z nich własny wycinek bazowej mocy obliczeniowej, pamięci i pamięci masowej. Zapobiega to wzajemnemu zakłócaniu się maszyn wirtualnych; więc jeśli na przykład jeden system operacyjny ulegnie awarii lub naruszy bezpieczeństwo, pozostałe przetrwają.

III.Zwirtualizowana sieć

Zwirtualizowana sieć to infrastruktura sieciowa, która jest tworzona i zarządzana za pomocą technologii wirtualizacyjnych. Wirtualizacja sieci pozwala na tworzenie, konfigurowanie i zarządzanie wirtualnymi komponentami sieciowymi, takimi jak przełączniki, routery, bramy oraz połączenia między nimi, bez konieczności posiadania fizycznego sprzętu. Głównym celem zwirtualizowanych sieci jest elastyczność, skalowalność i efektywne wykorzystanie zasobów sieciowych.

Kluczowe aspekty zwirtualizowanych sieci to:

1. Wirtualne przełączniki i routery: Tworzenie wirtualnych przełączników i routerów, które mogą działać jako odrębne jednostki w obrębie jednego fizycznego sprzętu. To umożliwia izolację ruchu sieciowego oraz segmentację sieci.
2. Wirtualne sieci: Możliwość tworzenia multipleksowanych wirtualnych sieci na jednym fizycznym medium, co pozwala na oddzielenie ruchu sieciowego i zastosowanie różnych reguł i polityk dla każdej z wirtualnych sieci.

3. Elastyczność i skalowalność: Zwirtualizowane sieci pozwalają na łatwe dodawanie, usuwanie i modyfikowanie komponentów sieciowych w zależności od potrzeb, co ułatwia dostosowywanie się do zmieniających się wymagań.
4. Izolacja i bezpieczeństwo: Wirtualizacja sieci pozwala na izolację ruchu między różnymi wirtualnymi sieciami oraz zastosowanie polityk bezpieczeństwa dla każdej z nich. To pomaga w zminimalizowaniu ryzyka przeniknięcia ruchu lub ataków międzysegmentowych.
5. Testowanie i symulacja: Zwirtualizowane sieci są idealne do testowania różnych scenariuszy sieciowych i konfiguracji bez konieczności ingerencji w produkcję.
6. Rozdział zasobów: Dzięki wirtualizacji sieci można efektywnie dzielić i alokować zasoby sieciowe między różnymi grupami lub projektami.

Przykłady technologii umożliwiających zwirtualizowaną sieć to:

a. VLAN (Virtual LAN): Dzielenie jednej fizycznej sieci na wiele logicznych segmentów.
b. VXLAN (Virtual Extensible LAN): Protokół rozszerzający koncept VLAN na skalę dużo większą, umożliwiający tworzenie wirtualnych sieci w sieci.
c. SDN (Software-Defined Networking): Technologia, która oddziela warstwę sterowania od warstwy danych w sieci, umożliwiając elastyczne zarządzanie i konfigurację.
d. NFV (Network Functions Virtualization): Przenoszenie funkcji sieciowych, takich jak routery, firewalle czy load balancery, na platformy wirtualne.
e. Overlay Networks: Tworzenie wirtualnych sieci na istniejącej infrastrukturze sieciowej, często wykorzystując protokoły tunelujące.

W skrócie, zwirtualizowana sieć to elastyczne, skalowalne i zarządzalne środowisko sieciowe oparte na technologiach wirtualizacyjnych, które umożliwiają oddzielenie ruchu, izolację, testowanie oraz efektywne wykorzystanie zasobów sieciowych.

IV.Przypadki użycia

Użycie sprzętu pojedynczego komputera fizycznego, aby uruchamiać w nim wiele maszyn wirtualnych

V.Kluczowe punkty:

- Użycie sprzętu systemowego.
- Przydziela procesor/pamięć RAM/pamięć masową do maszyn wirtualnych.
- Nie można przekroczyć CPU/RAM/Storage dostępne na fizycznym sprzęcie.

VI.Korzyści z wirtualizacji

Wirtualizacja przynosi kilka korzyści operatorom centrów danych i dostawcom usług:

1. Efektywne wykorzystanie zasobów: przed wirtualizacją każdy serwer aplikacji wymagał własnego dedykowanego procesora fizycznego - personel IT kupował i konfigurował osobny serwer dla każdej aplikacji, którą chciał uruchomić. (Działalność informatyczna preferowała jedną aplikację i jeden system operacyjny (OS) na komputer ze względu na niezawodność.) Niezmiennie każdy serwer fizyczny byłby niedostatecznie wykorzystywany. Z kolei wirtualizacja serwerów umożliwia uruchamianie kilku aplikacji - każdej na osobnej maszynie wirtualnej z własnym systemem operacyjnym - na pojedynczym komputerze fizycznym (zwykle na serwerze x86) bez utraty niezawodności. Umożliwia to maksymalne wykorzystanie mocy obliczeniowej fizycznego sprzętu.
2. Łatwiejsze zarządzanie: zastąpienie komputerów fizycznych maszynami wirtualnymi zdefiniowanymi programowo ułatwia korzystanie z zasad zapisanych w oprogramowaniu i zarządzanie nimi. Pozwala to na tworzenie zautomatyzowanych przepływów pracy związanych z zarządzaniem usługami IT.
Na przykład zautomatyzowane narzędzia wdrażania i konfiguracji umożliwiają administratorom definiowanie kolekcji maszyn wirtualnych i aplikacji jako usług w szablonach oprogramowania. Oznacza to, że mogą instalować te usługi wielokrotnie i konsekwentnie bez uciążliwego i czasochłonnego. i podatną na błędy konfigurację ręczną. Administratorzy mogą korzystać z zasad bezpieczeństwa wirtualizacji, aby narzucić określone konfiguracje zabezpieczeń w zależności od roli maszyny wirtualnej. Zasady mogą nawet zwiększyć wydajność zasobów, wycofując nieużywane maszyny wirtualne w celu zaoszczędzenia miejsca i mocy obliczeniowej.
3. Minimalny czas przestojów: awarie systemu operacyjnego i aplikacji mogą powodować przestoje i zakłócać produktywność użytkowników. Administratorzy mogą uruchamiać obok siebie wiele redundantnych maszyn wirtualnych i przełączać je między sobą w razie wystąpienia problemów. Uruchamianie wielu redundantnych serwerów fizycznych jest droższe.
4. Szybsze udostępnianie: kupowanie, instalowanie i konfigurowanie sprzętu dla każdej aplikacji jest czasochłonne. Pod warunkiem, że sprzęt jest już na miejscu, udostępnianie maszyn wirtualnych do uruchamiania wszystkich aplikacji jest znacznie szybsze. Możesz nawet zautomatyzować to za pomocą oprogramowania do zarządzania i zintegrować z istniejącymi przepływami pracy.

Inne:

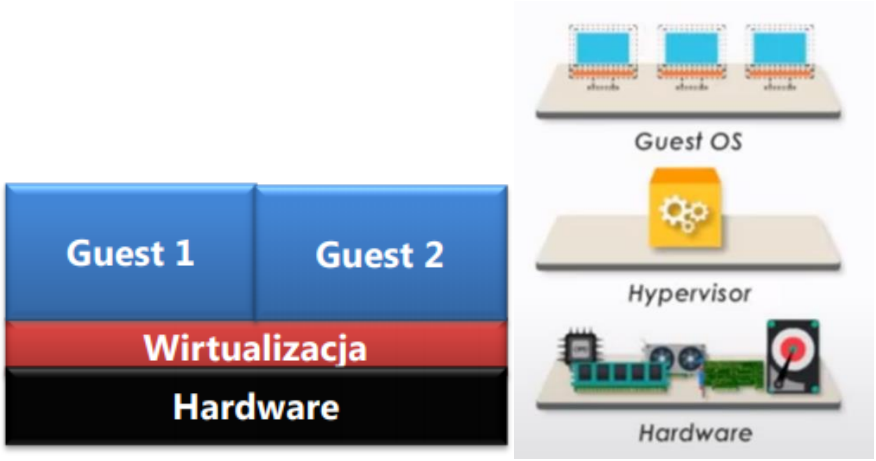
- Oszczędność energii/zmniejszona zajmowana powierzchnia.
- Odzyskiwanie (maszyny wirtualne można zapisać jako pliki).
- Elastyczność (maszyny wirtualne można przenosić).
- Badanie systemów operacyjnych.
- Oprogramowanie (sandbox - piaskownica) - środowisko testowe, zaprojektowane do celu prowadzenia dobrze izolowanych eksperymentów.

VII.Hipernadzorca

Hipernadzorca to narzędzie niezbędne do zarządzania procesami wirtualizacji. Hipernadzorca pozwala na uruchamianie wielu izolowanych środowisk wirtualnych nazywanych maszynami wirtualnymi (VM) na jednym serwerze fizycznym. Hipernadzorca może być instalowany bezpośrednio na sprzęcie (typ pierwszy) lub jako aplikacja na systemie operacyjnym (typ drugi).

1. Hipernadzorca typu 1

Hipernadzorca typu 1 (tzw. natywny albo z ang. bare metal) - działa bezpośrednio na poziomie sprzętu, mamy nad nim pełną kontrolę i monitorujemy uruchomione systemy operacyjne. Systemy operacyjne działają na poziomie wyżej niż hipernadzorca.



Przykładami hipernadzorców typu 1 są VMware ESXi, Citrix XenServer.

hiperwizory VMware VMware oferuje hiperwizory typu 1 i typu 2.

Hiperwizory typu 1 obejmują:

Hiperwizor ESXi (zintegrowany z Elastic Sky X) to hiperwizor typu 1 (lub bare-metal) ukierunkowany na wirtualizację serwerów w centrum danych. ESXi zarządza kolekcjami maszyn wirtualnych VMware.

Hiperwizor VSphere. Klienci mogą bezpłatnie korzystać z VMware ESXi w ramach bezpłatnego hiperwizora vSphere, który jest podstawową ofertą wirtualizacji serwerów. Firmy z korporacyjnymi środowiskami chmurowymi będą licencjonować vSphere, bardziej kompletny system, który obejmuje licencję na vCenter Server firmy VMware. Jest to osobny serwer służący do administrowania środowiskami vSphere działającymi na hostach fizycznych. VSphere może działać w prywatnym środowisku chmury lokalnej lub w konfiguracji hostowanej chmury.

Hiperwizory Citrix

XenServer, obecnie znany jako Citrix Hypervisor, to komercyjny hiperwizor typu 1 obsługujący systemy operacyjne Linux i Windows. XenServer narodził się z projektu open source Xen (odsyłacz prowadzi poza witrynę ibm.com).

Pośrodku początek

Hiperwizor Hyper-V

Microsoft Hyper-V. Nie ma jednej, powszechnie akceptowanej definicji typów hypervisorów.

Według Wikipedii, Hyper-V jest hypervisorem drugiego typu, ponieważ działa na poziomie systemu operacyjnego i ma jedną partycję nadrzędną z bezpośrednim dostępem do zasobów sprzętowych.

Jednak według innej strony, Hyper-V jest hypervisorem pierwszego typu, ponieważ nie wymaga dodatkowego systemu operacyjnego do działania i ma niski poziom abstrakcji.

Może więc zależy od tego, jak interpretujemy te kryteria i jak porównujemy Hyper-V z innymi hypervisora

Hyper-V jest uważany za hypervisora pierwszego typu przez Microsoft i IBM. Powodem jest to, że Hyper-V działa bezpośrednio na sprzęcie fizycznym, wstawiając się pod system operacyjny hosta.

Jednak niektórzy uważają, że Hyper-V jest hybrydą między typem pierwszym a drugim, ponieważ wymaga systemu operacyjnego do zarządzania partycjami i urządzeniami.

Microsoft określa Hyper-V jako hiperwizor typu 1, mimo że działa inaczej niż wielu konkurentów. Hyper-V instaluje się w systemie Windows, ale działa bezpośrednio na sprzęcie fizycznym, umieszczając się pod systemem operacyjnym hosta. Wszystkie systemy operacyjne gościa działają następnie przez hiperwizora, ale system operacyjny hosta uzyskuje specjalny dostęp do sprzętu, co daje mu przewagę wydajności.

Hypervisor KVM

KVM jest podobny do Hyper-V w tym sensie, że nie jest to jednoznaczny przypadek. Według Red Hat, KVM jest technologią pierwszego typu, ponieważ konwertuje jądro Linuxa na hypervisora działającego bezpośrednio na sprzęcie. Jednak według innej strony, KVM może być również uznany za technologię drugiego typu, ponieważ system operacyjny hosta nadal jest w pełni funkcjonalny i inne maszyny wirtualne są zwykłymi procesami Linuxa. Może więc zależy od tego, jak patrzymy na rolę jądra Linuxa i systemu operacyjnego hosta.

Pośrodku koniec

2. **Hipernadzorca typu 2**

Hipernadzorca typu 2 (tzw. hostowany) - działa jako program uruchomiony na danym systemie operacyjnym (hoście). Są to rodzaje emulatorów. W tym przypadku zwirtualizowane systemy działają dwa poziomy ponad sprzętem.

Przykładami są VMWare Workstation, VMware Server, Oracle Virtualbox i Microsoft VirtualPC, Microsoft Virtual Server.

VMware oferuje również hiperwizory typu 2 dla użytkowników komputerów stacjonarnych i laptopów:

VMware Fusion: Jest to oferta firmy skoncentrowana na systemie MacOS, która umożliwia użytkownikom komputerów Mac uruchamianie szerokiej gamy systemów operacyjnych gościa.

Stacja robocza: platforma VMware zorientowana na system Linux i Windows jest dostępna w dwóch wersjach: Pro, która jest wersją płatną, oraz Player, która jest bezpłatna do użytku osobistego. Wersja Pro pozwala użytkownikom uruchamiać wiele systemów operacyjnych na jednym komputerze, a także łączy się z VMware vSphere, podobnie jak Fusion. Workstation Player obsługuje tylko jeden system-gość.

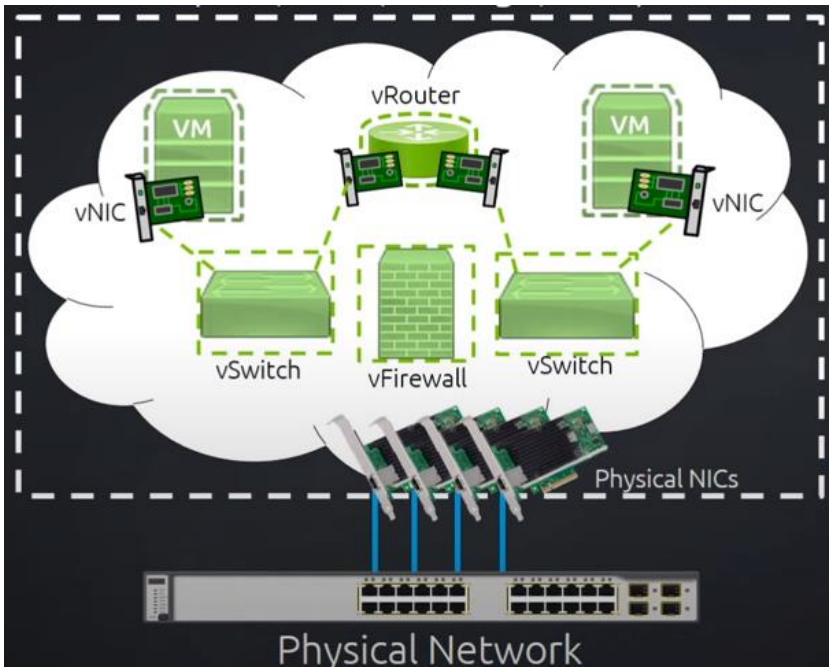
VirtualBox: hiperwizor typu 2 działający w systemach operacyjnych Linux, Mac OS i Windows. Oracle odziedziczyła produkt, kupując Sun Microsystems w 2010 roku. VirtualBox:

a. emuluje dyski twarde w trzech formatach: VDI, VMDK i VHD, może również łączyć się z celami iSCSI i surowymi partycjami na hoście,
b. obsługuje pełną wirtualizację sprzętową (iVT i AMD-V) oraz wirtualizację sprzętową wspomaganą przez system operacyjny,

c. oferuje funkcje takie jak zrzuty stanu, wirtualizacja oprogramowania i pełne szyfrowanie maszyn wirtualnych,

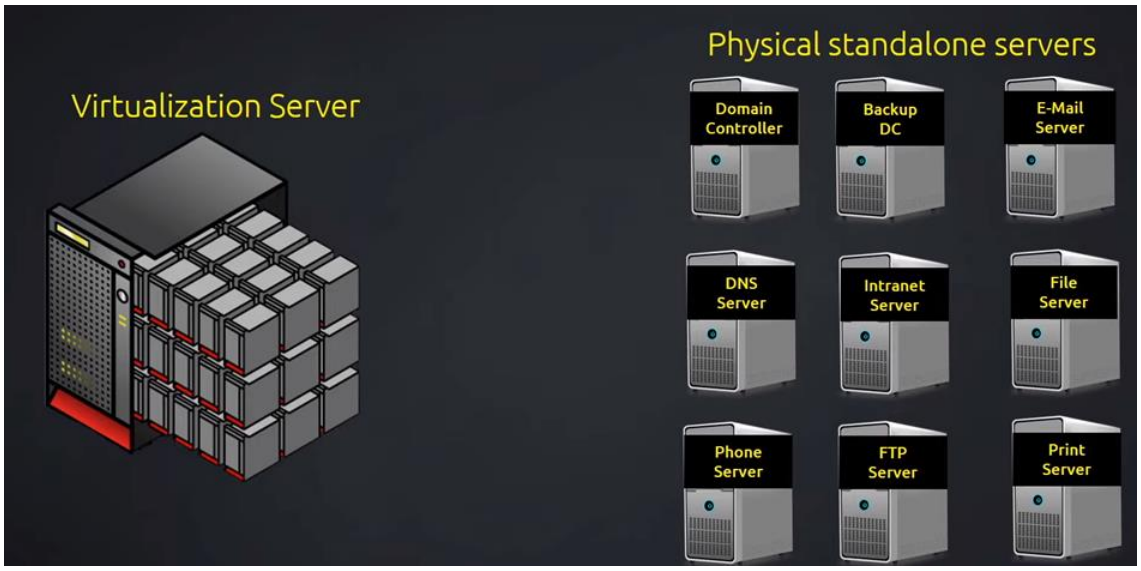
d. integruje się z OCI, oferuje ulepszoną obsługę 3D i automatyczny budowniczy maszyn wirtualnych.

Fizyczne serwery z hiperwizorem typu 1 (CPU, RAM, Storage, NICs)



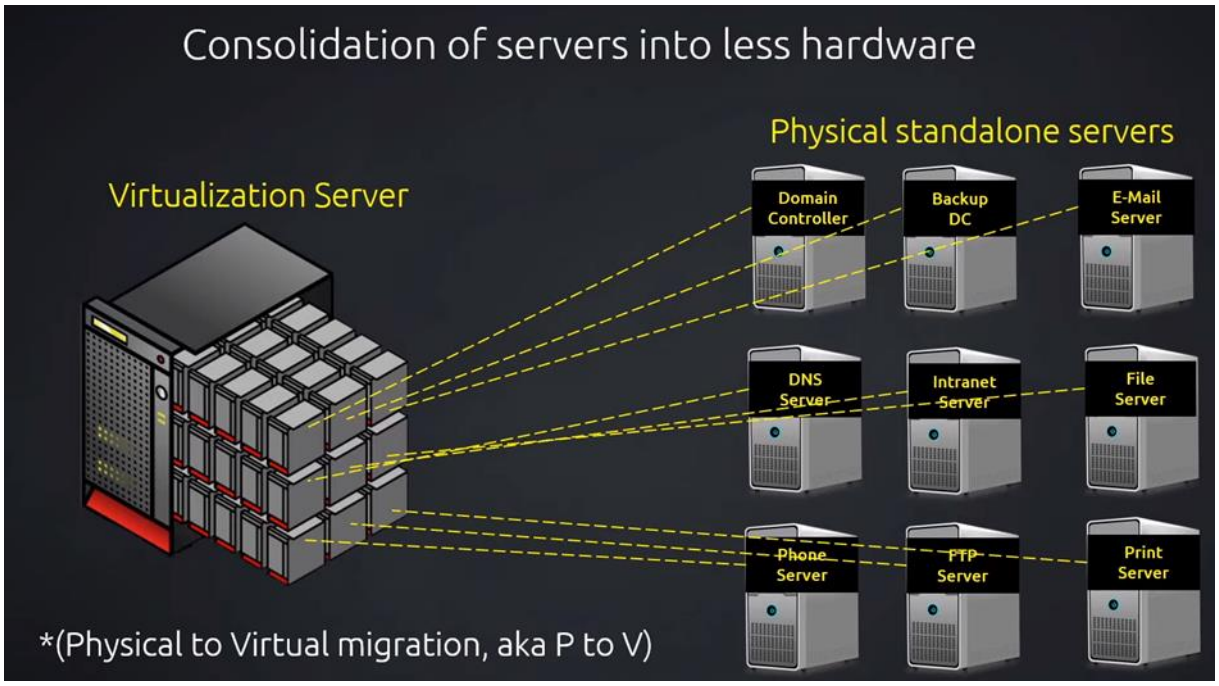
- Virtual Switch
- Virtual NIC
- Virtual Router
- Virtual Firewall

Fizyczne serwery autonomiczne



Konsolidacja serwerów w mniejszy sprzęt

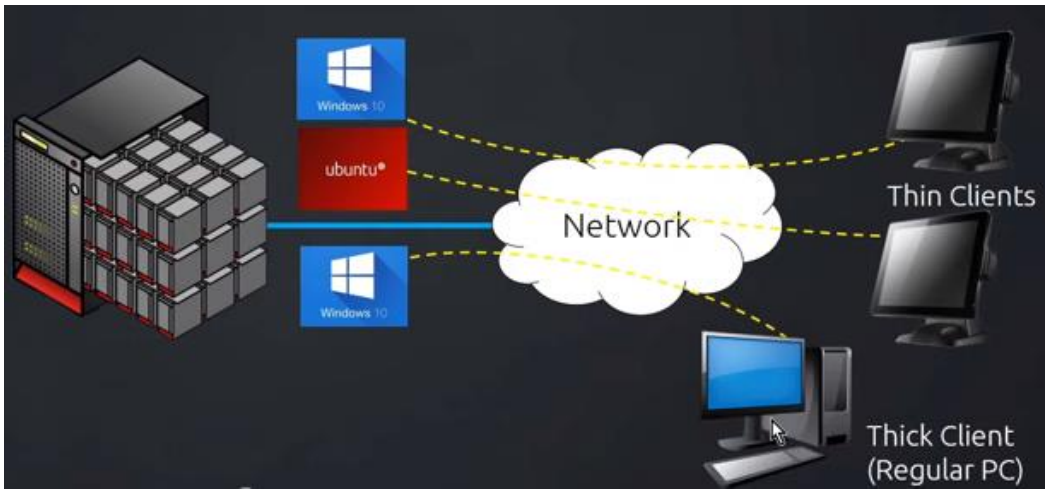
Fizyczne serwery autonomiczne



* (Migracja fizyczna do wirtualnej, inaczej z P do V)

Wirtualizacja komputera stacjonarnego / systemu operacyjnego działająca w centrum danych.

Punkty końcowe, takie jak cienki klient, uzyskują dostęp do maszyny wirtualnej za pośrednictwem sieci.

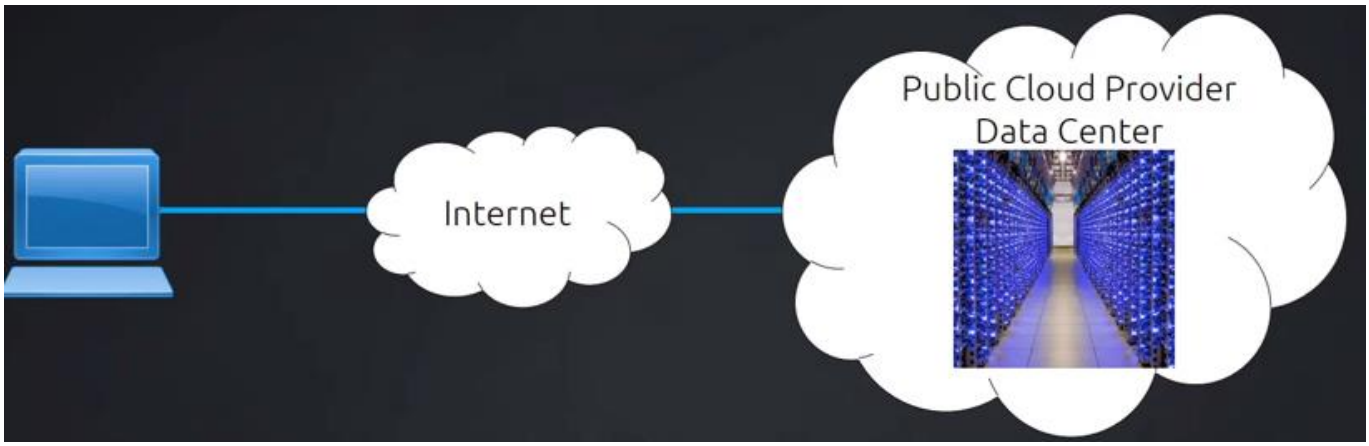


• Łatwiejsze zarządzanie • Większe bezpieczeństwo

• Łatwiejsze tworzenie kopii zapasowych • Oszczędność kosztów

Centra danych czerpią korzyści z wirtualizacji ze względu na możliwość uruchamiania większej liczby usług i oprogramowania na mniejszej powierzchni

Internet Centrum danych dostawcy chmury publicznej



Publiczne przetwarzanie w chmurze polega na uzyskiwaniu dostępu do usług i zasobów ze zdalnego centrum danych i płaceniu tylko za to, z czego korzystasz.

* Wirtualizacja i szybkie sieci naprawdę otwierają erę chmury obliczeniowej.

VIII.Wybrane rodzaje wirtualizacji:

Pełna wirtualizacja:

• realizowana przez hypervisor Typu 1 i Typu 2

• wirtualizacja dowolnego niezmodyfikowanego OS

• problem z realizacją uprzywilejowanych instrukcji jądra systemu gościa (np. emulacja operacji I/O)

• słaba wydajność

Pełna wirtualizacja wspierana sprzętowo:

• wymaga procesorów Intel-VT (vmx) lub AMD-V (svm)

• platforma sprzętowa wspierająca DEP

• natywna wirtualizacja gości w Ring 0

• bardzo dobra wydajność

Parawirtualizacja:

• wykorzystuje hypervisor Typu 1

• jeden z systemów gościa jest uprzywilejowany (Dom0)

• konieczność modyfikacji jądra systemów gości celem odwołań do hypervisora (hypercall)

• bardzo dobra wydajność systemów gości (przy zmodyfikowanym jądrze)

IX. **Podsumowanie**

Różnice w podejściu do wirtualizacji