

Środowisko do szybkiego wdrażania i testowania sieci chmurowych

Sławomir Przyłucki, Daniel Sawicki, Dariusz Czerwiński

Klasy usług w sieciach chmurowych

Zgodnie z definicją opracowaną przez NIST (ang. *The National Institute of Standards and Technology*) przetwarzanie danych w sieciach chmurowych oznacza model usługi umożliwiającej użytkownikom wygodny dostęp na żądanie do wspólnej puli zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji i usług), przy czym obsługa tych żądań jest realizowana przy możliwie minimalnej ingerencji dostawcy usługi lub operatora sieciowego [2]. Klasyfikacja usług w chmurze opiera się o specyfikę zasobów lub oprogramowania dostarczanego końcowym użytkownikom i w najczęściej spotykanym podejściu obejmuje trzy podstawowe klasy [1]:

- sprzęt jako usługa (ang. *Hardware as a Service* – HaaS) – oznacza dostęp do dedykowanego oprogramowania (najczęściej jest to określony firmware) poprzez sieć rozległą. Nie zawsze klasa ta jest wymieniana w omówieniach sieci chmurowych, ponieważ równie często jej funkcjonalność łączona jest z klasą HaaS;
- infrastruktura jako usługa (ang. *Infrastructure as a Service* – IaaS) – oznacza środowisko sieciowe, optymalizowane pod kątem wirtualizacji zasobów. Zestaw wirtualnych zasobów komputerowych, takich jak magazyny danych i moc obliczeniowa, jest przechowywany w sieci chmurowej. Klienci wdrażają i uruchamiają własne zestawy oprogramowania systemowego, które z kolei umożliwiają korzystanie z poszczególnych usług. Aktualnie do najpopularniejszych rozwiązań tej klasy należą Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) i SimpleDB;
- środowisko programowe jako usługa (ang. *Platform as a Service* – PaaS) – oznacza usługę polegającą na udostępnieniu wirtualnego środowiska pracy programistom. W tym przypadku sieć chmurowa stanowi platformę dla

systemów (a nie tylko pojedynczego oprogramowania). Aktualnie najlepszym przykładem rozwiązań PaaS jest Google App Engine.

- oprogramowanie jako usługa (ang. *Software as a Service* – SaaS) – oznacza dostęp do dedykowanych aplikacji uruchamianych pod nadzorem dostawcy usługi. Obecnie oznacza to, że aplikacje są przechowywane i dostarczane online za pomocą przeglądarki internetowej, która oferuje tradycyjną funkcjonalność pulpitu. Najbardziej znanymi przykładami SaaS są Google Docs, Gmail and MySAP.

Z przedstawionego wyżej podziału można wyciągnąć jasny wniosek, iż podstawą dla działania jakiegokolwiek formy usług uruchamianych w sieciach chmurowych jest klasa usług IaaS. Zależność pomiędzy klasami usług, potwierdzającą przedstawiony wyżej wniosek, zobrazowano na rys. 1.

Metody wdrażania struktur sieci chmurowych

Konfiguracja i wdrożenie sieci chmurowych może być realizowane w trzech podstawowych konfiguracjach, uzależnionych od zasad dostępu i kontroli korzystania z usług [4]. Są to odpowiednio:

- publiczne sieci chmurowe (ang. *public clouds*);
- prywatne sieci chmurowe (ang. *private clouds*). W przypadku integracji kilku chmur prywatnych określa się je mianem sieci chmurowych społecznościowych (ang. *community cloud*);
- hybrydowe sieci chmurowe (ang. *hybrid cloud*). Rosnąca liczba rozwiązań należących do tej klasy doprowadziła do wyodrębnienia coraz popularniejszego podtypu, określanego jako struktury chmur połączonych (ang. *combined cloud*).

System opisany w dalszej części artykułu służy wdrażaniu i uruchamianiu prywatnych sieci chmurowych. Przegląd rozwiązań dla sieci chmurowych,

Streszczenie: Artykuł prezentuje środowisko do szybkiego uruchamiania i testowania systemów chmur sieciowych. Główny nacisk położony jest na minimalizację niezbędnych zasobów sprzętowych przy jednoczesnym zachowaniu możliwości łatwej rozbudowy systemu. Za proponowane rozwiązanie zapewnia możliwość korzystania ze wszystkich kluczowych cech systemu Eucalyptus, które mają wpływ na bezpieczeństwo i elastyczność współczesnych usług uruchamianych w sieciach chmurowych. Wykorzystanie technik wirtualizacji umożliwiło zdefiniowanie całego środowiska na pojedynczym systemie komputerowym, co zdecydowanie przyspiesza proces wdrażania i upraszcza testowanie nowoczesnych struktur sieci chmurowych.

Słowa kluczowe: sieci chmurowe, Eucalyptus, wirtualizacja

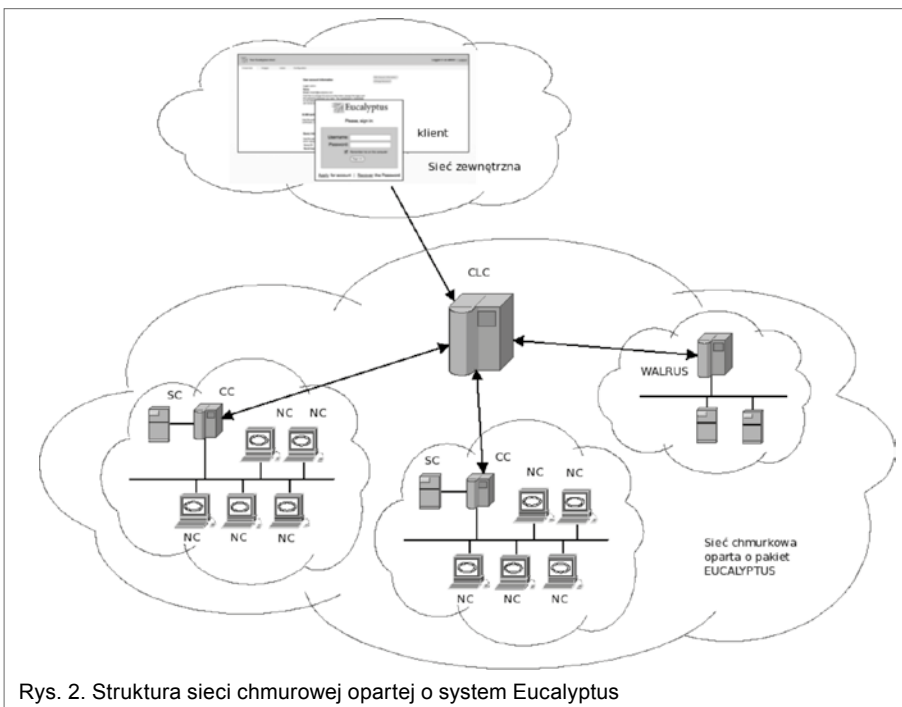
🇬🇧 CLOUD COMPUTING TESTBED

Abstract: The article presents the testbed for fast prototyping of the cloud computing structures. The main aim of our solution is the minimalization of the required hardware resources as well as an ease of system expansion. The testbed based on the Eucalyptus packet and it preserves all its specific features.

Keywords: cloud computing, Eucalyptus, virtualization

publicznych, jak i hybrydowych, można znaleźć w [9, 10].

Sieci chmurowe prywatne, które stanowią podstawę dalszych rozważań, zapewniają użytkownikom dostęp do zasobów zgromadzonych wewnątrz infrastruktury sieciowej i programowej danej



organizacji. Sposób zarządzania dostępem i korzystania z zasobów jest analogiczny, jak w przypadku chmur publicznych. Jednak ze względu na to, że zasoby są skupione wewnątrz infrastruktury jednej organizacji, możliwe jest zapewnienie wyższych lub niestandardowych wymogów odnośnie do bezpieczeństwa i wydajności przetwarzania oraz przechowywania danych. Planując wdrożenie usług wykorzystujących infrastrukturę sieci chmurowych, szczególną uwagę poświęca się właśnie zagadnieniu bezpieczeństwa zasobów i danych. To zagadnienie jest uważane za najistotniejszy czynnik ograniczający upowszechnienie technologii sieci chmurowych, szczególnie wśród klientów biznesowych [8]. Obawa

przed nieuprawnionym dostępem do danych, utratą kontroli nad wrażliwymi elementami działalności przedsiębiorstwa czy też uzależnieniem od stabilności i dostępności łączy teleinformatycznych są przeszkodami najczęściej wymienianymi przez potencjalnych użytkowników technologii sieci chmurowych. Sieci prywatne, w opinii większości analityków rynku IT, są najlepszą odpowiedzią na przedstawione wyżej obawy ze względu na ich

usytuowanie w ramach infrastruktury pojedynczej organizacji [8]. W związku z tym rośnie obecnie zainteresowanie metodami szybkiego i odpowiednio elastycznego tworzenia środowisk testowych dla chmur prywatnych. Jednocześnie wymieniony wcześniej podział ze względu na klasy usług jasno wskazuje, iż fundamentem wszystkich prac w obszarze przetwarzania chmurowego są usługi IaaS. Z tego też powodu rozwiązanie, opisane w dalszej części artykułu, poświęcone jest środowisku wdrażania klasy IaaS w strukturach chmur prywatnych.

System Eucalyptus

Architektura systemu Eucalyptus pozwala na budowę struktur chmur prywatnych zgodnych z szeroko akceptowanym standardem Amazon EC2. Oznacza to, że użytkownicy tego systemu wykorzystują zasoby chmury w ten sam sposób, jak zasoby chmury publicznej oferowanej przez firmę Amazon. Pozwala to na prostą integrację tego rozwiązania w ramach projektów chmur hybrydowych [3].

Struktura systemu Eucalyptus przedstawiona jest na rys. 2 i składa się z czterech elementów:

- kontrolera węzła NC (ang. *Node Controller*);
- kontrolera klastra CC (ang. *Cluster Controller*);
- kontrolera magazynowania Walrus (ang. *Storage Controller*);
- kontrolera chmury CLC (ang. *Cloud Controller*).

Kontroler węzła jest zasobem fizycznym (zazwyczaj pojedynczym hostem), na którym uruchamiane są poszczególne instancje maszyn wirtualnych. W najprostszym wypadku wystarczy jeden taki kontroler, ponieważ – w zależności od posiadanych zasobów sprzętowych – może on być podstawą do uruchomienia jednej lub więcej instancji maszyn wirtualnych. Zbór NC połączony jest w ramach sieci prywatnej, zarządzanej przez kontroler klastra CC.

Kontroler CC odpowiedzialny jest za trzy podstawowe funkcje: planowanie przydziału zasobów NC dla poszczegól-

reklama



gólnych zadań, nadzór nad instancjami maszyn wirtualnych oraz zbieranie i raportowanie informacji o stanie realizacji zadań i stopniu wykorzystania zasobów. Ostatnie z tych zadań pozwala na ocenę możliwości realizacji poszczególnych zadań i informowanie kontrolera chmury CLC o bieżącym stanie wykorzystania zasobów.

Razem z CLC działa kontroler magazynowania Walrus. Dostarcza on usługę przechowywania danych (obrazów maszyn wirtualnych, jak i danych użytkowników) zgodną z interfejsem Amazon's S3. W każdym systemie Eucalyptus musi być uruchomiony jeden kontroler CLC i jeden Walrus. Kontroler CLC jest odpowiedzialny za cały proces obsługi żądania dostępu do zasobów zgłaszanego przez użytkownika (autentykację, kontrolę przestrzegania reguł SLA (ang. *Service Level Agreement*), monitoring sesji), jak również za zadania planowania na poziomie klastra przydziału zasobów dla zgłoszonych żądań. Innymi słowy, CLC jest pomostem pomiędzy narzędziami udostępnionymi użytkownikowi a wewnętrzną strukturą planowania, przydziału i realizacji zadań zgłoszonych przez użytkowników [3, 5].

Cechy systemu Eucalyptus

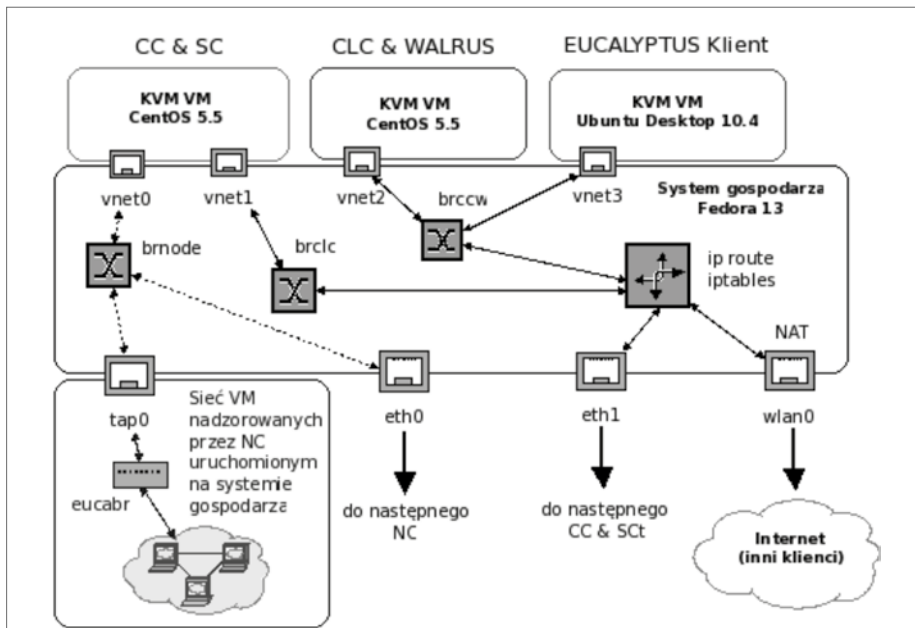
Eucalyptus zapewnia infrastrukturę sieciową, na której możliwe jest tymczasowe uruchamianie zasobów wirtualnych w postaci grupy maszyn wirtualnych VM (ang. *Virtual Machines*). Grupy VM lokowane są w wydzielonych podsieciach prywatnych, odseparowanych od ruchu w sieci łączącej poszczególne NC wchodzące w skład klastra [5].

Eucalyptus może zostać skonfigurowany w jednym z czterech trybów sieciowych (ang. *networking modes*): managed, managed-noVLAN, static oraz system. Poszczególne tryby określają sposób organizacji infrastruktury IaaS i definiują m.in. wykorzystanie przedstawionych poniżej narzędzi wewnętrznych systemu Eucalyptus [5].

Sterowanie IP (ang. *IP Control*) jest rozwiązaniem dostępnym we wszystkich trybach, z wyjątkiem trybu system. Dzięki temu mechanizmowi Eucalyptus przypisuje automatycznie adresy IP do poszczególnych VM. W trybie system należy natomiast zapewnić zewnętrzny serwer DHCP (ang. *Dynamic Host Configuration Protocol*). Narzędzie to, w połączeniu z elastycznymi

Tabela 1. Charakterystyka trybów sieciowych w pakiecie Eucalyptus

Tryb sieciowy	System	Static	Managed	Managed-noVLAN
Usługa DHCP. Zewnętrzna/wewnętrzna usługa pakietu Eucalyptus	tak/nie	nie/tak	nie/tak	nie/tak
Izolacja instancji VM	nie	nie	tak	nie
Prywatne/elastyczne IP	nie/nie	nie/nie	tak/tak	tak/tak
Grupy bezpieczeństwa	nie	nie	tak	tak



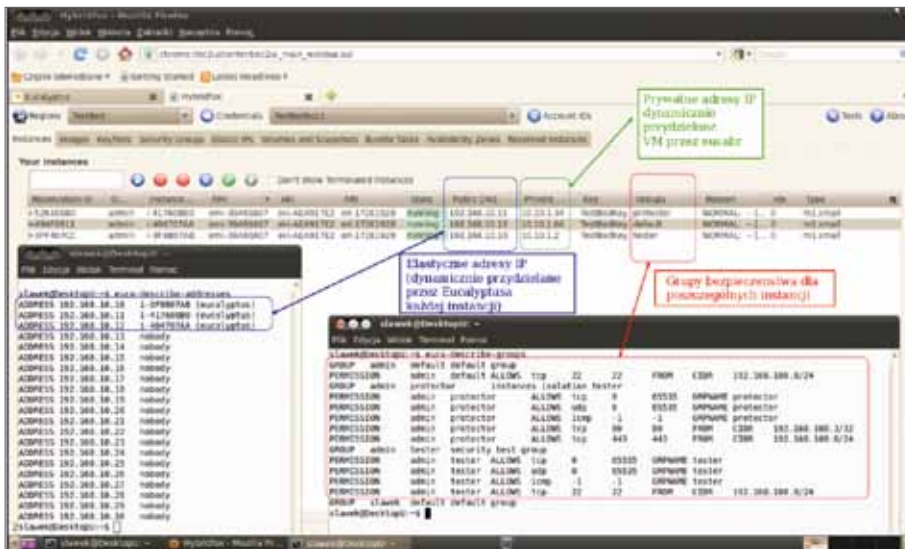
Rys. 3. Struktura chmury IaaS na bazie systemu Eucalyptus

IP, pozwala na dynamiczne zarządzanie usługami w sieci chmurowej i z tego względu odgrywa istotną rolę w obecnie projektowanych strukturach chmur prywatnych.

Grupy bezpieczeństwa (ang. *Security Groups*) są narzędziem, którego celem stosowania jest zdefiniowanie zestawu zasad sieciowych, jakie stosowane są do wszystkich VM w ramach danej grupy. W podstawowej konfiguracji zasady te określają prawa dostępu do poszczególnych VM, a tym samym do określonych zasobów. Można zatem stwierdzić, iż grupy bezpieczeństwa w pakiecie Eucalyptus są narzędziem do budowy specyficznych, z punktu widzenia wymagań, usług w sieciach chmurowych, zabezpieczeń typu firewall chroniących poszczególne instancje maszyn wirtualnych. Poprawne korzystanie z tego narzędzia ma kluczowe znaczenie dla sterowania bezpieczeństwem dostępu do usług, a tym samym do zasobów [8]. W prezentowanym środowisku domyślne ustawienie grup bezpieczeństwa umożliwia do-

stęp do obrazów systemów operacyjnych użytkownika wyłącznie poprzez protokół SSH (ang. *Secure Socket Shell*). Poprzez właściwą konfigurację grup bezpieczeństwa można określić zasady dostępu dla innych użytkowników, jak i adresów, spod których urządzenia inicjalizują daną usługę. Grupy bezpieczeństwa mogą być stosowane w trybach managed oraz managed-noVLAN.

Elastyczne IP (ang. *Elastic IP*) jest narzędziem pozwalającym na powiązanie publicznego adresu użytkownika z adresami VM w ramach danej usługi. Elastyczne adresy IP są statycznymi adresami IP stosowanymi w celu realizacji dynamicznych zmian struktury przetwarzania w sieciach chmurowych. Specyfika elastycznych adresów IP polega na tym, iż są one przypisane do użytkownika, a nie do konkretnej instancji maszyny wirtualnej. Dzięki temu ewentualne awarie, jak i modyfikacje struktury wewnętrznej zasobów są niewidoczne dla klienta ze względu na dynamiczne zmiany powiązań adresów wewnętrz-



Rys. 4. Implementacja grup bezpieczeństwa i elastycznych IP w prezentowanym środowisku testowym IaaS

nych systemu chmurowego ze stałym, elastycznym adresem IP. W prezentowanym środowisku elastyczne IP może być przepisane w danym momencie tylko do jednego adresu VM. Elastyczne IP są dostępne wyłącznie w trybach managed oraz managed-noVLAN.

Innym narzędziem wewnętrznym systemu Eucalyptus jest izolacja maszyn wirtualnych (ang. *VM Isolation*). Narzędzie to pozwala na wymuszenie izolacji ruchu pomiędzy grupami bezpieczeństwa, bez konieczności umieszczania ich w różnych podsieciach. Narzędzie to jest dostępne wyłącznie w trybie managed. Zestawienie omówionych narzędzi w odniesieniu do dostępnych trybów sieciowych przedstawiono w tabeli 1.

Środowisko wdrażania i testowania IaaS dla chmury prywatnej powinno dawać możliwość wykorzystania wszystkich cech i narzędzi wewnętrznych pakietu Eucalyptus. Na podstawie przytoczonych wyżej informacji środowisko takie powinno zawierać również wszystkie komponenty systemu przy jednoczesnej możliwości szybkiej i prostej jego rozbudowy. Innymi słowy, powinno dawać możliwość wykorzystania wszystkich narzędzi i opcji konfiguracyjnych, łącznie z najbardziej rozbudowanym trybem managed. Takie założenia spełnia proponowane środowisko.

Struktura środowiska wdrożeniowego

Na podstawie dokonanej przeglądu literatury, jak i opisów autorów systemu

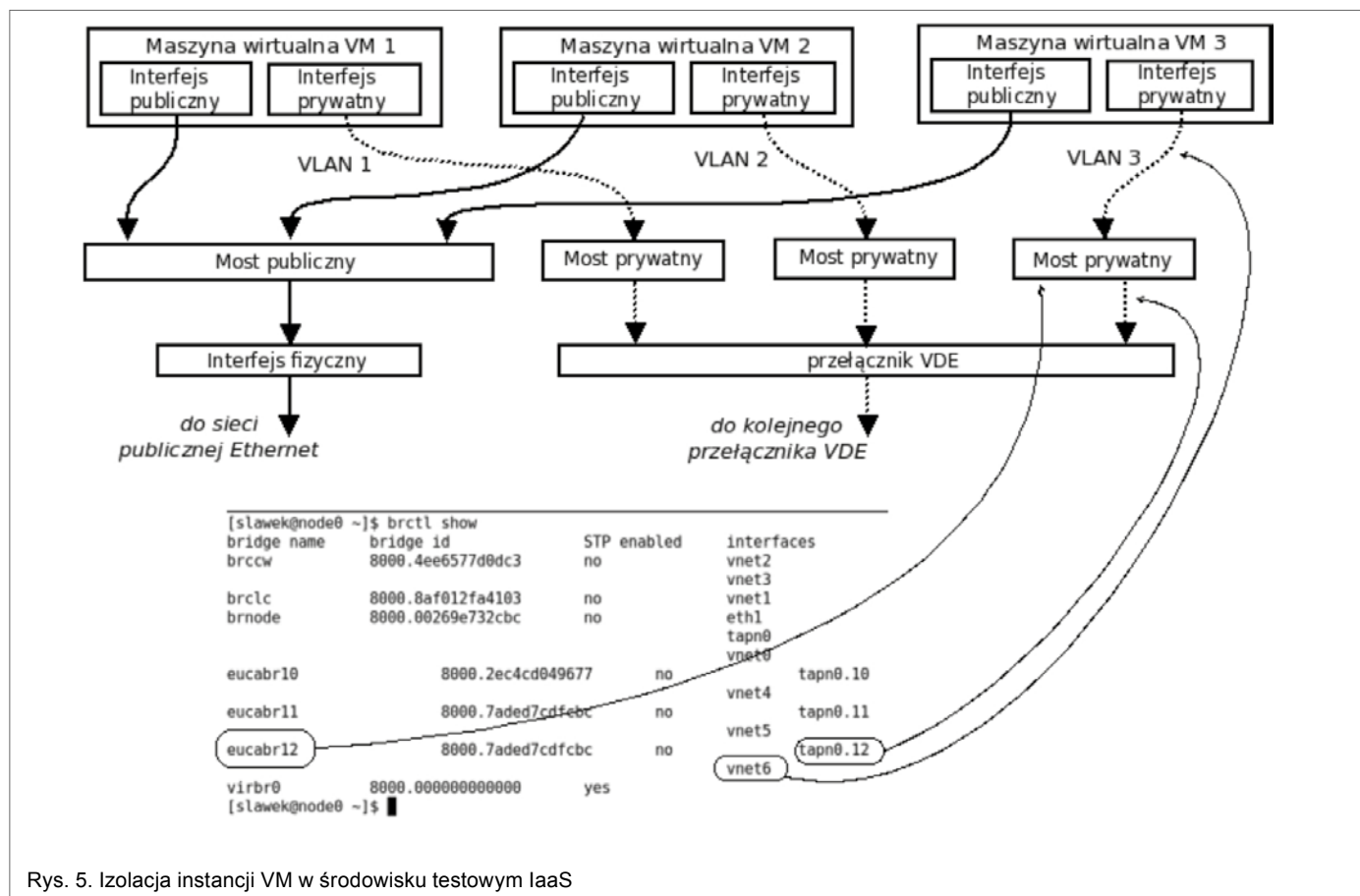
Eucalyptus, realizacja pełnej struktury chmury prywatnej, pracującej w trybie managed, wymaga zastosowania przynajmniej dwóch maszyn fizycznych: jednej dla potrzeb implementacji NC oraz drugiej, na której uruchomione zostałyby pozostałe komponenty, tj. kontrolery CC, CLC oraz Walrus [6]. Proponowane środowisko wdrożeniowe omija konieczność stosowania wielu maszyn. Możliwość wykorzystania dostępnych mechanizmów wirtualizacji zasobów pozwala na uruchamianie prostych struktur IaaS na pojedynczej maszynie, a jednocześnie na rozbudowywanie ich w razie potrzeby do wymaganej wielkości bez konieczności konfigurowania wszystkich elementów systemu od podstaw. Wykorzystana platforma sprzętowa jest powszechnie dostępna na komputerach klasy desktop, a nawet laptop, więc dodatkową cechą proponowanego rozwiązania jest jego ekonomiczność.

Podstawą do budowy środowiska testowego był komputer PC wyposażony w czterordzeniowy procesor firmy Intel ze wsparciem dla sprzętowej wirtualizacji, 8 GB pamięci RAM, pamięć dyskową o pojemności 500 GB oraz 3 interfejsy sieciowe. Zasoby te, z wykorzystaniem wirtualizacji opartej o hypervisor KVM zostały, przypisane w następujący sposób do elementów struktury systemu Eucalyptus:

- kontroler węzła (NC) – gospodarz KVM (4 rdzenie, 8 procesorów logicznych, współdzielonych), 4 GB RAM (współdzielona z gośćmi), 60 GB HDD (współdzielona z gośćmi), system Fedora 14 (x86_64);

Tabela 2. Specyfikacja połączeń sieciowych środowiska wdrażania prywatnej sieci chmurowej klasy IaaS

Składnik systemu Eucalyptus	NC	CC & SC	CLC & WALRUS
Interfejs sieciowy	eth0 – 1 Gbit, fizyczny interfejs Ethernet	eth0 – VM (sterownik virtio)	eth0 – VM (sterownik virtio)
	eth1 – 1 Gbit, fizyczny interfejs Ethernet	eth1 – VM (sterownik virtio)	
	wlan0 – IEEE11n, fizyczny interfejs bezprzewodowy		
	tap0 – interfejs wirtualny		
Konfiguracja interfejsów	eth0 – łącze do dodatkowych NCs, konfiguracja statyczna, połączony z mostem „brnode”	eth0 – łącze do sieci prywatnej NC (poprzez most „brnode”)	eth0 – łącze do sieci publicznej CLC (poprzez most „brccw”)
	eth1 – łącze do dodatkowych CC oraz SC, konfiguracja statyczna, połączony z mostem „brclc”	eth1 – łącze do sieci publicznej CC (poprzez most „brclc”),	
	wlan0 – łącze do sieci zewnętrznej, opcjonalna konfiguracja NAT		
	tap0 – łącze do podstawowego NC, połączony z mostem „eucabr”, a za jego pośrednictwem z instancjami maszyn wirtualnych		



Rys. 5. Izolacja instancji VM w środowisku testowym IaaS

- kontroler klastra oraz kontroler magazynu (CC & SC) – gość KVM (4 rdzenie, 8 procesorów logicznych, współdzielonych), 1 GB RAM, 40 GB HDD SATA (sterownik virtio), system CentOS5.5 (x86_64);
- kontroler chmury oraz Walrus (CLC & WS) – gość KVM (4 rdzenie, 8 procesorów

- kontroler klastra oraz kontroler magazynu (CC & SC) – gość KVM (4 rdzenie, 8 procesorów logicznych, współdzielonych), 1 GB RAM, 40 GB HDD SATA (sterownik virtio), system CentOS5.5 (x86_64),
- host użytkownika – gość KVM (1 rdzeń, 2 procesory logiczne, współdzielone), 512 MB RAM, 10 GB HDD SATA (sterownik virtio), system Ubuntu 10.4 (x86_32).

Wewnętrzne połączenia zostały zrealizowane poprzez trzy mosty o nazwach, odpowiednio: brnode, brclc oraz brccw. Architektura środowiska testowego została przedstawiona na rys. 3, natomiast konfiguracja interfejsów i elementów sieciowych środowiska testowego przedstawiona jest w tabeli 2.

Weryfikacja działania

Przedstawione poniżej wyniki weryfikacji działania zaproponowanego środowiska do szybkiego wdrażania i testowania sieci chmurowych mają na celu potwierdzenie pełnej funkcjonalności rozwiązania w kontekście przedstawionych cech chmur prywatnych i pakietu Eucalyptus, tj. grup bezpieczeństwa, elastycznego IP oraz izolacji VM. Do celów zarządzania systemem testowym wykorzystano dwa narzędzia programowe: pakiet Hybridfox [7] oraz program z interfejsem tekstowym euca_tools. Oba były zainstalowane na systemie gościnnym, którym był Ubuntu Desktop 10. Inni klienci mogą być podłączeni do systemu poprzez interfejs wlan0.

Na rys. 4 przedstawiono trzy instancje systemu Ubuntu uruchomione w testowym środowisku IaaS. Każda z nich przypisana jest do różnych grup bezpieczeństwa. W prawym dolnym rogu na rys. 4 znajduje się opis stworzonych grup (default, protector oraz tester). W lewym dolnym rogu znajduje się raport programu euca_tool, który potwierdza wykorzystanie mechanizmu elastycznych IP. Oprócz adresów prywatnych, Eucalyptus dynamicznie, bez udziału administratora, przypisał poszczególnym instancjom VM adresy publiczne. Dzięki temu użytkownicy mogą z łatwością łączyć się i korzystać z przydzielonych zasobów.

Interfejsy prywatne wszystkich instancji maszyn VM są połączone za pomocą narzędzia VDE (ang. *Virtual Distributed Ethernet*) [8]. Utworzony most VDE łączy interfejsy TAP przypisane poszczególnym VM z wykorzystaniem techniki VLAN. Określony numer VLAN-u łączy wszystkie VM przypisane do zadania zgłoszonego przez danego użytkownika. Zaimplementowany sposób wykorzystania dynamicznej infrastruktury VLAN w środowisku testowym przedstawiony jest na rys. 5.

Podsumowanie

Struktury i usługi w sieciach chmurowych łączą w sobie wiele mechanizmów z obszaru inżynierii sieciowej, jak i oprogramowania. Zaproponowane rozwiązanie środowiska do szybkiego wdrażania i testowania systemów klasy IaaS może stać się przydatne w wielu badaniach i wdrożeniach sieci chmurowych. Ponadto należy podkreślić, iż nie proponowano dotąd rozwiązania obejmującego wyłącznie pojedynczy system komputerowy, który jednocześnie z łatwością pozwalałby na rozbudowę do pełnowymiarowych struktur IaaS. Możliwość zaimplementowania wszystkich podstawowych cech chmur prywatnych czyni opisane środowisko wdrożeniowe przydatnym również w pracach nad rozwiązaniami z obszaru PaaS i SaaS.

Bibliografia

- [1] VAQUERO L.M., RODERO-MERINO L., CACERES J., LINDER M.: *A Break in the Clouds: Towards a Cloud Definition*, ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009, pp. 50–55.
- [2] FOSTER I., ZHAO Y., RAICU I., LU S.: *Cloud Computing and Grid Computing 360-Degree Compared*, Grid Computing Environments Workshop, 2008, pp. 1–10.
- [3] NURMI D., WOLSKI R., GRZEGORCZYK C., OBERTELLI G., SOMAN S., YOUSEFF L., ZAGORODNOV D.: *The Eucalyptus Open-source Cloud-computing System*, 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID), Vol. 0, 2009, pp. 124–131.
- [4] ARMBRUST M., FOX A., GRIFFITH R., JOSEPH A.D., KATZ R., KONWINSKI A., LEE G., PATTERSON D., RABKIN A., STOICA I., ZAHARIA M.: *Above the Clouds: A Berkeley View of Cloud Computing*, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, wrzesień 2011.
- [5] JOHNSON D., MURARI K., RAJU M., SUSEENDRAN R.B., GIRIKUMAR Y.: *Eucalyptus Beginner's Guide – UEC Edition*, CSS Corp. 2010, <http://www.csscorp.com/eucauebook>, lipiec 2011.
- [6] Eucalyptus Administrator's Guide (2.0), <http://open.eucalyptus.com/wiki/>, wrzesień 2011.
- [7] Hybridfox, <http://code.google.com/p/hybridfox/>, wrzesień 2011.
- [8] ROBINSON N., VALERI L., CAVE J., STARKEY T., CREESE S., HOPKINS P.: *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Raport Unit F.5, Directorate-General Information Society and Media, European Commission, 2010.
- [9] GROSSMAN R. ET AL.: *The Open Cloud Testbed: A Wide Area Testbed for Cloud Computing Utilizing High Performance Network Services*. <http://arxiv.org/ftp/arxiv/papers/0907/0907.4810.pdf>, wrzesień 2011.
- [10] HP Technical Report, HP-2009-122: Open Cirrus Cloud Computing Testbed: Federated Data Centers for Open Source Systems and Services Research. <http://OpenCirrus.org>, wrzesień 2011.

dr inż. Sławomir Przyłucki,
mgr inż. Daniel Sawicki – Katedra Elektroniki,
Politechnika Lubelska, Lublin,
e-mail: spg@politechnika.lublin.pl,
sawi@politechnika.lublin.pl;
dr inż. Dariusz Czerwiński –
Instytut Podstaw Elektrotechniki
i Elektrotechnologii,
Politechnika Lubelska, Lublin;
e-mail: d.czerwinski@pollub.pl