Cloud Computing (wycofana)

Usługa Cloud Computing została wycofana

Informacje podstawowe

Cloud Computing - obliczenia w chmurze - to rodzaj korzystania z mocy obliczeniowej i przestrzeni pamięci masowej polegający na tym, że użytkownik uzyskuje do swojej dyspozycji zestaw maszyn wirtualnych z uprawnieniami administratora do systemu operacyjnego.Maszyny pracują w wyizolowanej sieci lokalnej z możliwością udostępnienia wyselekcjonowanych usług publicznie.Dostęp do maszyn uzyskuje się za pomocą tunelu VPN. Maszyny mogą mieć podłączone odpowiednie zasoby dyskowe bezpośrednio, bądź użytkownik może korzystać z przestrzeni ogólnodostępnej. Odpowiedzialność za zarządzanie maszynami leży w gestii użytkownika, natomiast PL-Grid prowadzi monitorowanie mające na celu prawidłowe funkcjonowanie i bezpieczeństwo infrastruktury. Obecnie platforma Cloud Computing jest na etapie prototypowania i możliwe jest jedynie korzystanie z niej na zasadzie testowania.

Lokalizacja	ACK CYFRONET AGH
Nazwa systemu	`Zeus`
Nazwa maszyny dostępowej	`ui.cyfronet.pl`
Port dostępowy	22
Kontakt (maszyna dostępowa)	cyfronet-lcg2@helpdesk.plgrid.pl
Kontakt (usługa Cloud)	Cloud@helpdesk.plgrid.pl

Uzyskanie dostępu

Warunki wstępne.

W celu uzyskania dostępu do platformy należy uprzednio posiadać:

- konto użytkownika w Portalu PL-Grid - Zakładanie konta w portalu PL-Grid
- aktywny dostęp do UI w Cyfronecie - Aktywacja i rezygnacja z usług
- Zarejestrowany w portalu PL-Grid certyfikat PL-Grid CA lub Simple CA - Aplikowanie, rejestracja i użycie certyfikatu

Składanie wniosku o usługę

Przed rozpoczęciem pracy z platformą “Cloud Computing” należy uzyskać do niej dostęp z poziomu Portalu.

W tym celu należy:

- Zalogować się na portal PL-Grid
- Przejść do zakładki “Moje konto”
- W okienku “Usługi / Aplikuj o usługę/Dostęp do Platformy Cloud Computing Cyfronet” kliknąć “Aplikuj o usługę”

Po aktywacji usługi przez administratora można rozpocząć używanie platformy zgodnie z poniższą instrukcją.

Zarządzanie instancjami maszyn wirtualnych

Zestaw aplikacji klienckich umożliwiających zarządzanie usługą został udostępniony na UI w ACK CYFRONET AGH. Pracę należy rozpocząć od zalogowania się za pomocą klienta SSH na ui.cyfronet.pl – więcej informacji o logowaniu

Ładowanie modułu

Uwaga

Poprzednio stosowany moduł cloud/one-client jest nadal dostępny dla zachowania zgodności wstecznej - jednak ze względu na wygodę zalecamy moduł opisany poniżej.

Jednocześnie informujemy, że moduł cloud/one-client może zostać usunięty w przyszłości.

Przed rozpoczęciem pracy z klientem niezbędne jest załadowanie modułu cloud/rest-api-client. Operację tę można przeprowadzić za pomocą polecenia:

> *module add cloud/rest-api-client*

...system powinien odpowiedzieć komunikatem:

> *'cloud/rest-api-client/1.0' load complete.*
>
> *'ruby/1.8.7-p330.el5' load complete.*

Generowanie certyfikatu "proxy"

> **Uwaga**
>
> Prosimy do generowania certyfikatu stosować polecenie "voms-proxy-init", **nie** "grid-proxy-init". Osoby nie posiadające certyfikatu mogą skorzystać z poprzedniej wersji nie wymagających certyfikatów dostępnej po załadowaniu modułu cloud/one-client lecz wersja ta zostanie niebawem usunięta.

Wykonananie jakiejkolwiek operacji za pomocą w/w modułu wymaga uprzedniego załadowania modułu cloud. W tym celu prosimy wykonać polecenie:

> *voms-proxy-init*

Jeśli posiadamy prowidłowo zlokalizowany certyfikat gridowy i klucz do niego zostaniemy poproszeni o hasło a następnie, po podaniu prawidłowego hasła, poinformowani o sukcesie procedury generowania "proxy":

> *Enter GRID pass phrase for this identity:*
>
> *Created proxy in /tmp/x509up_uXXXXX.*
>
> *Your proxy is valid until ...*

Od tego momentu kolejne polecenia nie będą wymagać podawania hasła (z wyjątkiem polecnia oneport).

Przeglądanie listy dostępnych obrazów systemów operacyjnych

W ramach usługi dostępny jest zestaw obrazów systemów operacyjnych, które mogą zostać uruchomione przez użytkowników jako instancje maszyn wirtualnych. Ponieważ podstawową cechą usługi jest jej elastyczność lista ta może dynamicznie się zmieniać dostosowując się do wymagań.

W związku z tym przed utworzeniem nowego szablonu maszyny zalecamy zapoznanie się z aktualną listą poprzez wywołanie komendy:

> *oneimage list*

Jeżeli certyfikaty zostały zainstalowane zgodnie z instrukcją, to powinna ukazać się lista dostępnych obrazów.

Najistotniejsze pola oznaczone są jako “ID” - identyfikator obrazu, który należy zapamiętać/zapisać, gdyż jest on niezbędny do stworzenia szablonu wirtualnej maszyny i “NAME” - czyli nazwa obrazu umożliwiająca odnalezienie właściwego obrazu.

W przypadku generycznych obrazów systemów określa ona nazwę systemu operacyjnego / dystrybucji oraz wersję. W przypadku specjalizowanych obrazów na potrzeby konkretnych zespołów naukowych (np. zawierających specjalistyczne oprogramowanie) nazwa ta jest indywidualnie uzgadniania z zespołem.

Przeglądanie listy dostępnych wirtualnych sieci.

Podobnie jak identyfikator obrazu – identyfikator wirtualnej sieci jest niezbędny do stworzenia szablonu używanego do uruchamiania instancji maszyn wirtualnych.

Listę sieci wirtualnych można uzyskać za pomocą komendy:

> *onevnet list*

W odpowiedzi powinna zostać zwrócona tabelka podobna do poprzedniej – również zawierająca pola ID i NAME. Wszystkie osoby posiadające dostęp do usługi mają dostęp do sieci o ID 0 (LAN_PLG_COMMON) - jest to wspólna sieć przydzielające prywatne adresy IP (dostęp z zewnątrz możliwy jest poprzez opisany poniżej mechanizm przekierowania portów TCP/UDP lub poprzez usługę dostępową PL-Grid VPN). Niektóre osoby mogą posiadać dodatkowo dostęp do wydzielonych sieci - będą one wtedy wyświetlone również w odpowiedzi na powyższe polecenie.

Tworzenie szablonu maszyny wirtualnej.

Przed uruchomieniem maszyny wirtualnej konieczne jest istnienie jej szablonu. Określa on m.in. powiązanie między ID obrazu systemu operacyjnego, ID wirtualnej sieci oraz kluczem publicznym, który ma zostać umieszczony w maszynie (w celu umożliwienia zalogowania się na maszynę przez SSH z użyciem klucza prywatnego). Dlatego też dla każdej w/w trójki musi zostać utworzony nowy szablon, jednak później może on być używany do uruchomienia wielu instancji maszyn wirtualnych (tego samego typu).

W celu ułatwienie tworzenia i rejestracji szablonów udostępniliśmy specjalny skrypt, który należy uruchomić w następujący sposób:

> *onegentempl.sh*

Na kolejne pytania skryptu należy odpowiedzieć zgodnie z poniższymi wskazówkami:

- “Enter Image ID” - ID obrazu systemu operacyjnego
- “Enter Network ID” - ID sieci wirtualnej

… jeśli nie posiadamy wcześniej wygenerowanej pary kluczy RSA w domyślnej lokalizacji (~/.ssh/id_rsa) skrypt zaproponuje nam jej utworzenie (“No RSA key found. Press <ENTER> to generate or Ctrl+C to terminate.”) – krok ten jest niezbędny do rejestracji szablonu, dlatego należy potwierdzić operację wciskając <ENTER> - uruchomiony zostanie standardowy mechanizm generowania pary kluczy, który wymaga podania następujących informacji:

- “Enter file in which to save the key...” - należy pozostawić puste pole i wcisnąć <ENTER> w celu wybrania domyślnej lokalizacji;
- “Enter passphrase (empty for no passphrase)” - należy podać silne hasło – mimo sugestii aplikacji generującej klucze o możliwości utworzenia klucza bez hasła, w tym przypadku należy BEZWZGLĘDNIE stosować hasło, gdyż klucz ten będzie umożliwiał logowanie na maszyny wirtualne z uprawnieniami superużytkownika (root) ;
- “Enter same passphrase again” - należy ponownie podać powyższe hasło.

W odpowiedzi system powinien wyświetlić ID zarejestrowanego szablonu, który będzie potrzebny do uruchomienia maszyny wirtualnej. W przyszłości możliwe będzie odnalezienie tego identyfikatora zgodnie z procedurą opisaną w kolejnym punkcie.

Przeglądanie listy szablonów maszyn wirtualnych

Jeśli już wcześniej utworzyliśmy szablon maszyny wirtualnej, a nie wiemy jakie posiada on ID możemy uzyskać tę informację za pomocą komendy:

> *onetemplate list*

W odpowiedzi powinniśmy uzyskać tabelę podobną jak poprzednio zawierającą m.in. pola ID i NAME. ID jest poszukiwanym identyfikatorem maszyny, natomiast pole NAME utworzonego w/w skryptem szablonu zawsze zaczyna się od sekwencji AUTO<ID>- gdzie <ID> zastąpione jest numerem obrazu – np. AUTO3-... .

Usuwanie szablonu maszyny.

Jeśli jesteśmy pewni, że nie będziemy potrzebowali tworzyć kolejnych maszyn wirtualnych danego typu możemy usunąć wcześniej utworzony szablon. W tym celu możemy posłużyć się poleceniem:

> *onetemplate delete <ID>*

...zastępując <ID> przez właściwy identyfikator szablonu.

Uruchamianie instancji wirtualnej maszyny.

W celu uruchomienia instancji wirtualnej maszyny na podstawie uprzednio utworzonego szablonu należy wykonać polecenie:

> *onetemplate instantiate <ID>*

…zastępując <ID> przez właściwy identyfikator szablonu.

Jeśli operacja ta przebiegnie poprawnie system zwróci wartość „VM ID”, czyli identyfikatora maszyny wirtualnej. Jest on niezbędny m.in. do uzyskiwania informacji o maszynie (takiej jak jej status, przydzielony adres IP), a także np. do zatrzymania i usunięcia maszyny.

Przeglądanie listy wirtualnych maszyn.

Użytkownik ma możliwość przeglądania listy maszyn do których posiada uprawnienia (w szczególności – maszyn, które sam uruchomił). W tym celu należy zastosować komendę:

> *onevm list*

Zwróci ona listę maszyn wirtualnych w formie tabeli (analogicznie jak poprzednie komendy „list”). Tabela ta zawiera jednak jedynie podstawowe informacje o każdej maszynie (takie jak ID, nazwę, ilość przydzielonej pamięci RAM itp.). Procedura pozwalająca na uzyskanie bardziej szczegółowych informacji (w tym adresu IP) opisana jest w kolejnej sekcji.

Najistotniejszym polem w tabeli (poza ID) jest pole STAT – dzięki niemu możemy szybko sprawdzić czy nasza maszyna została już przygotowana i uruchomiona – informuje o tym wpis „runn” w w/w polu.

Uzyskiwanie szczegółowych informacji o maszynie wirtualnej.

W celu uzyskania szczegółowych informacji, takich jak adres IP niezbędny do zalogowania się na maszynę wirtualną, należy wykonać polecenie:

> *onevm show <ID>*

… zastępując jak zwykle ID przez właściwy identyfikator – tym razem maszyny wirtualnej.

W odpowiedzi system powinien zwrócić wiele informacji, z których najistotniejsze dla użytkownika znajdują się w sekcji podobnej do poniższej:

> *NIC=[*
>
> *BRIDGE=”v…",*
>
> *IP="172.16.xx.xx",*
>
> *MAC="82:84:00:xx:xx:xx",*
>
> *NETWORK="LAN_PLG_COMMON",*
>
> *NETWORK_ID="0",*
>
> *VLAN="XX"]*

Szczególnie istotne jest oczywiście pole IP – niezbędne do uzyskania dostępu do maszyny.

Przekerowanie portu TCP/UDP

W celu udostępnienia "na zewnątrz" usługi (np. SSH, HTTP) oferowanej przez oprogramowanie zainstalowane na maszynie wirtualnej możliwe jest przekierowanie portu/ów TCP i/lub UDP. Dokonać tego można za pomocą polecenia:

> *oneport -A -a <IP> -p <port> -P <protokól>*

gdzie <IP> - to otrzymany wg. wcześniej opisanego sposobu prywatny adres IP maszyny, <port> to numer portu jaki chcemy przekierować (22, 80 itp) a <protokół> to wybrany protokół - odpowiednio tcp lub udp . Opcję -P można pominąć dla TCP (jest to domyślny protokół) stąd np. w celu przekierowania usługi SSH możemy zastsować polecenie analogiczne do poniższego (IP trzeba zamienić na właściwe):

> *oneport -A -a 172.16.XX.XX -p 22*

W odpowiedzi powinniśmy otrzymać odpowiedź podobną do poniższej:

> *Port redirected:*
> *Public IP: 149.156.XX.XX*
> *Public port: YYYYY*
> *Private IP: 172.16.XX.XX*
> *Private port: 22*

...bardzo istotną informacją (wartą zapamiętania) jest zewnętrzny (publiczny) adres i port którym należy się posługiwać przy połączeniach z zewnątrz (przykład został zamieszczony poniżej).

Uzyskiwanie dostępu do maszyny wirtualnej.

Przed właściwą próbą logowania warto upewnić się czy maszyna jest w stanie „runn”.

Jeśli maszyna jest już uruchomiona można podjąć próbę zalogowania się na nią na konto root-a przez ssh:

> *ssh -p <portZewn> root@<IPZewn>*

UWAGA: <portZewn> i <IPZewn> są portem i adresem IP jaki uzyskaliśmy przekierowując port TCP 22 na maszynie wg instrukcji powyżej. Tj. dla powyższego przykładu <portZewn> to 6747 a <IPZewn> 149.156.XX.XX (na UI zostanie wyświetlone pełne IP) !!!

Klient ssh powinien zapytać nas o hasło do wygenerowanego podczas tworzenia szablonu klucza:

> *Enter passphrase for key…*

… należy zwrócić uwagę czy zapytanie ma formę podobną do powyższej – zapytanie o hasło na konto roota (a nie do w/w klucza prywatnego) jest nieprawidłowe i oznacza, że klient nie może użyć klucza. Należy się upewnić czy klucz prywatny w katalogu .ssh nie został gdzieś przeniesiony, skasowany oraz, że nie zmieniono jego uprawnień. Jeśli zaistniała któraś z powyższych operacji niezbędne będzie jej cofnięcie / przywrócenie klucza z kopii. Jeśli klucz został bezpowrotnie skasowany (nie ma jego kopii) oraz użytkownik nie utworzył innego dostępu do maszyny (inny klucz, hasło) odzyskanie dostępu do maszyny wymaga interwencji administratora platformy „Cloud Computing".

> **Uwaga**
>
> WAŻNE: Ze względu na stosowanie mechanizmu przekierowania portów - a co za tym idzie wspólnego zewnętrznego adresu IP dla wielu maszyn wirtualnych - klient OpenSSH w domyślnej konfiguracji po próbie dostępu do drugniej maszyny zgłosi ostrzeżenie dot. możliwego ataku Man-in-the-middle i odmówi dostępu - należy podjąć wtedy dodatkowe kroki opisane poniżej.

Informacja o możliwym ataku wygląda następująco:

> *@@@*
>
> *@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @*
>
> *@@@*
>
> *IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!*
>
> *Someone could be eavesdropping on you right now (man-in-the-middle attack)!*
>
> *[...]*
>
> *RSA host key for 149.156.XX.XX has changed and you have requested strict checking.*
>
> *Host key verification failed.*

...w tym przypadku jest to jednak "fałszywy alarm" wynikający z faktu, że w pliku known_hosts maszyny identyfikowane są tylko po adresie / nazwie bez portu. Obecnie domyślna konfiguracja nie pozwoli na zalogowanie się w przypadku wykrycia powyższej sytuacji nawet za pomocą klucza. Aby nie usuwać za każdym razem wpisu w known_hosts istnieją 2 rozwiązania opisane poniżej.

Ustawienie osobnych plików "KnownHosts" dla maszyn wirtualnych

Można ustawić każdej maszynie osobny plik do którego będą zapisywane "odciski palca" klucza poprzez dodanie do pliku ~/.ssh/config wpisu:

> *Host cloud_p6747*
>
> *HostName 149.156.XX.XX*
>
> *Port 6747*
>
> *UserKnownHostsFile ~/.ssh/cloud_p6747*

... oczywiście numer portu i nazwę pliku należy dostosować do konkretnego przypaku - numer portu jest to numer zwrócony przez powyżej opisane polecenia oneport a nazwa pliku musi być unikalna stąd sensowną wydaje się np. powyższa konwencja "cloud_p<portZewn>". Podobnie "Host" powinien być unikalny i nie konfliktujący z nazwami istniejących serwerów. Po wykonaniu powyższej operacji logujemy się na VM **nie w sposób wyżej podany** lecz poleceniem:

> *ssh root@cloud_p6747*

Oczywiście "cloud_p6747" należy zamienić na właściwą nazwę (podaną w pliku konfiguracyjnym). UWAGA: Jak widać powyżej nie używamy tu opcji -p gdyż numer portu zawarty jest w konfiguracji.

Wyłączenie opcji "StrictHostKeyChecking"

> **Uwaga**
>
> To rozwiązanie wydaje się łatwiejsze (wymaga tylko pojedyńczej zmainy pliku konfiguracyjnego) lecz wpływa negatywnie na bezpieczeństwo - stąd jest mniej polecane.

Należy **raz** dla danego IP (zewnętrznego) dodać do pliku ~/.ssh/config wpis:

```
Host 149.156.XX.XX
  StrictHostKeyChecking no
```

Umożliwi to logowanie za pomocą klucza pomimo zgłaszanego wyżej problemu. **W tym przypadku logujemy się jak opisano na początku tej sekcji** tj podając zewnętrzny adres IP (149.156.XX.XX) i port poprzez opcję '-p'.

W obu powyższych przypadkach po podaniu hasła do klucza użytkownik uzyskuje dostęp do konta root na maszynie wirtualnej.

Przygotowywanie maszyny wirtualnej do zapisania

Istnieje możliwość zapisania stanu maszyny wirtualniej. W wyniku tej operacji powstaje obraz systemu operacyjnego, analogiczny jak obrazy omawiane na początku tego dokumentu, który jest jednak dostępny tylko dla osoby która go zapisała. Obraz ten można użyć jak każdy inny do tworzenia nowych maszyn wirtualnych. Zawiera on wszystkie dane zapisane na lokalnym dysku maszyny - w tym zainstalowane oprogramowanie i dane użytkowników.

W celu zapisania maszyny należy ją najpierw oznaczyć do zapisania poleceniem:

```
onevm saveas <ID> <DISK_ID> <nazwa>
```

...gdzie <ID> jest identyfikatorem maszyny zwróconym podczas jej uruchomienia (można go też uzyskać wcześniej wspomnianym polecenie onevm list), <DISK_ID> jest identyfikatorem dysku wirtualnego - można go uzyskać poleceniem onevm show <ID>, jednak w obecnej wersji usługi maszyny uruchamiane są jedynie z jednym dyskiem stąd zwykle wystarczy podać jako <DISK_ID> 0, <nazwa> jest unikalną nazwą maszyny - najelpiej przyjąć konwencję prefixowania nazw swoim loginem np. plguser_SL63_1 (białe znaki są dopuszczalne ale trzeba je odpowiednio potraktować np. poprzez ujęcie w cydzysłów - stąd najprościej jest ich unikać) - przykładowe pełne wywołanie:

```
onevm saveas 45 0 plguser_SL63_1
```

... w odpowiedzi system powinien zwrócić ID zaalokowanego obrazu np.:

```
Image ID: 17
```

> **Uwaga**
>
> Powyższe polecenie NIE zapisuje obrazu a jedynie "oznacza go do zapisania podczas prawidłowego wyłączenia maszyny !!!

Powyższy fakt możena potwierdzić wyświetlając listę obrazów poprzez:

```
oneimage list
```

...na liście tej nowo zdefiniowany obraz będzie widoczny lecz będzie miał status (kolumna "STAT") ***lock*** , w przeciwieństwie do dostępnych maszyn mających status ***rdy*** lub ***used***.

W celu zakończenia procesu zapisu maszyny należy ją prawidłowo zatrzymać zgodne z opisem w kolejnej sekcji.

Zatrzymywanie (opcjonalnie z zapisaniem) instancji maszyny wirtualnej.

Gdy maszyna nie jest już potrzebna należy ją zatrzymać (co spowoduje jej usunięcie, z możliwością zapisu stanu jeśli maszyna została oznaczona "do zapisania") w celu zwolnienia zajmowanych przez nią zasobów. W tym celu należy wydać polecenie:

```
onevm shutdown <ID>
```

...gdzie <ID> - identyfikator maszyny. W ciągu kilkunastu sekund maszyna powinna zostać zatrzymana, (opcjonalnie zapisana) i usunięta z listy uruchomionych maszyn. Postęp ten można monitorować poprzez polecenie:

> *onevm list*

... a dokładnie monitorując kolumnę "STAT" - wpis ***runn*** oznacza że maszyna jest uruchomiona (proces zatrzymywania się nie rozpoczął), wpisy ***shut*** l ub ***epil*** oznaczają że maszyna jest wyłączana/zapisywana. Brak maszyny o danym ID na liście oznacza, że zostala ona zatrzymana.

Po zatrzymaniu maszyny która została oznaczona do zapisuje (poprzez "onevm saveas") status zapisanego obrazu powinien się zmienić z ***lock*** na ***rdy*** . Status ten można sprawdzić poleceniem:

> *oneimage list*

... patrząc na kolumnę "STAT". Zapisany obraz maszyny można uruchomić jak każdy inny dostępny obraz systemu operacyjnego.

Bezwzględne usuwanie instancji maszyny wirtualnej.

> **UWAGA (ryzyko utraty danych)**
>
> Opcje tą należy używać tylko jeśli jest to absolutnie konieczne, np. maszyna którą nie zawiera istotnych danych nie chce się prawidłowo wyłączyć powyżej opisaną metodą. Spowoduje ona natychmiastowe zatrzymanie maszyny wirtualnej i bezpowrotne usunięcie jej obrazu na wet w przypadku wcześniejszego oznaczenia go do zapisu poleceniem "onevm saveas" (w tym przypdku dodatkowo powtaje niekompletny obraz). Jeśli maszyna zawiera istotne dane - nigdy nie należy używać tej opcji. W tym przypadku jeśli maszyna nie chce się wyłączyć sposobem opisanym w poprzedniej sekcji należy pozostawić ją włączoną i zgłosić ticket do Helpdesku.

Należy pamiętać, że usunięcie maszyny wirtualnej tym sposobem spowoduje nieodwracalne skasowanie wszystkich danych z jej lokalnego dysku – należy więc upewnić się, że wszystkie wyniki prowadzonych obliczeń (oraz inne ważne dane) została skopiowane na inny serwer (np. przez SCP).

W celu usunięciu maszyny należy zastosować polecenie:

> *onevm delete <ID>*

… zastępując <ID> identyfikatorem maszyny do usunięcia. Po potwierdzeniu operacji za pomocą loginu i hasła maszyna zostanie usunięta. Fakt usunięcia maszyny można zweryfikować przeglądając listę maszyn wcześniej opisanym sposobem.