Răzvan Constantin GUȚULOV, Ștefan-Mihai MOGA, grupa 1100
Facultatea de Cibernetică, Statistică și Informatică Economică
Academia de Studii Economice din București

Cloud computing – arhitectură și exemple

Cuprins

Acest articol științific prezintă principalele concepte și oferă un exemplu concret de Cloud Computing. Sunt explicate atât tipurile de servicii cloud computing – Infrastructure as a service (IaaS), Platform as a service (PaaS) și Software as a service (SaaS) – cât și modelele de implementare cloud computing – private cloud, public cloud și hybrid cloud. În final, este arătat modul în care compania Oracle a introdus aplicația ***PeopleSoft*** *în norul Oracle.*

Cuvinte cheie*: cloud computing, IaaS, PaaS, SaaS, Internet, database, networking, PeopleSoft.*

Introducere

Conform cu Wikipedia, ***Cloud computing***, tradus prin „computerizare în nori” sau simplu „nor informatic”, este un concept modern în domeniul computerelor și informaticii, reprezentând un ansamblu distribuit de servicii de calcul, aplicații, acces la informații și stocare de date, fără ca utilizatorul să aibă nevoie să cunoască amplasarea și configurația fizică a sistemelor care furnizează aceste servicii[1].

Istoric

Originea termenului de ***Cloud Computing*** este neclară. Cuvântul "nor" este utilizat în mod obișnuit în știință pentru a descrie o aglomerare mare de obiecte, care apar vizibil de la distanță ca un nor și care descriu orice set de lucruri ale căror detalii nu sunt inspectate în continuare într-un anumit context. O altă explicație este că programele vechi, care au atras schemele de rețea, au înconjurat pictogramele pentru servere cu un cerc, iar un grup de servere într-o diagramă de rețea avea mai multe cercuri suprapuse, care seamănă cu un nor. În mod analog cu utilizarea de mai sus, cuvântul *cloud* a fost folosit ca o metaforă pentru Internet și o formă standardizată de tip cloud a fost folosită pentru a desemna o rețea pe scheme de telefonie. Mai târziu a fost folosit pentru a descrie Internetul în diagramele rețelelor de calculatoare. Cu această simplificare, putem trage concluzia că specificul modului în care sunt conectate punctele de capăt ale unei rețele nu este relevant pentru înțelegerea diagramei. Simbolul nor a fost utilizat pentru a reprezenta rețelele de echipamente de calcul în originalul ARPANET încă din 1977 și CSNET din 1981, predecesorii Internet-ului[3]. Referințele la ***Cloud Computing***, în sensul său modern, au apărut încă din 1996 când este menționat prima dată într-un document intern Compaq[4]; însă acest termen a devenit popular abia în 2006 când Amazon.com și-a prezentat *Cloud Computing Elastic*.

Concepte similare

Cloud computing este rezultatul evoluției și adoptării tehnologiilor și paradigmelor existente. Scopul cloud computing este de a permite utilizatorilor să beneficieze de toate aceste tehnologii, fără a avea nevoie de cunoștințe profunde sau expertiză. Norul informatic își propune să reducă costurile și să-i ajute pe utilizatori să se concentreze asupra dezvoltării produselor informatice, în loc să fie împiedicați de obstacolele IT[5].

Principala tehnologie de activare pentru cloud computing este virtualizarea. Software-ul de virtualizare separă un dispozitiv de calcul fizic într-unul sau mai multe dispozitive "virtuale", fiecare dintre acestea putând fi ușor utilizate și gestionate pentru a efectua activități de calcul. Cu ajutorul virtualizării la nivel de sistem de operare, care creează în esență un sistem scalabil de dispozitive computerizate independente, resursele inutile de calcul pot fi alocate și utilizate mai eficient. Virtualizarea oferă agilitatea necesară pentru a accelera operațiunile IT și reduce costurile prin creșterea utilizării infrastructurii. Acesta autonomizează procesul prin care utilizatorul poate furniza resurse la cerere. Prin minimizarea implicării utilizatorilor, automatizarea accelerează procesul, reduce costurile forței de muncă și reduce posibilitatea unor erori umane. Utilizatorii se confruntă în mod obișnuit cu probleme de afaceri dificile. Cloud computing adoptă concepte din arhitectura orientată spre servicii (*Service-Oriented Architecture*), care ajută utilizatorul să spargă aceste probleme în servicii ce pot fi integrate pentru a oferi o soluție. Cloud computing oferă toate resursele sale ca servicii și utilizează standarde bine definite cât și cele mai bune practici dobândite în domeniul SOA, pentru a permite accesul global și ușor la serviciile cloud într-un mod standardizat.

Cloud computing are în comun caracteristici cu:

- *Modelul client-server* – se referă la orice aplicație distribuită care distinge între furnizorii de servicii (servere) și solicitanții de servicii (clienți);
- *Computer bureau* – un birou de servicii care oferă servicii informatice, în special din anii 1960 până în anii 1980;
- *Grid computing* - o formă de calcul distribuită și paralelă, prin care un calculator superrapid și virtual este compus dintr-un grup de computere conectate în rețea, care acționează concertat pentru a îndeplini sarcini foarte mari;
- *Fog computing* - paradigma de calcul distribuită care oferă servicii de date, calcul, stocare și aplicații mai aproape de dispozitivele de vârf ale clienților sau utilizatorilor apropiați, cum ar fi routerele de rețea; *fog computing* se ocupă de datele de la nivelul rețelei, de dispozitivele inteligente și de partea clientului final (de exemplu, dispozitivele mobile), în loc să trimită date către o locație la distanță pentru procesare;
- *Dew computing* – este baza paradigmelor *cloud computing* și *fog computing*; în comparație cu *fog computing*, care necesită latență în timp real și reconfigurabilitatea dinamică a rețelei, *dew computing* se folosește de utilizatorii finali pentru a gestiona aplicațiile de calcul, datele și servicii oferite;
- *Mainframe computer* – computer puternic, utilizat în principal de organizații mari pentru aplicații critice, cum ar fi: recensământul; statisticile de consum; serviciile de informații secrete; planificarea resurselor intreprinderii și prelucrarea tranzacțiilor financiare;
- *Utility computing* – oferirea unor resurse de calcul precum calculul și stocarea, ca un serviciu măsurat, similar cu un serviciu tradițional de utilitate publică, cum ar fi electricitatea;
- *Peer-to-peer* – o arhitectură distribuită, fără o coordonare centrală, astfel încât participanții sunt și furnizori și consumatori de resurse, spre deosebire de modelul client-server tradițional;
- *Green computing*;
- *Cloud sandbox* – un mediu de lucru izolat, în care un program poate funcționa fără a afecta aplicația în care rulează.

Caracteristici

Conexiunea permanentă a utilizatorului la Internet a devenit foarte răspândită, astfel încât acum aproape toate resursele disponibile se pot plasa în Internet și partaja, uneori chiar între utilizatori complet independenți unii de alții: software (programele) și datele/informațiile sunt aduse din Internet pe calculatorul utilizatorului la cerere (*on demand*), ca și cum ar fi vorba de servicii publice banale precum apa sau energia electrică.

Executarea aplicațiilor de computer online în Internet, și nu pe stația de lucru (*workstation*) proprie, reprezintă o nouă schimbare de paradigmă, urmașă a celei din anii 1980, când s-a trecut de la mainframes la conceptul client-server. Dacă interfața pusă la dispoziție de furnizorul (*provider*) de cloud computing este de bună calitate, atunci utilizatorul e eliberat de sarcina de a fi un expert în tehnologia și infrastructura folosite. De exemplu, el nu mai trebuie să-și actualizeze software-ul, deoarece aceasta se face central, la furnizor.

Cloud computing folosește noi metode de oferire și consumare a serviciilor IT în Internet, servicii care de obicei pot fi dimensionate dinamic și care includ resurse virtualizate. Este de fapt doar o posibilitate secundară, urmare a ușurinței cu care se pot acum accesa toate serverele și centrele de calcul interconectate prin intermediul Internetului.

Furnizorii tipici de cloud computing pun la dispoziție, de exemplu, aplicații comerciale standard; utilizatorul are acces la acestea doar prin intermediul unui browser local, deoarece atât aplicația cât și datele proprii ale utilizatorului sunt găzduite în cloud, pe serverul furnizorului de servicii. În aceste condiții asigurarea confidențialității și drepturilor de acces la date în contextul Internetului atotprezent joacă un rol primordial.

Deseori furnizorii de clouds prevăd și servicii suplimentare, consolidând toate ofertele lor, pentru toți clienții lor, într-o singur loc (pagină sau sit web). Ofertele comerciale trebuie în general să îndeplinească standardele de calitate cerute de clienți, ca de ex. așa numitele Service Level Agreements (SLA) și altele. Cei mai mari furnizori din acest domeniu sunt companiile Microsoft, Salesforce, Skytap, HP, IBM, Amazon, ***Oracle*** și Google.

Avantaje și dezavantaje

Avantaje:

- Sincronizarea datelor utilizatorului care folosește mai multe dispozitive legate la cloud (de ex. un smartphone, o tabletă, un notebook, dar și un PC) este simplificată;
- Documentele online din cloud se pot prelucra cu ajutorul unor aplicații web;
- Viteză de calcul și capacitate de stocare sporite, dar fără investiții în propria configurație;
- Datele nu pot fi furate, purtătorul de date nu se poate defecta etc.

Dezavantaje:

- E necesară o legătură la Internet rapidă și stabilă;
- Securitatea necesară a datelor din cloud poate prezenta probleme și poate produce neîncrederea utilizatorilor;
- Situația legală este de obicei complexă, deoarece utilizatorul nu află nici măcar în ce țară se află serverele care îi găzduiesc datele sale.

Modele de servicii

Deși arhitectura orientată spre servicii (SOA) pledează pentru "totul ca serviciu" (cu acronimele EaaS sau XaaS sau pur și simplu *aas*), furnizorii de cloud computing oferă serviciile lor în funcție de diferite modele, dintre care cele 3 modele standard pe NIST sunt: Infrastructura ca Serviciu (IaaS), Platforma ca Serviciu (PaaS) și Software-ul ca Serviciu (SaaS). Aceste modele oferă o abstractizare tot mai mare și sunt adesea reprezentate ca straturi independente într-o stivă: infrastructură, platformă și software-ca-serviciu. De exemplu, se poate furniza SaaS implementat pe mașini fizice, fără a utiliza straturi subadiacente PaaS sau IaaS, iar invers se poate rula un program pe IaaS și accesa direct, fără a folosi SaaS.

NIST definește modelele de servicii de ***cloud computing***, după cum urmează[6]:

Software-ul ca serviciu (SaaS) – capacitatea furnizată consumatorului este de a utiliza aplicațiile furnizorului care rulează pe o infrastructură cloud. Aplicațiile sunt accesibile de la diverse dispozitive client, fie printr-o interfață de client prietenoasă, cum ar fi un browser web (de ex., un e-mail bazat pe interfață web), fie o interfață de program. Consumatorul nu administrează sau nu controlează infrastructura cloud, inclusiv rețeaua, serverele, sistemele de operare, capacitățile de stocare sau chiar aplicațiile individuale, cu excepția posibilelor setări de configurație a aplicațiilor specifice.

Platforma ca serviciu (PaaS) – capacitatea oferită consumatorului de a implementa pe infrastructura cloud aplicațiile create sau achiziționate de către consumatori, folosind limbaje de programare, biblioteci, servicii și instrumente suportate de furnizor. Consumatorul nu administrează sau nu controlează infrastructura cloud, inclusiv rețeaua, serverele, sistemele de operare sau spațiul de stocare, dar are control asupra aplicațiilor implementate și chiar asupra setărilor de configurare pentru mediul de găzduire a aplicațiilor.

Infrastructura ca serviciu (IaaS) – capacitatea furnizată consumatorului de a furniza servicii de procesare, stocare, rețele și alte resurse de calcul fundamentale, în care consumatorul poate implementa și executa software arbitrar, care poate include sisteme de operare și aplicații. Consumatorul nu gestionează sau nu controlează infrastructura cloud, dar are control asupra sistemelor de operare, a aplicațiilor de stocare și a aplicațiilor desfășurate și, posibil, un control limitat al componentelor de rețea selectate (de exemplu, firewall-uri gazdă).

Modele de implementare

Cloud-ul privat este o infrastructură cloud care funcționează exclusiv pentru o singură organizație, fie administrată intern sau de către un terț și găzduită fie intern, fie extern. Efectuarea unui proiect cloud privat necesită un nivel semnificativ de implicare în virtualizarea mediului de afaceri și cere organizației să reevalueze deciziile cu privire la resursele existente. Când este implementat bine poate îmbunătăți afacerea, dar fiecare pas în proiect ridică probleme de securitate, care trebuie abordate pentru a preveni vulnerabilitățile serioase. Centrele de date de tip self-run sunt în general mari; ele au o amprentă fizică semnificativă, care necesită alocări imense de spațiu hardware și software. Însă aceste active trebuie să fie actualizate periodic, ducând la cheltuieli suplimentare. Acestea au atras critici, deoarece utilizatorii "trebuie să le cumpere, să le construiască și să le administreze" și, prin urmare, nu beneficiază de un cost redus de gestionare, contrar modelului economic care face conceptul de ***cloud computing*** atât de interesant.

Un cloud este public atunci când serviciile sunt redate prin intermediul unei rețele care este deschisă publicului; *serviciile de cloud publice* pot fi gratuite. Din punct de vedere tehnic, ar putea exista o mică diferență între arhitectura cloud-ului public și cel privat, totuși considerațiile privind securitatea pot diferi în mod substanțial pentru serviciile care sunt puse la dispoziție de un furnizor pentru publicul larg și când comunicarea este făcută printr-o rețea nesecurizată. În general, furnizorii de servicii publice de cloud, cum ar fi Amazon Web Services (AWS), Microsoft, Google și Oracle dețin și operează infrastructura la centrul de date și accesul este, în general, prin Internet. AWS și Microsoft oferă, de asemenea, servicii de conectare directă, numite "AWS Direct Connect" și "Azure ExpressRoute", astfel de conexiuni obligând clienții să cumpere sau să închirieze o conexiune privată pentru acces.

Norul hibrid este o compoziție a două sau mai multor nori (privat, comunitar sau public), care rămân entități distincte, dar sunt legate între ele, oferind avantajele mai multor modele de implementare. Norul hibrid poate însemna și abilitatea de a conecta serviciile de colocare, gestionate și/sau dedicate cu resursele cloud. Gartner, Inc. definește un serviciu de cloud hibrid ca un serviciu de cloud computing care este compus dintr-o combinație de servicii cloud private, publice și comunitare, de la diferiți furnizori de servicii.[7] Un serviciu cloud hibrid traversează limitele de izolare și de furnizor, astfel încât să nu poată fi pur și simplu introdus într-o singură categorie de servicii cloud private, publice sau comunitare. Aceasta permite extinderea capacității unui serviciu cloud prin agregare, integrare sau personalizare cu un alt serviciu cloud.

Există cazuri de utilizare variată pentru compoziția norului hibrid. De exemplu, o organizație poate să stocheze date despre clienți sensibili într-o aplicație cloud privată, dar să interconecteze aplicația respectivă cu o aplicație de business intelligence furnizată într-un cloud public ca serviciu software.[8] Acest exemplu de cloud hibrid extinde capacitățile întreprinderii de a furniza un anumit serviciu de afaceri prin adăugarea de servicii public cloud disponibile extern. Adoptarea norilor hibrizi depinde de o serie de factori, cum ar fi cerințele de securitate a datelor și de conformitate, nivelul de control necesar datelor și aplicațiile pe care le utilizează o organizație.

Un alt exemplu de cloud hibrid este unul în care organizațiile IT folosesc resurse publice de cloud computing pentru a satisface nevoile temporare de capacitate care nu pot fi îndeplinite de cloud-ul privat. Această capacitate permite norilor hibrizi să utilizeze spargerea norului pentru scalarea pe nori. *Cloud bursting* este un model de implementare a aplicațiilor în care o aplicație rulează într-un cloud privat sau centru de date și "explodează" într-un nor public atunci când crește cererea de calcul. Un avantaj primar al exploziei de nori și al unui model de cloud hibrid este că o organizație plătește resurse suplimentare de calcul numai atunci când este necesar. Spargerea norului permite centrelor de date să creeze o infrastructură IT internă care să suporte încărcări medii și să utilizeze resursele norilor de la nori publici sau privați, pentru cereri diferite de procesare.

Modelul specializat de cloud hibrid, care este construit pe un hardware heterogen, se numește "*Cloud Hybrid Cross-platform*". Un nor hibrid cross-platform este de obicei alimentat de arhitecturi diferite ale procesorului, de exemplu, x86-64 și ARM. Utilizatorii pot implementa și scinda în mod transparent aplicațiile fără a cunoaște diversitatea hardware a cloud-ului. Acest tip de nor iese din creșterea sistemelor bazate pe ARM pe computer pentru clasa de server.

Studiu de caz: **PeopleSoft**

Norul Oracle: nor public de generație următoare care se adaptează la organizația clientului.

Cu 88% dintre întreprinderi care folosesc acum nori publici, nu este de mirare că norul public a intrat în ceea ce numeroși analiști numesc o fază de hiperinovare.

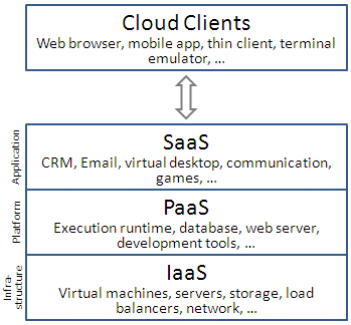
Oferind deja beneficii enorme în jurul costului, agilității și experienței clienților, norii publici transformă practicile de afaceri și remodelează IT-ul.

Dincolo de aceasta, schimbă și modul în care organizațiile concurează, numărul soluțiilor și al cazurilor de utilizare crescând.

Dar, în timp ce norul reprezintă în mod clar viitorul, multe organizații rămân împovărate în trecut - nu pentru că nu au reușit să îmbrățișeze norul, ci pentru că sunt îngrădite de soluțiile de primă generație care abia zgârie suprafața potențialului norului modern. Astfel de soluții sunt deseori înguste (împiedică împărtășirea informațiilor la nivel de întreprindere) și nu reușesc să recunoască realitatea unui univers cu multi-nor în care datele și aplicațiile trebuie transferate cu viteză și ușurință între norii publici, privați și hibrizi și accesați de mii de dispozitive pe care le utilizează clienții și angajații.

În timp ce norul a evoluat, Oracle a investit miliarde de dolari dezvoltând un nor de întreprindere, care reprezintă primul nor real de generație următoare. Când se investește în norul Oracle, se beneficiază de un mediu unificat, care oferă infrastructura cloud flexibilă, o platformă puternică bazată pe standarde și un portofoliu cuprinzător de aplicații pentru afaceri – toate pe bază de abonament.

În timp ce alți furnizori se pot lăuda cu soluții complete de nor, nimeni nu poate oferi ceea ce face norul Oracle: cea mai largă colecție de servicii cloud de pe piață, soluții la fiecare strat al stivei de tehnologie nor, precum și posibilitatea de a muta aplicații și volumul de lucru între nor și mediul local, rapid și ușor.



Oferind avantaje în ceea ce privește costurile, securitatea, managementul, fluxul de lucru și integrarea afacerilor, această abordare multiplă a norului este inclusă în fiecare categorie de servicii a norului Oracle:

- **Software ca serviciu (SaaS)**. Oferă cel mai complet portofoliu din orice nor public, SaaS de la norul Oracle oferă aplicații nor moderne care conectează procesele de business din întreaga companie. Acoperă totul, de la experiența clienților până la planificarea resurselor întreprinderii, managementul capitalului uman și multe altele.
- **Platforma ca serviciu (PaaS)**. Furnizează baza de date # 1 din industrie (Oracle Database) și serverul de aplicații # 1 (Oracle WebLogic Server), platforma Oracle Cloud's PaaS este cea mai importantă platformă de cloud enterprise din industrie. Construit pe o tehnologie Oracle dovedită, care rulează peste tot, norul Oracle PaaS ajută organizațiile să conducă inovația și transformarea afacerii.
- **Infrastructura ca serviciu (IaaS)**. Oferă un set complet de servicii, inclusiv infrastructura de calcul elastică și IaaS de stocare. Norul Oracle permite companiilor de a executa orice volum de lucru în nor. Cel mai bun lucru este ca acesta se face într-un mediu complet integrat care a fost optimizat pentru nor și oferă un model de securitate unificat.

Prima generație de nori părea să se concentreze mai mult asupra furnizorului de nor decât asupra clientului de nor - forțând organizațiile să adapteze totul, de la fluxurile de lucru la aspectul și simțul aplicației și la upgrade-urile programate de către furnizorii de nor.

De la infrastructura de bază la platforma de dezvoltare, norul Oracle le permite dezvoltatorilor să-și modifice rapid aplicațiile pentru a satisface nevoile organizației. Specialiștii IT ajung să-și adapteze mediile pentru a implementa și actualiza software-ul pe propriile condiții. Și utilizatorii de afaceri ajung să-și definească experiența prin tablouri de bord configurabile, rapoarte, fluxuri de lucru și date.

Datele deconectate, procesele disparate și informațiile incomplete devin lucruri din trecut, când integrarea este furnizată în fiecare strat al norului. Conectând oameni, procese, informații și analize printr-o suită integrată de servicii de aplicații, platforme și infrastructură, norul Oracle este impregnat cu un model de securitate unificat și cu analize integrate care vor permite întreprinderilor să înregistreze un curs constant în viitor. Cu norul Oracle, angajații beneficiază de o experiență consistentă, iar dezvoltatorii și personalul IT văd productivitatea în creștere, deoarece procesele, datele și volumul de lucru sunt mutate între nor și local, cu ușurință prin buton.

Sprijinită de 19 centre de date la nivel mondial, de o armată de experți în securitatea cloud-ului Oracle precum și monitorizarea și suportul în permanență, norul Oracle oferă asigurarea necesară pantru ca datele clientului să fie în siguranță.

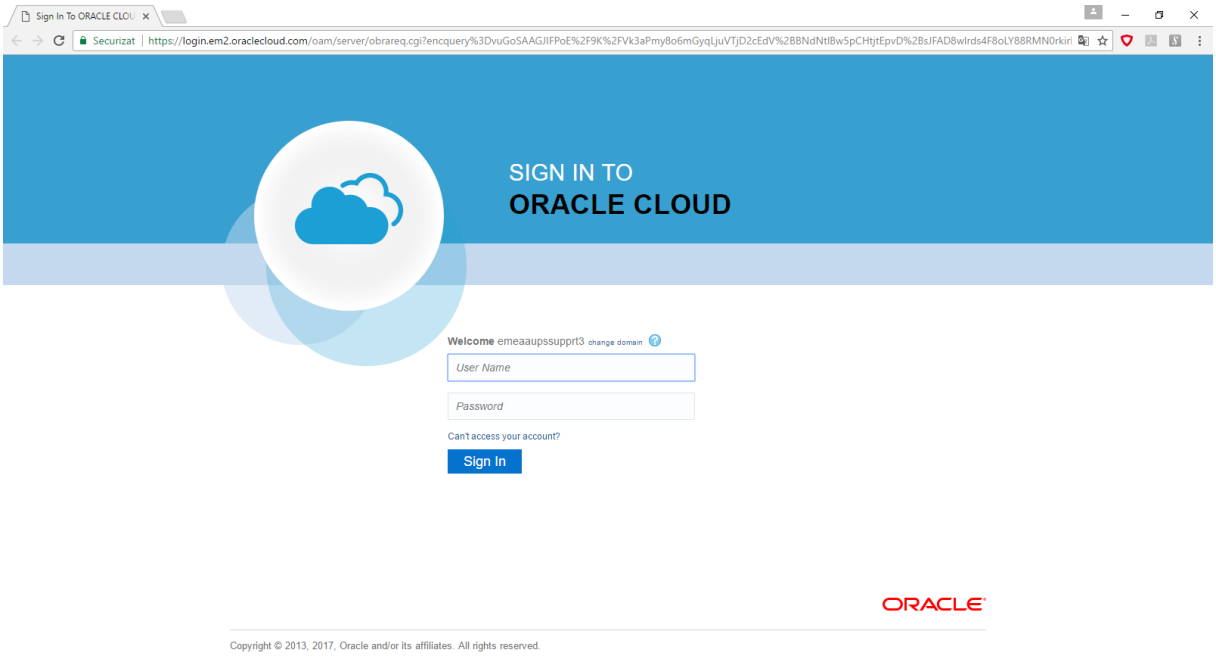
Implementarea PeopleSoft în norul public Oracle

În următoarele vom demonstra pașii de implementare a unei instanțe PeopleSoft HCM în norul public Oracle (IaaS).

Aceștia sunt pașii care vor fi acoperiți:

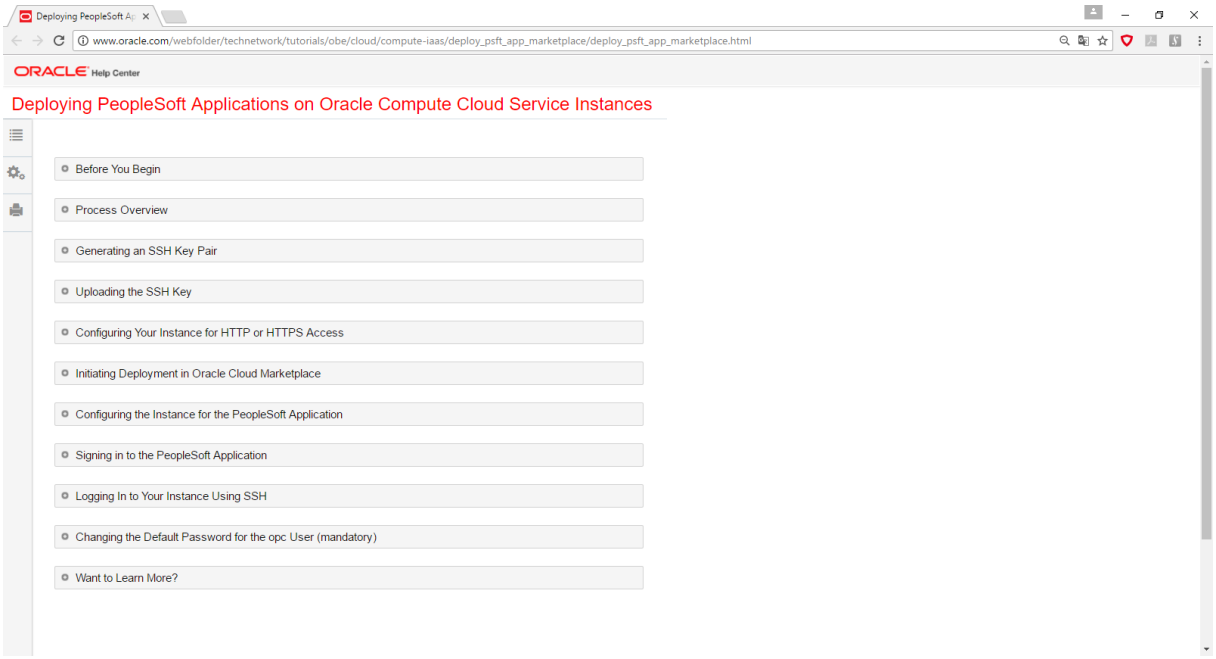
- Generarea unei perechi de chei SSH;
- Încărcarea perechii de chei;
- Configurarea instanței pentru accesul HTTP;
- Inițierea implementării în Magazin Nor Oracle;
- Configurarea și crearea instanței;
- Conectarea la PeopleSoft după crearea instanței;
- Conectarea utilizând SSH;
- Schimbarea parolei implicite la nivelul sistemului de operare.

Conectarea la norul public Oracle:
https://myservices.em2.oraclecloud.com/mycloud/emeaaupssupprt3/faces/dashboard.jspx



Se deschide tutorialul OBE pentru a se urmări pașii întocmai cum sunt prezentați

http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/deploy_psft_app_marketplace/deploy_psft_app_marketplace.html



Expandăm: Prezentare generală a proceselor

Pentru a implementa o aplicație PeopleSoft de pe Magazin Nor Oracle, se urmează pașii următori:

1. Se generează o pereche de chei SSH folosind un sistem Linux sau Microsoft Windows local;
2. Se încarcă cheia publică SSH în Serviciul Evaluare Nor Oracle;
3. Se configurează instanța Serviciului Evaluare Nor Oracle pentru accesul HTTP;
4. Se determină aplicația PeopleSoft care urmează să fie implementată și se inițiază implementarea în Magazin Nor Oracle;
5. Se utilizează consola Web a Serviciului Evaluare Nor Oracle pentru a configura instanța care va fi utilizată pentru găzduirea aplicației PeopleSoft;
6. Conectarea la aplicația PeopleSoft;
7. Conectarea la instanță folosind SSH;
8. Schimbarea parolei implicită pentru utilizatorul opc (obligatoriu).

Urmăm pașii detaliați pentru a implementa PeopleSoft în norul public.

Se începe cu: Generarea unei perechi de chei SSH

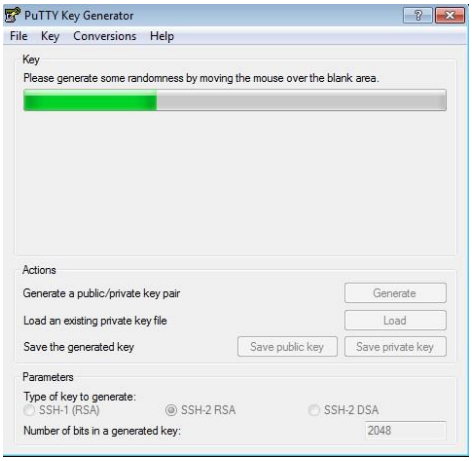
Când se crează instanța Serviciului Evaluare Nor Oracle, trebuie furnizată o cheie publică sigură a shell-ului (SSH) care va fi utilizată pentru autentificare atunci când ne conectăm la instanță. Se generează perechea de chei SSH și se încărcă cheia publică SSH în Serviciul Evaluare Nor Oracle înainte de a se începe să se creeze instanța.

- Generarea unei perechi de chei SSH pe sisteme UNIX sau UNIX Utilizând ssh-keygen
- Generarea unei perechi de chei SSH pe Windows utilizând generatorul de chei PuTTY

1. Se găsește puttygen.exe în dosarul PuTTY de pe computer și se face dublu clic pe el.

2. Se acceptă tipul de cheie implicit, SSH-2 RSA și se setează numărul de biți dintr-o cheie generată la 2048, dacă nu este deja setată. Apoi se face clic pe Generați.

3. Se mută mouse-ul în jurul zonei goale pentru a genera valori întâmplătoare. Se generează perechea de chei SSH.



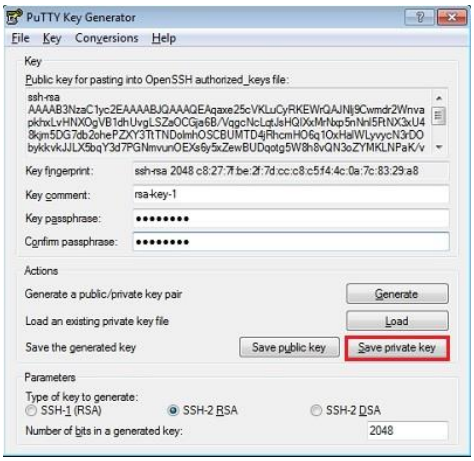
4. Se salvează cheia privată.

a. Comentariul cheie este numele cheii. Se poate păstra comentariul cheie generat sau se creează propriul comentariu.

b. Se introduce o expresie de acces în fraza de acces cheie și câmpurile. Se confirmă expresia de acces.

Notă: Se reține fraza de acces. Nu se poate recupera o expresie de acces dacă se uită.

c. Pentru a salva cheia privată în formatul PuTTY PPK, se face clic pe Salvați cheia privată.
Introducem același nume ca și cel folosit pentru comentariul cheie, astfel încât să știm ce cheie publică să utilizăm cu această cheie privată. Cheia privată este salvată în formatul PuTTY privat (PPK), care este un format proprietar care funcționează numai cu setul de instrumente PuTTY. Se poate utiliza această cheie ori de câte ori se utilizează PuTTY pentru SSH.

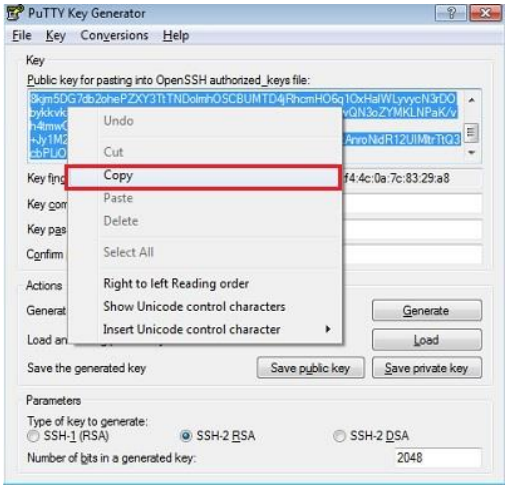


5. Apoi, se salvează cheia publică SSH.

a. Pentru a salva cheia publică, în Generatorul de chei PuTTY, se selectează toate caracterele din cheia publică pentru a le insera în câmpul OpenSSH authorized_keys file.

Notă: Ne asigurăm că selectăm toate caracterele, nu doar cele pe care le putem vedea în fereastra îngustă. Dacă în dreptul caracterelor există o bară de defilare, nu se văd toate caracterele.

b. Se face clic dreapta undeva în textul selectat și se selectează Copy din meniu.



c. Se deschide un editor de text și se lipesc caracterele. Ne asigurăm că inserăm textul la primul caracter din editorul de text și nu se introduce nici o pauză de linie.

d. Salvăm cheia utilizând același nume rădăcină pe care l-am utilizat pentru cheia privată. Se adăugă o extensie .pub. Se poate să i se dea orice extensie se dorește, dar .pub este o convenție utilă pentru a se indica faptul că aceasta este o cheie publică.

e. Ieșim din generatorul cheie PuTTY.

6. Notăm numele de chei publice și private și în cazul în care acestea sunt salvate.
Când se creează instanțe, trebuie să se specifice cheia publică SSH. Când ne conectăm la o instanță, trebuie să introducem calea către cheia privată SSH corespunzătoare și să introducem expresia de acces când se solicită.

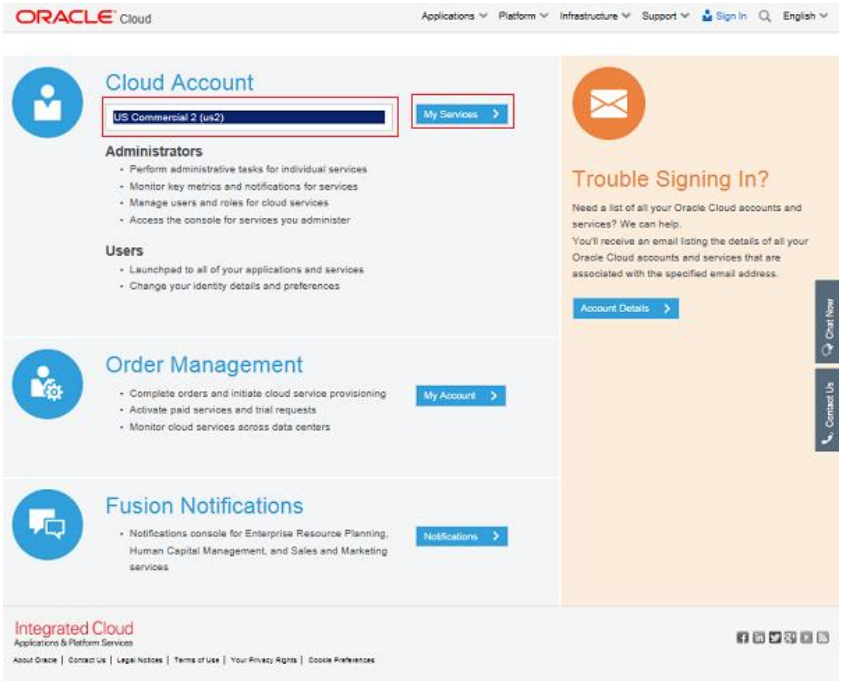
Continuând ...

Încărcarea cheii SSH

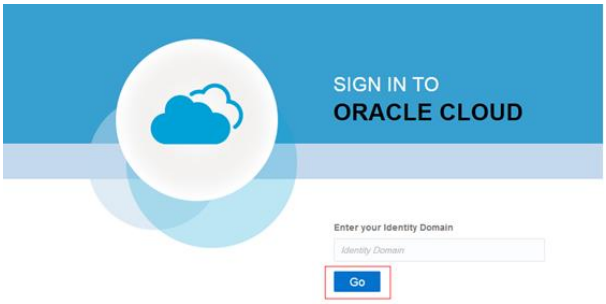
1. Ne conectăm la aplicația Serviciile Mele Nor Oracle la adresa https://cloud.oracle.com/sign_in.

2. Selectăm Centrul/regiunea de date care găzduiește domeniul de identitate Oracle Nor și se face clic pe butonul My Services.

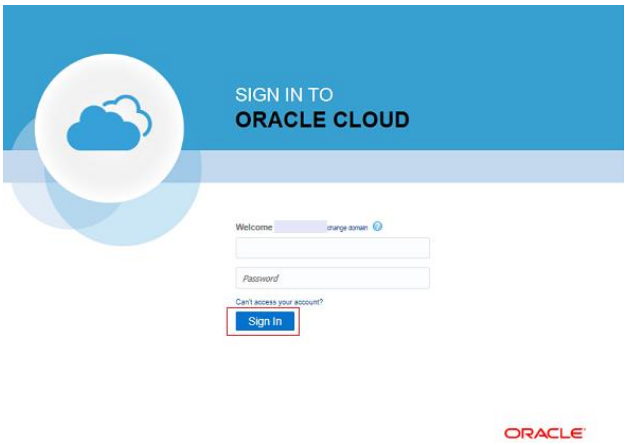
În acest exemplu, a fost selectat Centrul de date US Commercial 2 (us2):



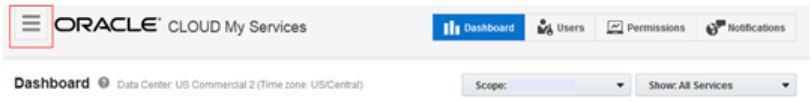
3. Introducem domeniul nostru de identitate în pagina de sign-in Oracle Nor și apoi facem clic pe butonul Go:



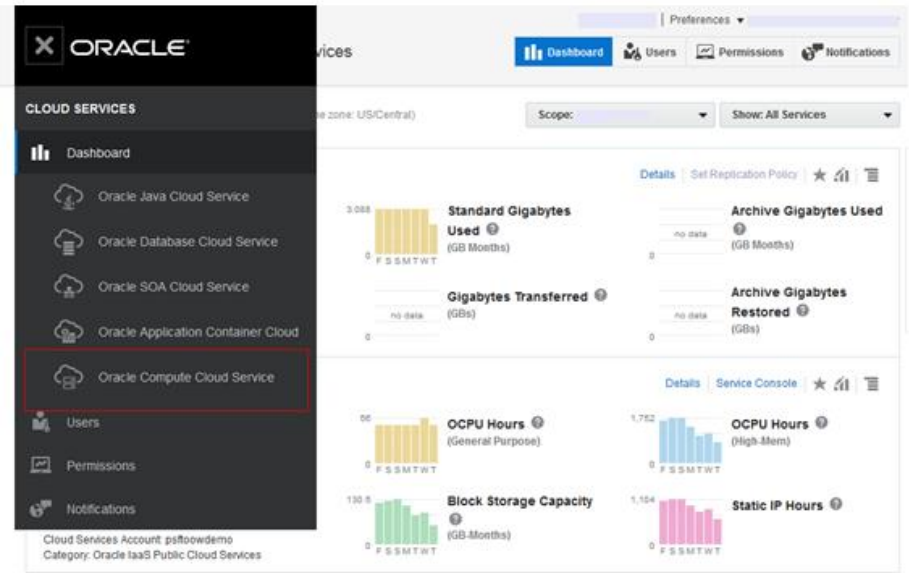
4. Introducem un nume de utilizator și o parolă validă pentru domeniul nostru de identitate, apoi facem clic pe „Sign In”:



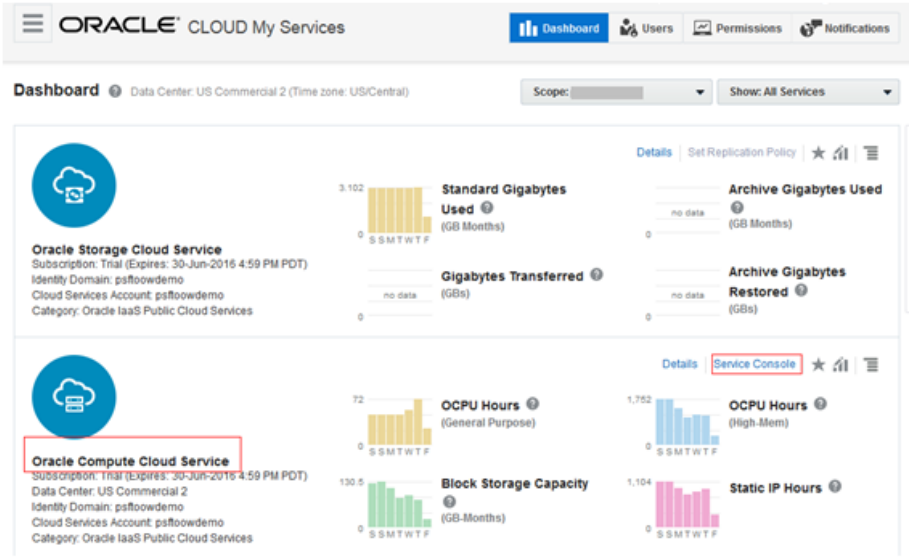
5. Selectăm serviciul Oracle Compute Cloud din meniul de navigare din colțul din stânga sus al paginii My Services.



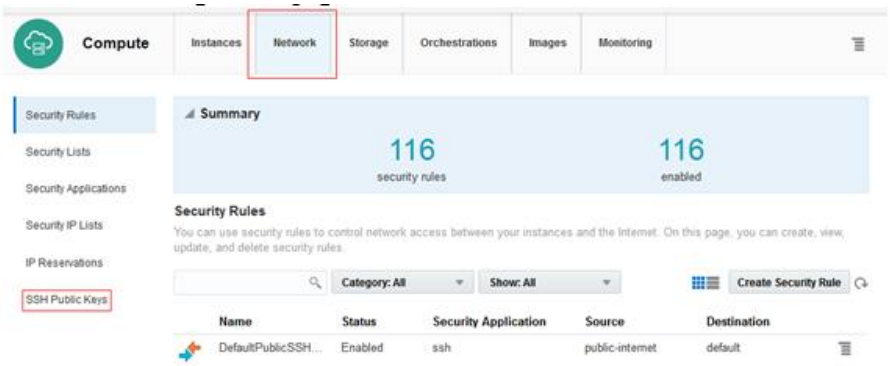
Apare tabloul de bord, așa cum se arată în acest exemplu:



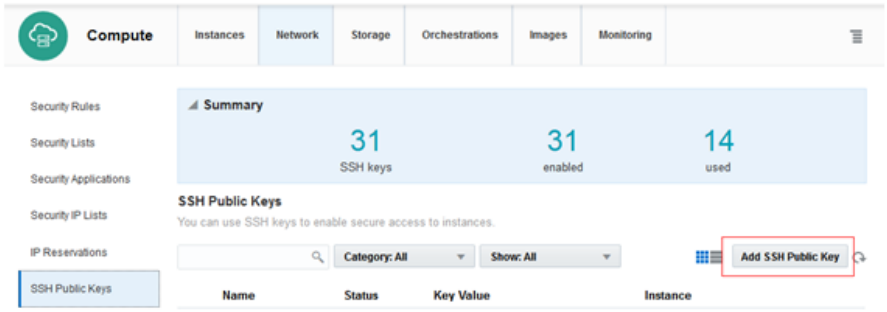
Alternativ, facem clic pe legătura Consola de Service pentru serviciul de calcul al norului Oracle, de asemenea de pe pagina My Services, după cum se arată în acest exemplu:



6. Selectăm fila Network și apoi selectăm link-ul SSH Public Keys din partea stângă a paginii de configurare a rețelei.



Se afișează pagina SSH Public Keys.

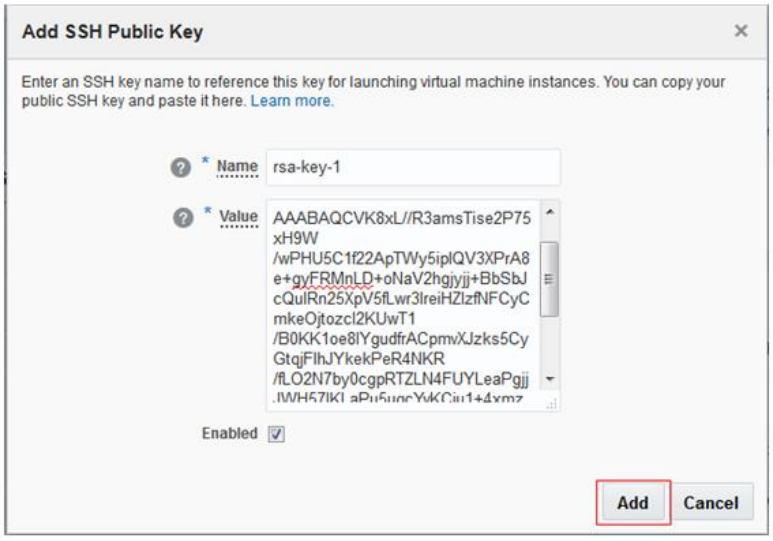


7. Facem clic pe Add SSH Public Key.

8. În caseta de dialog Add SSH Public Key, introducem un nume și valoarea cheii publice SSH generată anterior și apoi facem clic pe Adăugare.

Notă: Lipiți valoarea cheie exact așa cum a fost generată. Nu adăugați și nu inserați caractere suplimentare, pauze de linie sau spații.

Cheia publică SSH este adăugată serviciului de calcul al norului Oracle.



Configurarea instanței pentru accesul HTTP sau HTTPS

Imaginile de boot PeopleSoft găsite în Magazin Nor Oracle conțin o instalare a serverului web configurat pentru a asculta cereri pe porturile 8000 (HTTP) și 8443 (HTTPS).

Notă: Oracle recomandă foarte mult să se utilizeze protocolul HTTPS în toate implementările. Se urmează instrucțiunile din documentația de produs System and Server Administration pentru a se implementa cheile de criptare și certificatele necesare pentru criptarea Secure Sockets Layer (SSL).

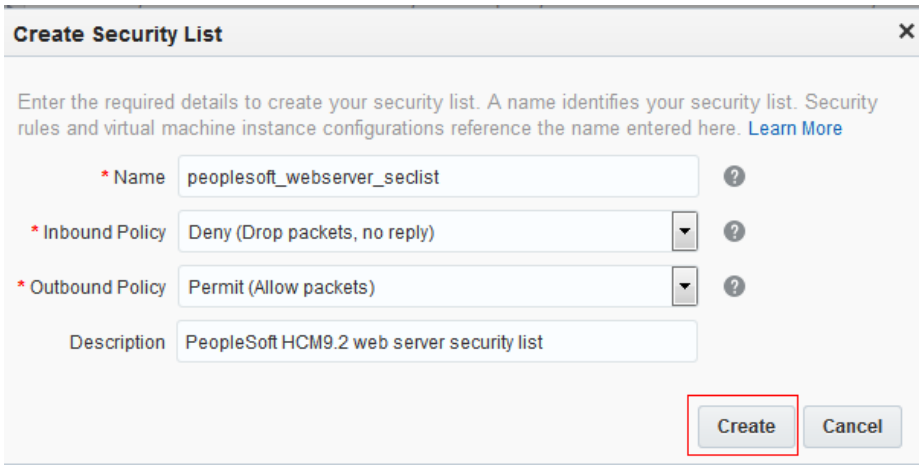
Crearea unei liste de securitate, crearea unei aplicații de securitate și crearea secțiunilor de reguli de securitate oferă un exemplu care demonstrează modul de definire a unei liste de securitate utilizând portul 8000 pentru http; cu toate acestea se recomandă utilizarea acestui lucru doar ca exemplu și apoi se activează portul 8443 numai pentru conexiuni sigure (https / SSL).

Crearea unei liste de securitate

O listă de securitate este un grup de instanțe Oracle Nor. Pentru a deschide portul 8000 pentru o anumită instanță, se creează o listă de securitate. Într-un pas ulterior, instanța serviciilor de calcul va fi adăugată la această listă de securitate.

Pentru a crea o listă de securitate:

1. În consola de Servicii de Calcul al Norului Oracle, facem clic pe fila Rețea;
2. Selectăm link-ul Liste de securitate, apoi facem clic pe Creare Listă de Securitate;
3. În caseta de dialog Creare Listă de Securitate, selectăm sau introducem următoarele informații:
   * Nume: Se introduce un nume pentru noua listă de securitate. În scopul acestui tutorial, se introduce peoplesoft_webserver_seclist. Se reține acest nume. Se va utiliza mai târziu în acest tutorial.
   * Politica Inbound: Acceptăm opțiunea implicită, Deny (Droppets, no reply);
   * Politica de ieșire: Selectăm Permite (Permiteți pachetele);
   * Descriere: Introducem o descriere pentru noua listă de securitate dacă se dorește, de exemplu, lista de securitate PeopleSoft HCM9.2 pentru serverul web.



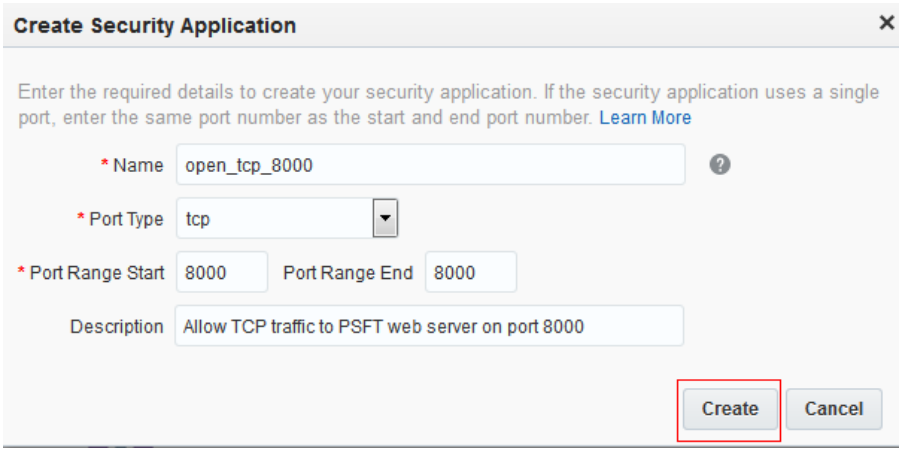
4. Facem clic pe Create.

Crearea unei aplicații de securitate

O aplicație de securitate este o mapare între un număr de port și un tip de port (TCP, UDP sau ICMP). Pentru a deschide portul 8000, trebuie să se creeze o aplicație de securitate pentru acel port.

1. Facem clic pe fila Rețea și apoi pe Securitatea aplicațiilor;
2. Facem clic pe Creați aplicația de securitate;
3. În caseta de dialog Creare securitate aplicație, se selectează sau se introduc următoarele informații:
   * Nume: Se introduce un nume pentru noua aplicație de securitate. În scopul acestui tutorial, se introduce open_tcp_8000. Se reține acest nume. Se va utiliza mai târziu în acest tutorial.
   * Tip port: Selectăm TCP.
   * Port Range Start și Port Range End: În ambele câmpuri, introducem portul pe care dorim să îl deschidem, portul 8000.
   * Descriere: Introducem o descriere pentru noua aplicație de securitate (de exemplu, Permitem traficul TCP pe serverul web PSFT pe portul 8000).

4. Facem clic pe Create.

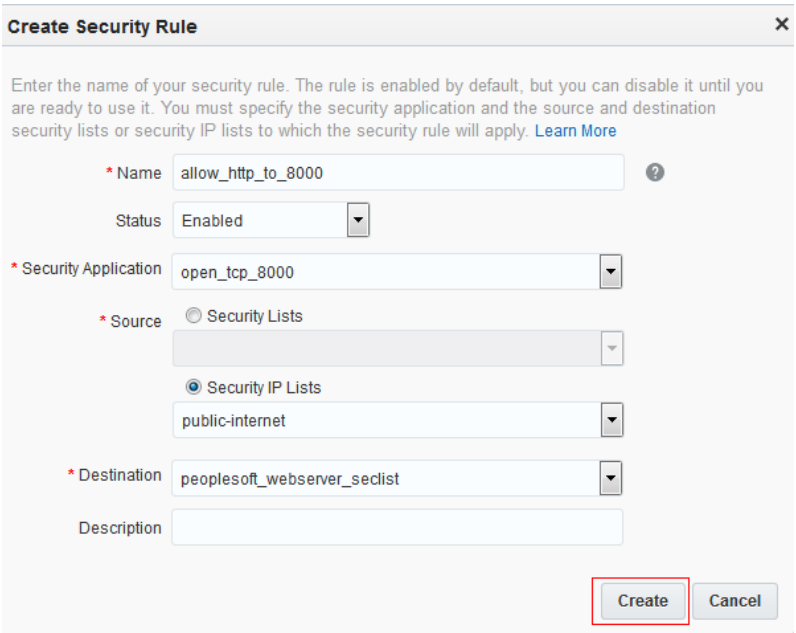


Crearea unei reguli de securitate

Se creează o regulă de securitate pentru a permite traficul TCP de pe Internet pe portul 8000.

1. Facem clic pe fila Rețea;
2. Selectăm legătura Reguli de securitate;
3. Facem clic pe Creare regulă de securitate;
4. În caseta de dialog Creare securitate, se selectează sau se introduc următoarele informații:
   * Nume: Se introduce un nume potrivit pentru această regulă. În scopul acestui tutorial, se introduce allow_http_to_8000.
   * Stare: Selectam Activat.
   * Aplicație de securitate: Selectăm open_tcp_8000, care este aplicația de securitate creată mai devreme.
   * Sursă: Selectăm butonul radio IP Listă de securitate și din lista derulantă Listă de securitate IP, selectăm public-internet.
   * Destinație: Selectăm lista de securitate peoplesoft_webserver_seclist creată mai devreme.

   * Descriere: Introducem o descriere a regulii (de exemplu, Permiteți traficul TCP pe serverele web pe portul 8000).

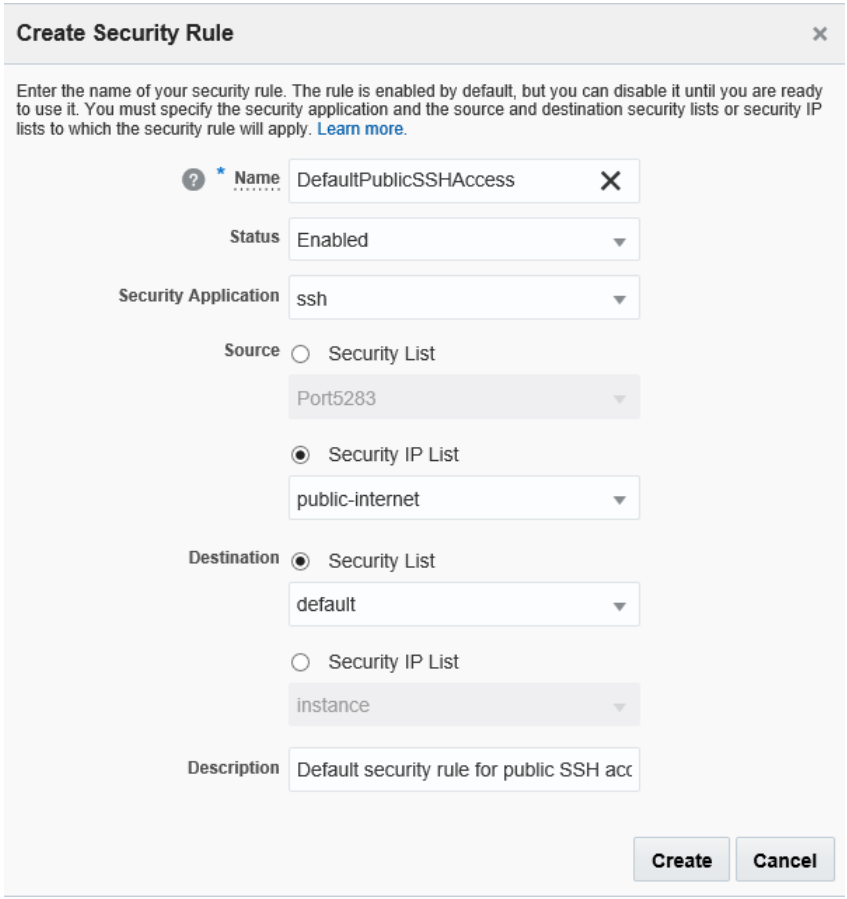


5. Facem clic pe Create.

Activarea accesului SSH cu lista de securitate implicită

Activăm accesul SSH în mod implicit pentru toate instanțele. Această procedură presupune prezența listei de securitate implicite. Lista de securitate implicită trebuie să fie prezentă în calea / Compute- <domain> / default / default.

1. În consola Serviciului de Calcul al Norului Oracle, facem clic pe fila Rețea;
2. Pe pagina Rețea, selectăm Reguli de securitate, apoi facem clic pe Creare regulă de securitate;
3. În caseta de dialog Creare securitate, se definește o regulă de securitate pentru a permite conexiunile SSH de la Internet public la lista de securitate implicită creată în pașii anteriori.
   Introducem sau selectăm următoarele informații:
   * Nume: Se introduce un nume descriptiv, de exemplu DefaultPublicSSHAccess.
   * Aplicație de securitate: Se selectează ssh din lista derulantă.
   * Sursă: Selectăm opțiunea Adresă de securitate IP și selectăm internet public din lista derulantă.
   * Destinație: Selectăm opțiunea Listă de securitate și selectăm lista de securitate implicită din lista derulantă.
   * Descriere: Introducem o descriere, cum ar fi regula de securitate implicită pentru accesul public SSH.

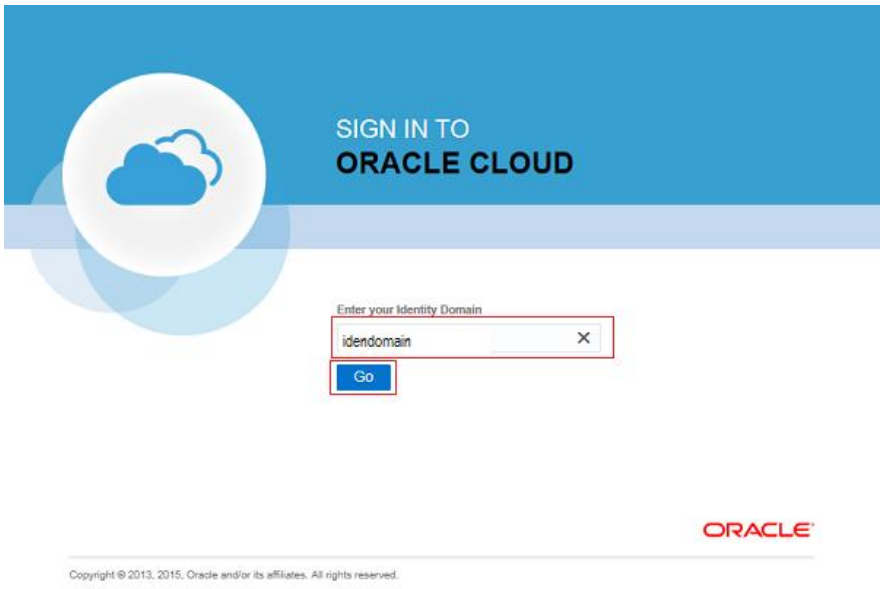


4. Facem clic pe Create.

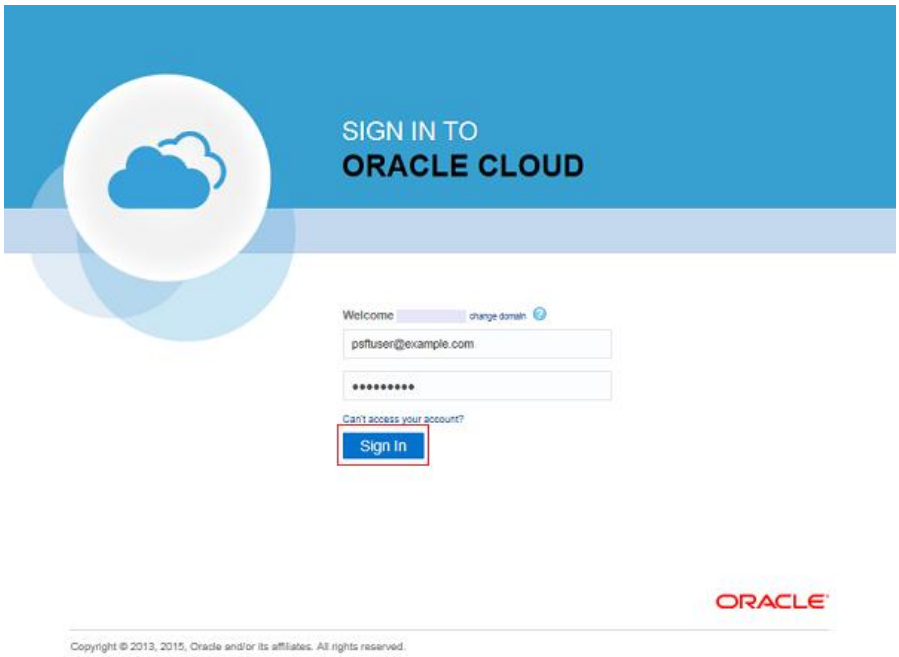
Inițierea implementării în Oracle Cloud Marketplace

Se utilizează consola Web a Serviciului Evaluare Nor Oracle pentru a configura instanța care va fi utilizată pentru găzduirea aplicației PeopleSoft.

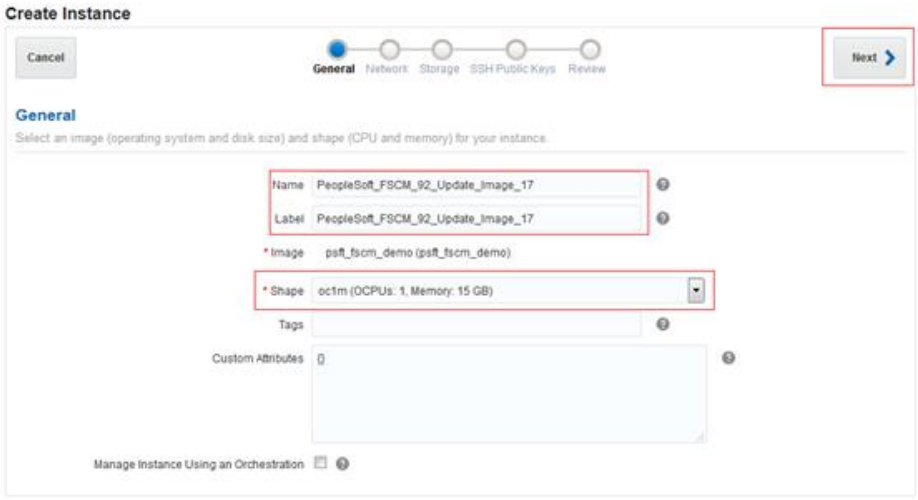
1. Introducem numele domeniului de identitate asociat abonamentului Oracle Compute Cloud Service, care este „idendomain” în acest exemplu, apoi facem clic pe Go.



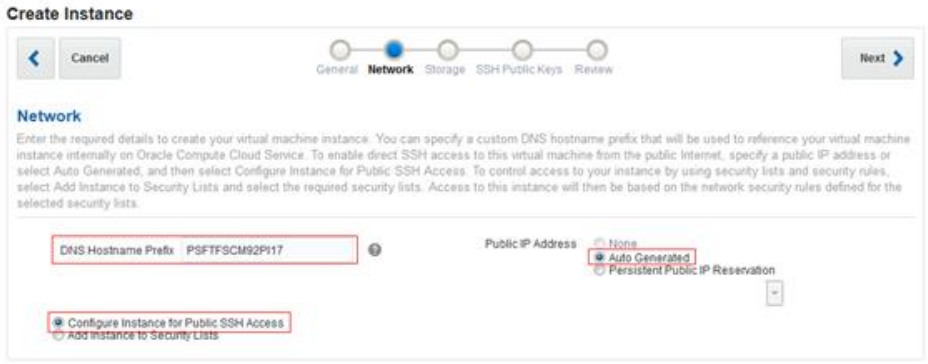
2. Ne conectăm la serviciul Oracle Compute Cloud. Aceasta inițiază expertul Creare instanță.



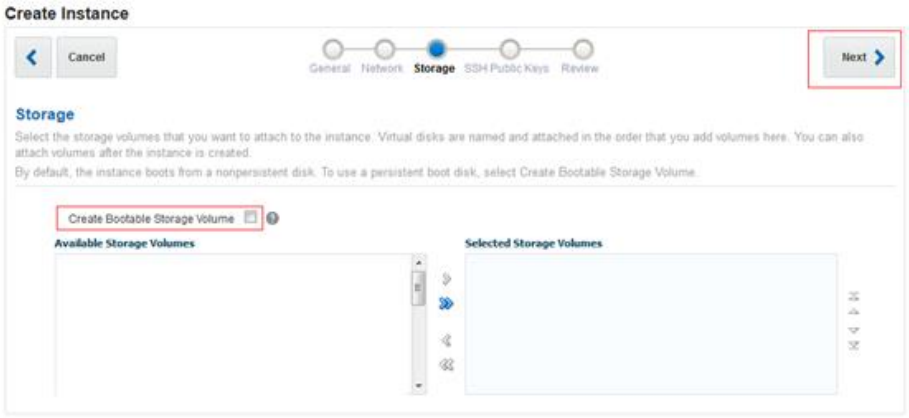
3. Pe pagina Generală a expertului Crează Instanță specificăm următoarele informații și apoi facem clic pe butonul Next:
   * Introducem un nume și o etichetă pentru instanța serviciului de calcul
   * Selectăm o formă (numărul de OCPU cu alocare de memorie) pentru instanța serviciului de calcul din lista derulantă. Forma din acest exemplu este oc1m (OCPUs: 1, Memory, 15 GB).



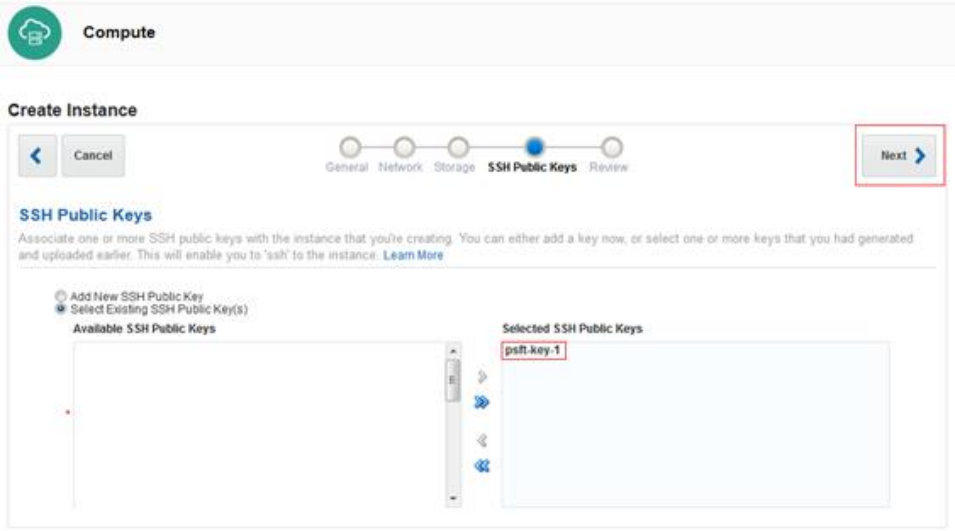
4. Pe pagina Rețea, configurăm după cum urmează, apoi facem clic pe butonul Next:
   * Adăugăm un nume de gazdă în câmpul Prefix nume DNS, care este PSFTFSCM92PI17 în acest exemplu.
   * Selectăm butonul radio Configurare instanță pentru acces public SSH.
   * Selectăm butonul radio Generat automat în zona Adresa IP publică.



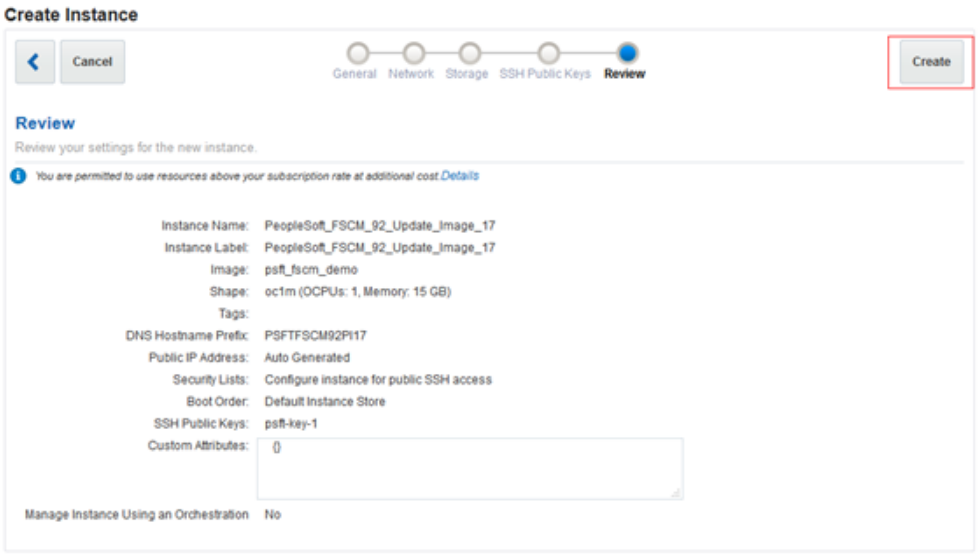
5. În pagina Stocare, debifăm caseta Creare Volum de Stocare Bootabilă și apoi facem clic pe butonul Next.



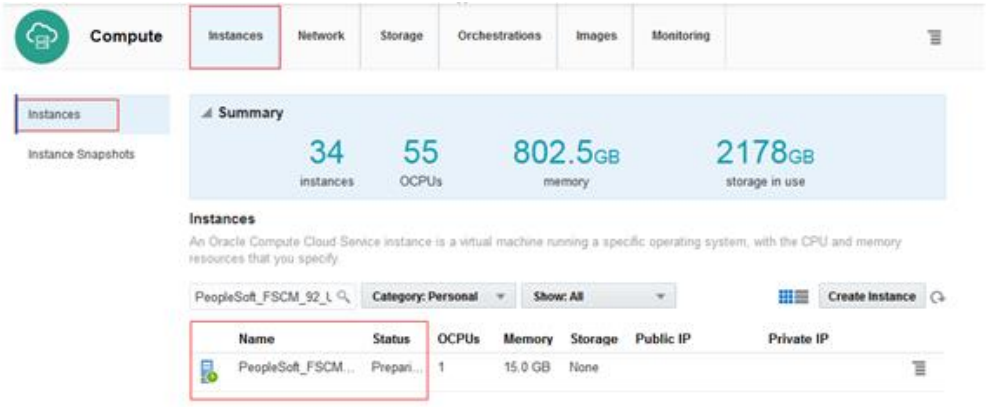
6. În pagina Chei Publice SSH, selectăm cheia SSH încărcată în secțiunea Încărcarea Cheii SSH, care este psft-key-1 în acest exemplu, apoi facem clic pe butonul Next.



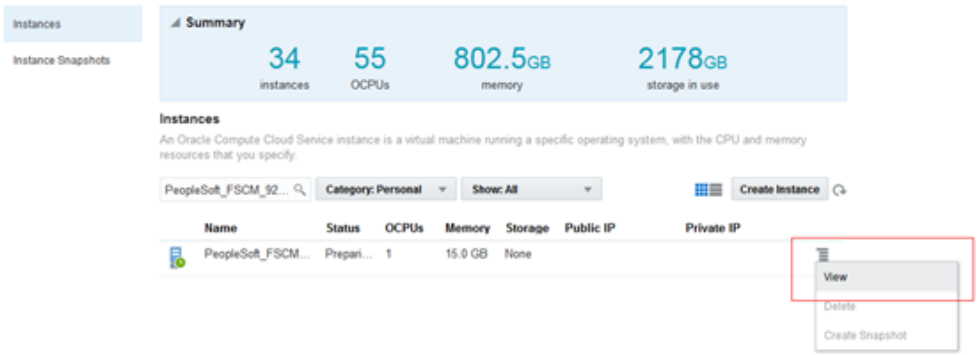
7. Examinăm configurația instanței și facem clic pe butonul Creare pentru a crea instanța Serviciului de Calcul al Norului Oracle.



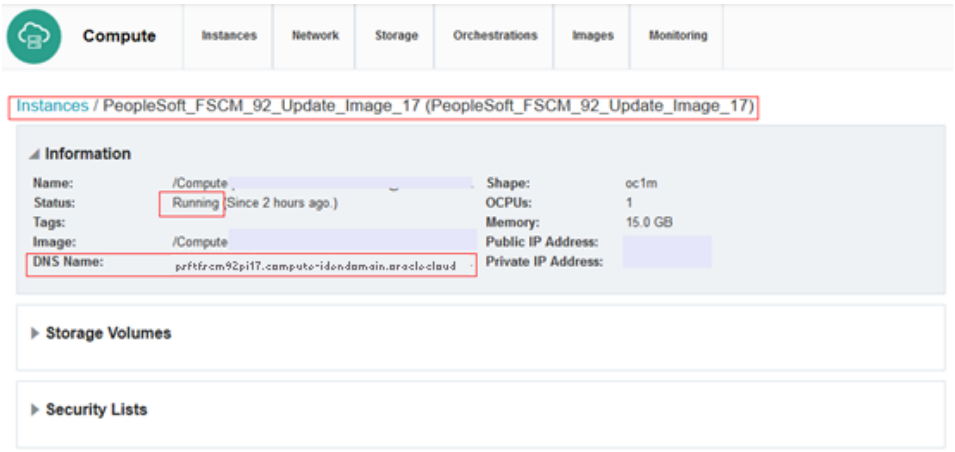
8. Verificăm starea Serviciului de Calcul al Norului Oracle utilizând fila Instante. În acest exemplu, starea este Pregătire.



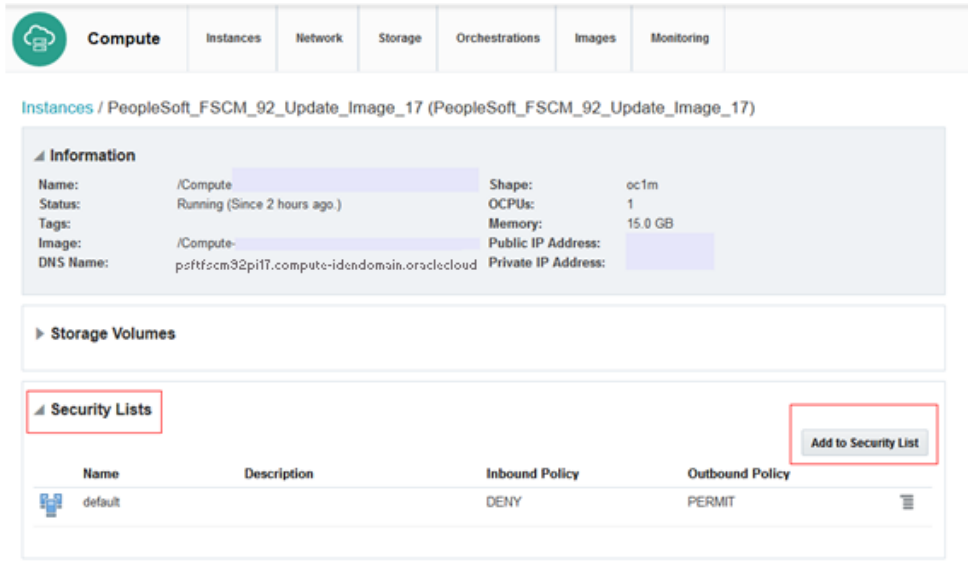
9. Facem clic pe meniul din partea dreaptă și selectăm Vizualizare.



10. Când Statutul sa schimbat la Rulează, ca în acest exemplu, utilizăm pașii următori pentru a adăuga noua instanță a Serviciului de Calcul al Norului Oracle în lista de securitate definită în secțiunea Configurarea Instanței pentru Accesul HTTP.



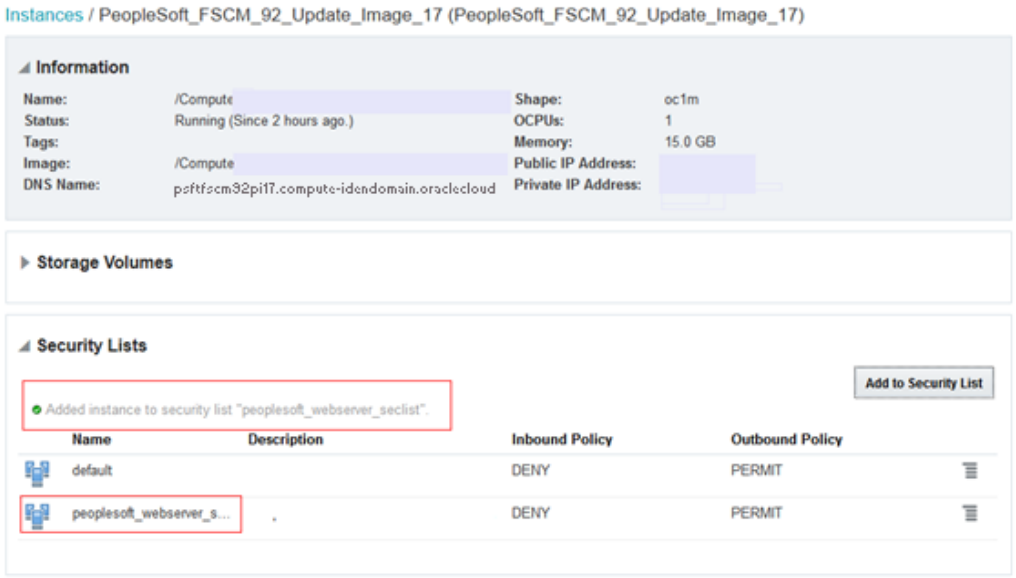
11. Facem clic pe Liste de securitate, apoi facem clic pe Adăugare la lista de securitate.



Se afișează caseta de dialog Adăugare la lista de securitate.

12. Selectăm peoplesoft_webserver_seclist pe care l-am creat mai devreme din lista derulantă Listă de Securitate.

13. Facem clic pe Add. Exemplul apare în zona Listelor de Securitate ca în acest exemplu:

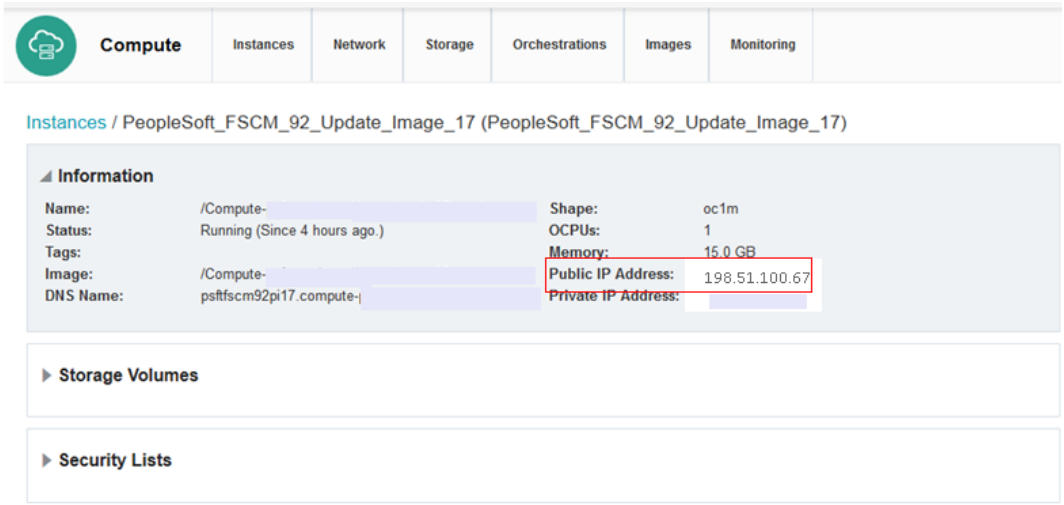


Conectarea la aplicația PeopleSoft

Ne conectăm la instanța PeopleSoft care rulează într-un browser, utilizând o adresă URL construită din numele DNS adresabil public. Pentru a determina adresa URL, găsim adresa IP publică a instanței Serviciului de Calcul al Norului Oracle.

1. Facem clic pe fila Instanțe.
2. Din lista de instanțe afișate, identificăm instanța și meniul corect din dreapta pentru a vedea instanța care rulează.
3. Reținem adresa IP publică.
   URL-ul PeopleSoft va urma întotdeauna acest format pentru HTTP:
   http://oc-public-ip-address-using-hyphens.compute.oraclecloud.com:8000/ps/signon.html
   Pentru HTTPS:
   https://oc-public-ip-address-using-hyphens.compute.oraclecloud.com:8443/ps/signon.html

   De exemplu, adresa URL a aplicației PeopleSoft FSCM 9.2 Update Image 17 găzduită de această instanță Oracle Compute Cloud Service este:
   http://oc-198-51-100-67.compute.oraclecloud.com:8000/ps/signon.html



4. Introducem URL-ul PeopleSoft într-un browser pentru a afișa fereastra de conectare:

Notă: Oracle recomandă cu insistență să se schimbe parolele utilizatorilor PIA standard (PeopleSoft Arhitectura Internet Pură), deoarece Serviciului de Calcul al Norului Oracle se află pe Internetul public.

Conectarea la instanța utilizând SSH

Pentru a configura SSL, după cum s-a menționat anterior, utilizând instrucțiunile din documentația produsului PeopleTools System și Server Administration, trebuie să putem accesa Linux VM cu SSH.

Este posibil să facem SSH la orice instanță a serviciului Linux Serviciu de Calcul al Norului Oracle care este pornită dintr-o imagine PeopleSoft bootabilă din Magazin Nor Oracle folosind id-ul de utilizator opc.

Utilizatorul opc este configurat pentru acces la distanță prin intermediul protocolului SSH folosind cheile RSA. Cheia publică atașată la domeniul de identitate într-un pas anterior este adăugată automat la VM.

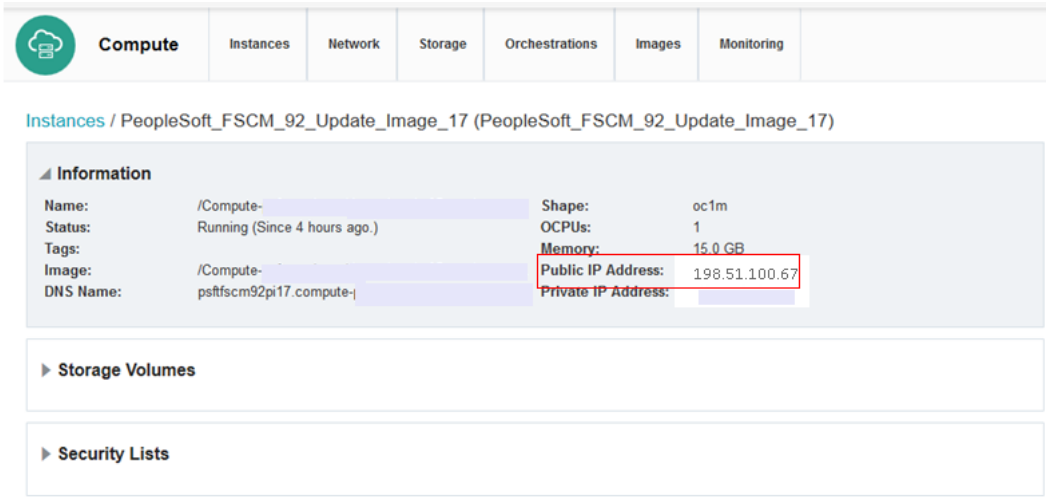
Utilizatorul opc are privilegii sudo și are o parolă implicită, care trebuie schimbată la prima încercare de SSH la VM. Instrucțiunile de modificare a acestei parole se găsesc în secțiunea următoare, Schimbarea parolei implicite pentru utilizatorul opc (obligatoriu). Mai întâi, se urmează pașii din această secțiune pentru a efectua cu succes SSH la instanța PeopleSoft Linux, fie dintr-un sistem UNIX sau UNIX, fie din Microsoft Windows.

Conectarea dintr-un sistem UNIX sau UNIX-Like

1. Introducem următoarea comandă:

```
ssh -o ServerAliveInterval=5 -o ServerAliveCountMax=1 $HOST -i/path/to/<private_key_name> opc@<public_ip_address_of_instance>
```

2. Dacă nu cunoaștem adresa IP publică a instanței, o putem găsi accesând fila Instanțe din consola Serviciului de Calcul al Norului Oracle. Din lista de instanțe afișate, identificăm instanța corectă și utilizăm meniul din partea dreaptă pentru a vizualiza instanța care rulează.
   Căutăm adresa IP publică:



3. Dacă am introdus o frază de acces la crearea perechii de chei SSH, introducem expresia de acces când ni se solicită.

4. La prima conectare la instanță, utilitarul SSH va solicita să confirmăm cheia publică. Ca răspuns la prompt introducem da.

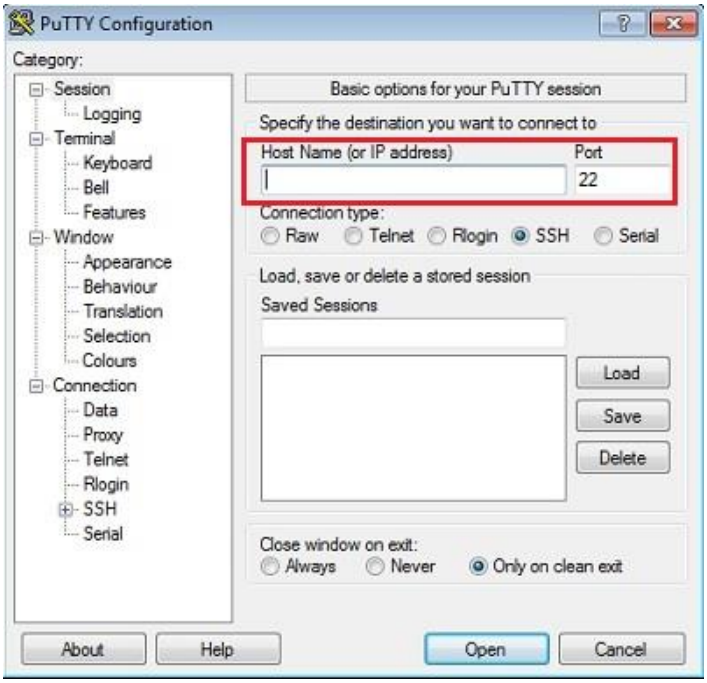
Conectarea dintr-un sistem Windows

1. Pornim PuTTY. Se afișează fereastra Configurare PuTTY, care afișează panoul Sesiune.

2. În câmpul Nume gazdă (sau adresa IP), introducem adresa IP publică a instanței.

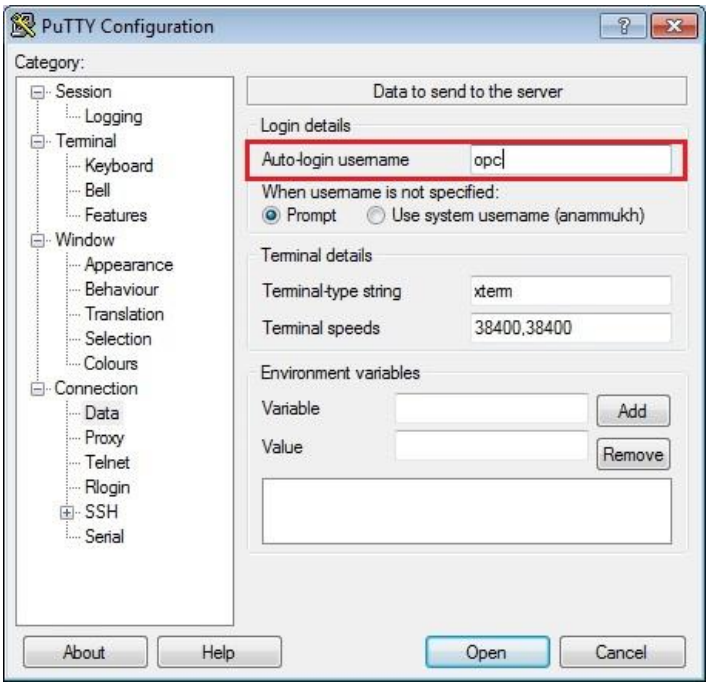
   Notă: Dacă nu cunoaștem adresa IP publică a instanței, o putem găsi accesând fila Instațe din consola Serviciului de Calcul al Norului Oracle și făcând clic pe instanța pentru a accesa pagina cu detalii.

3. În câmpul Tip conexiune, selectăm SSH dacă nu este deja selectat.

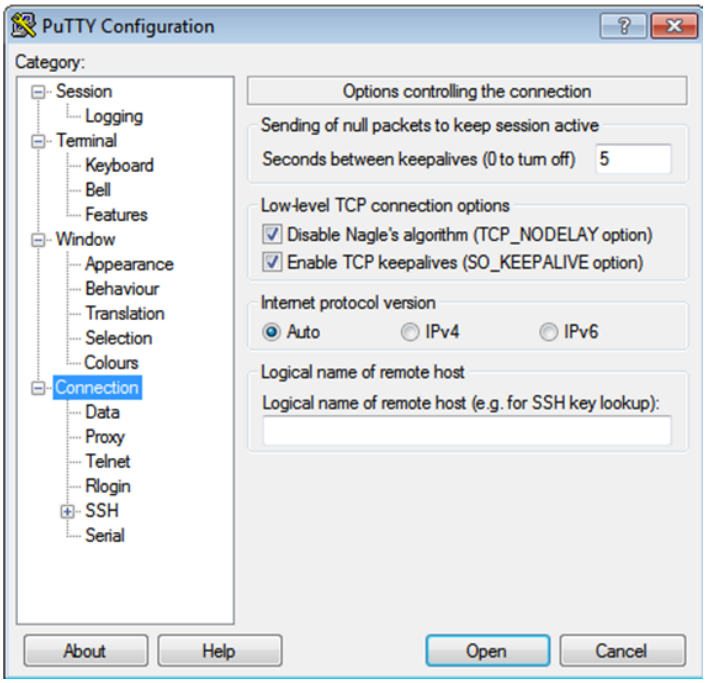


4. În panoul Categorie, extindem conexiunea, apoi facem clic pe Date. Se afișează panoul Date.

5. În câmpul Nume utilizator automat de conectare, introducem opc. Confirmați că opțiunea *Când numele de utilizator nu este specificată* este setată la Prompt.

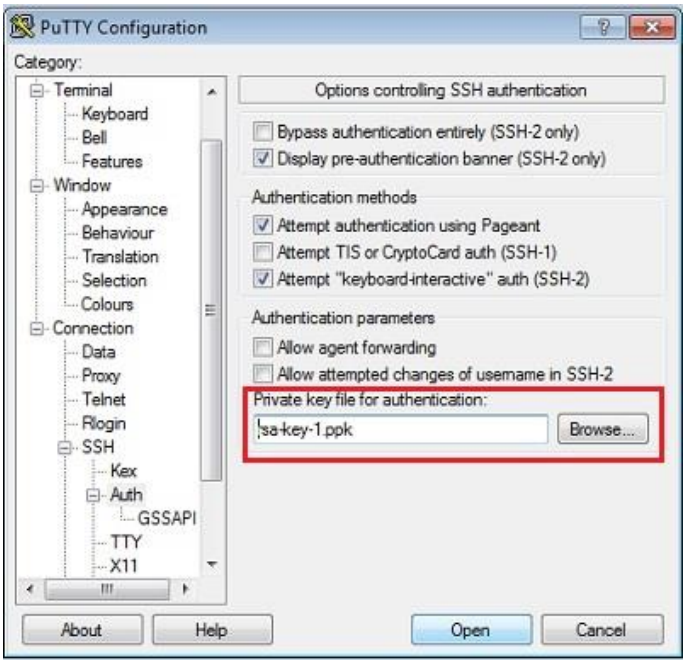


6. În panoul Categorie, facem clic pe Conexiune. Introducem 5 în caseta text Secunde între păstrați (0 pentru a opri).
   Ne asigurăm că este selectată caseta de selectare Enable TCP keepalives (opțiunea SO_KEEPALIVE).



7. În panoul Categorie, extindem SSH, apoi facem clic pe Auth. Se afișează panoul Auth.

8. În fișierul Cheie privată pentru autentificare, facem clic pe Browse și selectăm fișierul cu chei private pe care l-am salvat mai devreme, psa-key-1.ppk în acest exemplu.



9. În arborele Categoria, facem clic pe Sesiune.
   Se afișează panoul Sesiune.

10. În câmpul Sesiuni salvate, introducem un nume pentru această configurație a conexiunii, apoi facem clic pe Salvare.

11. Facem clic pe Deschidere pentru a deschide conexiunea.
    Fereastra Configurare PuTTY este închisă și fereastra PuTTY este afișată.

12. Introducem expresia de acces furnizată pentru perechea de chei SSH.

13. Prima dată când ne conectăm la, este afișată fereastra Alertă de securitate PuTTY, solicitând să confirmăm cheia publică. Facem clic pe Da pentru a continua.

<u>Modificarea parolei implicite pentru utilizatorul opc (obligatoriu)</u>

După ce efectuăm cu succes conexiunea inițială la instanța Serviciului de Calcul al Norului Oracle folosind protocolul SSH, trebuie să schimbăm imediat parola implicită a utilizatorului opc.

1. Dacă nu s-a făcut deja acest lucru, SSH către VM fie dintr-un sistem Linux sau Windows:

```
$ ssh -o ServerAliveInterval=5 -o ServerAliveCountMax=1 $HOST -i/home/bob/.ssh/id_rsa opc@19
2.51.100.67
```

2. Vom vedea următorul mesaj care spune să schimbăm parola, la prima conexiune prin SSH:

```
You are required to change your password immediately (root enforced)
Authorized uses only. All activity may be monitored and reported.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user opc.
Changing password for opc
(current) UNIX password:
```

* Parola implicită (actuală) este OracleCloud.

* Nu putem face nimic de la linia de comandă Linux până când parola implicită nu a fost modificată.

* Schimbăm parola implicită utilizând următoarele linii directoare:

* Utilizați o parolă alfanumerică.

* Lungimea trebuie să fie de minimum 8 caractere.

* Utilizăm cel puțin un caracter alfabetic superior.

* Utilizăm cel puțin un caracter numeric.

* Utilizăm cel puțin un caracter special, cum ar fi @, #, $ și așa mai departe.

* Nu se poate asemăna foarte mult cu un cuvânt din dicționar.

3. Când parola a fost modificată cu succes, vom fi imediat deconectați și ar trebui să vedem un mesaj care să indice succesul, similar cu următorul:

```
You are required to change your password immediately (root enforced)
Authorized uses only. All activity may be monitored and reported.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user opc.
Changing password for opc
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Putem acum efectua SSH la instanță folosind utilizatorul opc după cum a fost direcționat anterior. Parola pentru utilizatorul opc trebuie schimbată cel puțin o dată la 90 de zile.

Bibliografie

- [1] https://en.wikipedia.org/wiki/Cloud_computing
- [2] https://www.tutorialspoint.com/cloud_computing/
- [3] http://www.computerhistory.org/internethistory/1970s/
- [4] https://www.technologyreview.com/s/425970/who-coined-cloud-computing/

- [5] http://www.stargroup.uwaterloo.ca/~mhamdaqa/publications/Cloud_Computing_Uncovered.pdf
- [6] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- [7] http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud/
- [8] http://www.cio.com/article/2375744/business-intelligence/business-intelligence-takes-to-cloud-for-small-businesses.html
- http://www.oracle.com/us/solutions/cloud/oracle-cloud-brief-2565474.pdf
- http://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/compute-iaas/deploy_psft_app_marketplace/deploy_psft_app_marketplace.html#section6