POPIS TEHNOLOGIJA

* GOOGLE COMPUTE ENGINE

Google compute engine (GCE) je infrastruktura kao usluga (IaaS) komponenta Google cloud platforme koja je građena kao globalna infrastruktura koja pokreće Google search engine, Gmail,Youtube i ostale servise.

GCE omogučava klijentima keiranje i pokretanje vlastitih programa na Google fizičkom hardveru.

GCE nam pruža veći broj skalabilnih virtualnih mašina(VMs) koje služe kao računalni cluster za navedenu svrhu.

GCE-om se može upravljati preko RESTful API-a, CLI-a(Command line interface) ili preko Web konzole.

VMs se mogu pokreniti preko standardne slike (system images) ili prilagođene slike kreirane od strane korisnika.

GCE omogučava administratoru da izabere regiju i zonu gdje će podatkovni resursi biti pohranjeni i korišteni. Do sada na raspolganju stoji United States, Europa i Azija.

GCE također pruža paket alata koji omogučava administratorima izgradnju napredne mreže na regionalnom nivou.

Podržava Linux i windows slike (system images) koje su nužne za pokretanje VMs.

Uporaba GCE virtualnih mašina nije besplatna, već se nakon 10-minutnog rada naplačuje po minuti.

* GOOGLE CLOUD SHELL

Google cloud shell nam pruža Command-line pristup našim cloud resursima iz samog browsera.

Omogučava nam da upravljamo našim projektima i resursima bez instaliranja Google Cloud SDK-a ili drugih alata. Uz pomoć Cloud shell-a, Cloud SDK gcloud command-line alati su nam uvijek dostupni i ažurirani.

Cloud shell pruža command-line pristup instanci virtualne mašine (VM) u terminalskom prozori koji se otvara u web konzoli.

Cloud shell tako pruža sigurnost pristupa projektima i resursima korištenjem autorizacije.

Cloud shell također pruža široki izbor već instaliranih i ažuriranih command-line alata iz basha,sh-a,emacs-a,vim-a, kao i administrativnih alata kao što su mysql client i kubernetes.

Osim command-line alata Cloud shell također pruža široki izbor razvojnih alata kao što su Java,Python,Go,node.js, PHP i uby.

Cloud shell pruža 5GB memorije na persistent disku za pohranu podataka koji je mountan kao $HOME direktorij na Cloud shell instanci.

* WEB SERVICE SECURITY (WSS)

WSS je SOAP ekstenzija koja uvodi sigurnosni sloj kod web usluga.

U 2002, Microsoft, IBM, i Verisign su izdali WS-Security specifikaciju jer SSL/TLS nije bio dovoljan kada SOAP poruka prolazi kroz posredne točke.

U 2003, WS-Security je predložen kao OASIS norma, i u 2004 je izdan kao OASIS norma.

WS-Security specificira SOAP sigurnosne ekstenzije koje omogućavaju tajnost uporabom XML Encryption i integritet podataka uporabom XML Signature.

WS-Security također uključuje profil koji specificira kako umetnuti različite tipove binarnih i XML sigurnosnih tokena u WS-Security zaglavljima za provjeru autentičnosti i autorizacijske namjere:

* Korisničko ime s opcionalnim pregledom lozinke (definira kako korisnik Web usluge može dostaviti korisničko ime kao ovlaštenje za provjeru autentičnosti; uz korisničko ime može biti priložen *hashed* lozinka).
* X.509 certifikat (potpisana struktura podataka dizajnirana za slanje javnog ključa stranki koja prima).
* Kerberos etiketa (token za provjeru autentičnosti i sesiju).
* Security Assertion Markup Language (SAML) sigurnosni tokeni (više detalja o SAML kasnije u ovom dokumentu).
* REL dokument (*rights expression language* (REL) odobreni tokeni umetnuti u WS-Security zaglavlja se rabe za autorizaciju).
* XCBF dokument (definira kako uporabiti XML Common Biometric Format (XCBF) jezik za provjeru autentičnosti s WS-Security specifikacijom).

* XML DIGITAL SIGNATURE

Definira sintaksu i pravila za kreiranje digitalnog potpis XML sadržaja.

XML (Extensible Markup Language) je vrlo jednostavan, fleksibilan tekstualni format razvijen iz SGML (Standard Generalized Markup Language) jezika.

SGML je ISO (International Organization for Standardization) standard za definiranje markup jezika za dokumente.

Digitalni potpis je elektronička zamjena za rukom pisani potpis, a služi istoj funkciji. Uz to pruža i potvrdu autentikacije, integriteta, te povjerljivosti izvora i podataka koji se prenose.

digitalni potpis nije kopija ručno pisanog potpisa.

U tehničkom smislu, digitalni potpis stvara i provjerava posebna aplikacija koja generira kriptografske poruke. Kako bi digitalni potpis funkcionirao, stvaraju se dva različita ključa. Prvi, zvan javni ključ, kreira digitalni potpis transformacijom podataka u nerazumljiv kod. Drugi, zvan privatni ključ, provjerava digitalni potpis te dešifrira transformiranu poruku u izvorni oblik. Ovaj sustav je siguran dok je privatni ključ zadržan tajnim.

XML digitalni potpis je u principu digitalni potpis dizajniran za uporabu u XML transakcijama, a može se koristiti za potpisivanje bilo kojeg tipa podataka.

Dobra strana XML digitalnih potpisa je bolja fleksibilnost od digitalnih potpisa kao što su PGP (Pretty Good Privacy) i CMS12 (Cryptographic Message Syntax), jer ne radi na binarnim podacima nego na XML informacijskom skupu.

XML digitalni potpie koristi koncept kanonizacije što omogućuje potpisivanje samo važnog dijela, te uklanjanje manje važnih podataka poput praznih razmaka i završetka retka.

Nepravilno rukovanje XML digitalnim potpisima može dovesti do pojave sigurnosnih ranjivosti. Jedno od važnih obilježja ovih potpisa je da se potpisani XML elementi, zajedno s potpisom, mogu kopirati iz jednog dokumenta u drugi uz zadržavanje mogućnosti za provjeru potpisa.

* XPATH

Xpath je jezik za specifkaciju upita nad XML podacima (kao sql za upite nad relacijskim bazama).

Služi za lociranje dijela XML dokumenta, pronalaženje elemenata I atributa koji odgovaraju određenom kriteriju I omogučava traženje u bilo kojem smjeru (unaprijed, unatrag, u oba smjera).

Rezultat XPath izraza može bit skup čvorova ili atomarnih vrijednost (sadržaj), odnosno bilo koji slijed u podatkovnom modelu.

Zadnja verzija Xpatha je Xpath 3.1(W3C preporuka 21.03.2017) i u usporedbi s Xpathom 1.0(prvom verzijom, W3C preporuka 16.11.1999) podržava bogatiji skup podatkovnih tipova, mapa i nizova, iskorištava tip informacije kod validacije putem XML Scheme i uvodi podršku za JSON.