AWS - globalni pregled

AWS - Global Infrastructure

- AWS Global Infrastructure
  - regions (24) - geografska zona, najčešće sadrži dva (ili više) availability zones
  - availability zones (72) ~ u osnovi možemo ih poistovetiti sa Data Center-om (ponekad su grupisani, pa se nekoliko računa kao jedan). Svaki Data Center je opskrbljen redundantim napajanjem, redundantnom mrežnom infrastrukturom.
  - edge locations - endpointi za AWS - služe za keširanje sadržaja.
    Tipično CloudFront.

AWS - ključni servisi

- Security, Identity and Compliance
- Network and Content Delivery
- Compute
- Storage
- Databases

Lorem Ipsum Dolor

AWS -
Identity Access Management

AWS - Identity Access Management (IAM)

- IAM omogućava upravljanje korisnicima i određivanje nivoa pristupa koji se pojedinim korisnicima dozvoljava na Management Console-i
- Omogućava kreiranje korisnika, grupa, rola i prava
- Obezbeđuje:
  - Centralizovanu kontrolu na AWS nalogu (Centralized Control)
  - Deljeni pristup AWS nalogu (Shared Access)
  - Granularizaciju prava pristupa (Granular permissions)
  - Federalizaciju upravljanja identitetom (Identity Federation - Active Directory, LinkedIn, Facebook…)
  - Multifactor Authentication
  - Privremeni pristup (temporary access)
  - Upravljanje politikom izmene lozinki (password rotation policy)
  - PCI/DSS compliance

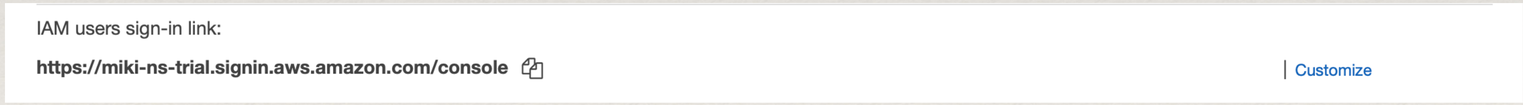
AWS - IAM key terms

- IAM ključni termini

  1. Users - pojedinačni korisnik
  2. Groups - kolekcija pojedinačnih korisnika. Prava dodeljena grupi nasleđuju svi članovi grupe
  3. Policies - policy documents - JSON dokumenti koji specificiraju prava pojedinačnih korisnika, grupa i rola
  4. Roles - uloge koje mi kreiramo i određujemo koje AWS resurse mogu da koriste

AWS - IAM Essentials

- Root account - email nalog sa kojim je kreiran AWS nalog - on je u God modu - može da radi šta hoće na celom AWS nalogu
- Po logovanju na IAM nije loše promeniti account alias - jer je inače adresa naloga (koju ostali korisnici koriste kao link za pristup) sa numeričkim brojem AWS accounta



- Dobro je odmah po logovanju na IAM uključiti MFA za root account
- Kad god se nešto podešava u IAM to se uvek obavlja u „Global“ regionu

AWS - IAM Kreiranje grupa

- Prilikom kreiranja grupa zadaje se naziv grupe
- Neophodno je izabrati Policy koji se primenjuje na novokreiranu grupu, u startu se nudi AWS managed policies, mada je moguće kreirati i sopstvene.

AWS - IAM Kreiranje korisnika

- Kreiranjem novog korisnika omogućava se pristup dodatnim korisnicima AWS nalogu
- Pri kreiranju za korisnika se može odobriti
  - Programmatic access
  - AWS Management Console Access
- Korisniku se može zahtevati da pri prvom logovanju mora da promeni password
- Korisniku se zatim dodeljuju prava (pri tome prvo ga treba dodati u određenu postojeću grupu ili napraviti novu).

AWS - IAM Kreiranje korisnika

- Kada se korisnik napravi dobiće i
  - Access Key ID - ovo se koristi kao username za programski pristup AWS,
  - Secret Access Key - ovo se koristi kao password za programski pristup AWS
- Korisnik se može konfigurisati tako da može samo da se uloguje na AWS, ili da koristi samo programski pristup (koristeći Access Key ID i Secret Access Key, ali tada ne može da se uloguje na AWS), ili da ima oba prava pristupa AWS nalogu

AWS - IAM Password Policy

- Korisnik koji ima administratorska prava može podesiti politiku kreiranja passworda koju svi korisnici moraju poštovati (minimalna dužina, da li se zahtevaju mala, velika slova, cifre, specijalni znaci, da li i u kom periodu password ističe, da li sme da se koristi već korišćeni…)

AWS - IAM - kreiranje rola

- Role primarno određuju prava da određeni AWS servis pristupi i koristi neki drugi AWS servis koji smo kreirali u našem AWS nalogu (npr. virtuelnoj mašini se dozvoljava pristup S3 storage-u)
- Prilikom kreiranja Role prvo se bira servis koji će je koristiti, a zatim policy koja se primenjuje za pristup

Lorem Ipsum Dolor

AWS - Cloud Watch

AWS - Cloud Watch

- Management servis kojim se nadzire upotreba resursa na vašem AWS nalogu
- Omogućava:
  - da se postavi metrika za merenje upotrebe određenih servisa, kao i alarmi koji nas obaveštavaju ako upotreba određenih resursa prevazilazi naš postavljeni prag
  - monitoring korišćenih servisa i pristup logovima
  - kreiranje prilagođenih dashboarda
  - pisanje pravila koji nam omogućavaju da lakše pratimo događaje od interesa
- Npr moguće je postaviti alarme koji će nas upozoravati da određeni servis dostiže prag koji smo postavili za to koliko želimo da platimo

Lorem Ipsum Dolor

AWS - S3

AWS - Secured Storage Services (S3)

- Obezbeđuje prostor za sigurno smeštanje fajlova
- Object based
- Podaci se čuvaju na više uređaja i na više lokacija
- Fajlovi mogu biti do 5TB
- Fajlovi se smeštaju u „korpe“ (Buckets)
  - Bucketi praktički predstavljaju foldere na cloudu
- S3 koristi univerzalni namespace - tako da ime mora biti jedinstveno jer se za svaki bucket kreira web adresa
- Kada se uspešno uploaduje fajl na s3 bucket response je u formi HTTP response statusa 200 OK

AWS - S3 objekti

- S3 objekti = fajlovi
- S3 objekat ima
  - key - naziv objekta
  - value - podaci (bajtovi)
  - version ID (isti fajl može postojati u više verzija)
  - metadata - opisni podaci
  - subresources - npr. access control list

AWS - konzistentnost S3 objekata

- Za upload novih fajlova
  Read after Write - fajl je dostupan za čitanje odmah nakon potvrde uspešnog uploada
- Za overwrite ili delete fajlova
  Eventual consistency - neophodno je određeno vreme da se promene propagiraju pa nije garantovavno da su promene odmah vidljive svima

AWS - S3 osobine

- Arhitektura je izgrađena da podržava 99,99% dostupnost S3 platforme
- Amazon garantuje 99,9% dostupnost S3 platforme
- Amazon garantuje 99,999999999% trajnost podataka (11 nines)

AWS - S3 osobine

- Tiered storage (6 tiers)
- Lifecycle Management - omogućava nam da upravljamo objektima i njihovim raspoređivanjem po slojevima (npr. pravilo da fajlove starije od mesec dana automatski prebacujemo u sledeći tier)
- Versioning - verzioniranje objekata je podržano
- Podržava enkripciju (at rest)
- Moguće je zahtevati MFA za operacije brisanja
- Zaštita podataka obezbeđena je pomoću Access Control List i Bucket Policy

AWS - S3 klase

- S3 Standard
  - 99,99% availability
  - 99,999999999% durability
  - Podaci se čuvaju redundantno na više uređaja, na više lokacija, podaci mogu preživeti uništenje dve lokacije istovremeno

AWS - S3 klase

- S3-IA (Infrequently Accessed)
  - Namenjeno za podatke kojima se ređe pristupa, ali kada se pristupi zahteva se velika brzina
  - Jeftiniji od S3 Standard, ali se plaća dodatni „retrieval fee“

- S3 One Zone - IA
  - isto kao i gore, ali se ovom opcijom smanjuju troškovi jer se ne obezbeđuju višestruke kopije u različitim availability zonama

AWS - S3 klase

- S3 Inteligent Tiering
  - Koristi AI i ML kako bi utvrdio obrasce korišćenja za različite objekte i shodno tome obezbedio (finansijski) najpovoljnije raspoređivanje objekata po različitim klasama storage-a

AWS - S3 klase

- S3 Glacier
  - Storage za sigurno, trajno i jeftino čuvanje arhiviranih podataka.
  - Vreme pristupa (preuzimanja arhiviranih podataka) može da se konfiguriše između nekoliko minuta do nekoliko sati.

- S3 Glacier Deep Archive
  - najjeftini storage. Kao i prethodni služi za arhiviranje podataka, ali je kod ovoga vreme pristupa (preuzimanja arhiviranih podataka) veće od 12h.

AWS - S3 naplata

- S3 se naplaćuje po sledećim principima
  - storage - po količini podataka
  - requests - po broju pristupa podacima
  - storage management pricing - različite cene za različite klase (tiers)
  - data transfer pricing
  - transfer acceleration - brz i efikasan način za prenos fajlova na velike udaljenosti između krajnjih korisnika i S3 bucketa. Koristi CloudFront (koristeći edge locations krajnji korisnici pristupaju AWS, a zatim se privatnim backbone-om podaci prebacuju na S3 storage)
  - cross region replication transfer - omogućava da se uspostave pravila kojim se određeni podaci (bucketi) automatski repliciraju u druge regione

AWS - S3 security

- Svi bucketi su po kreiranju privatni
- Prava pristupa se kontrolišu putem
  - Bucket policies - određuju prava pristupa na nivou bucketa
  - Access Control Lists - prava se mogu podešavati do nivoa individualnih fajlova
- S3 Buckets se mogu konfigurisati tako da se u logovima zapisuje svaki pristup bucketu

AWS - S3 security

- Encription in transit - podaci se kriptuju tokom prenosa (HTTPS)
  - SSL/TLS
- Encription at rest - podaci se kriptuju na samom mediju
  - server side encription
    - S3 Managed Keys - (SSE-S3) / Amazon upravlja svim ključevima
    - AWS Key Management Service (SSE-KMS)/ Managed Keys - ključevima se upravlja od strane Amazona i klijenta
    - Server Side Encription sa ključevima koje dostavlja klijent (SSE-C)
  - client side encription - klijent enkriptuje podatke kod sebe i kao takve ih uploaduje na S3 storage

AWS - S3 version control

- Verzioniranje omogućava da se sačuvaju sve verzije nekog objekta (fajla), dakle sve izmene, pa i brisanje
- BITNO: jednom kada se za neki bucket uključi verzioniranje ne može se isključiti može se samo prebaciti u suspendovano stanje. Za potpuno isključivanje bi bilo neophodno obrisati bucket i kreirati novi koji nije verzioniran
- Verzioniranje se integriše sa Lifecycle pravilima
- Za operacije brisanje verzioniranje podržava MFA Delete - koji zahteva višefaktorsku autentikaciju za DELETE operacije
- Prilikom svakog uploada nove verzije istog fajla prava pristupa se resetuju (fajl se mora ponovo učiniti javno dostupnim, ukoliko je to potrebno)
- Kada se uključi opcija prikaza verzija moguće je videti sve verzije fajla u bucketu (inače se prikazuje samo poslednja)
- BITNO: Ukoliko je verzioniranje uključeno, a bucket sadrži velike fajlove koji se često menjaju, to će jako negativno uticati na ukupnu količinu podataka koje bucket sadrži - ozbiljno razmotriti pri razmatranju arhitekture sistema.

AWS - S3 brisanje verzioniranih fajlova

- Kada se obriše verzionirani fajl zapravo se samo u bucket zapiše delete marker kao nova verzija fajla. Ovo se i vidi kada se za bucket uključi prikaz verzija.
- Stare verzije još uvek postoje i dostupne su (ako smo ih ostavili kao public) preko linka
- Ukoliko želimo undelete „obrisanog“ objekta (fajla) dovoljno je da se ukloni delete marker i poslednja verzija će ponovno postati vidljiva u bucketu. Svaku verziju moguće je pojedinačno obrisati preko menija Action u bucketu.

AWS - S3 lifecycle management

- S3 Lifecycle management omogućava da se postave pravila za upravljanje objektima u bucketu
  - Obezbeđuje transfer objekata u različite S3 tier-s
  - Moguće je postaviti i pravila za proglašavanje objekata „isteklim“ (expired objects) koji će biti automatski uklonjeni iz S3 storage-a

AWS - S3 Object Lock

- S3 Object Lock omogućava da se za neki objekat definiše zaključavanje tj. primeni WORM (Write Once Read Many) model pristupa.
- Na ovaj način se objekat štiti od naknadnih izmena ili brisanja. Ovo može biti postavljeno kao trajno ili u zadatom vremenskom periodu.
- Nekoliko režima:
  - Governance mode - objekat standardno ne može biti menjan niti brisan, ali se specijalnim korisnicima mogu odobriti prava da promene ovo podešavanje ili uklone sam objekat.
  - Compliance mode - nijedan korisnik, čak ni root user AWS naloga ne može menjati ili ukloniti objekat niti skratiti period u kome je objekat zaključan.

AWS - S3 Object Lock

- S3 Object Lock Retention Period - vremenski period u kome se primenjuju pravila zaključavanja objekat (korisno kada postoji obaveza da se neki dokumenti čuvaju određeni vremenski period). Nakon isteka tog perioda objekat može biti menjan ili obrisan, osim ako se na njega postavi *Legal Hold*
- Legal Hold obezbeđuje zaključavanje objekta, ali za razliku od Retention Perioda nije vremenski ograničen, ukida se eksplicitnim skidanjem Legal Holda sa objekta (zna se ko je to uradio, a sam korisnik mora imati s3:PutObjectLegalHold pravo).

AWS - S3 Glacier Vault Lock

- S3 Glacier Vault Lock - omogućava da se postave i sprovode kontrole nad S3 Glacier Vaults putem Vault Lock policy.
- Mogu se specificarti WORM pravila, i druge kontrole, kao što je zaključavanje same Vault Lock policy.
- Jednom kada se postavi ne može biti menjan.

AWS - S3 Performanse - Prefixi

- Kako dizajnirati AWS aplikaciju da ima najbolje performanse prilikom korišćenja S3 storage-a?
- Bitan koncept S3 Prefixi
  - Šta je prefix - sve što se nalazi između bucket name i object name
  - mybucket/category1/folder1/slika.jpg > **category1/folder1**
  - mybucket/files/docs/doc1.docx > **files/docs**
- S3 obezbeđuje obradu do 3500 PUT/COPY/POST/DELETE zahteva i do 5500 GET/HEAD zahteva u sekundi **po prefixu**
- **Ukoliko se zahtevi rasporede na više prefixa ukupne performanse su bolje jer aplikacija može da obradi više zahteva u sekundi**

AWS - S3 Performanse - KMS kvote

- Ukoliko se koristi SSE-KMS treba voditi računa da se svaki pristup broji do zadate kvote (KMS limits)
  - Pri uploadu se poziva Generate Data Key
  - Pri downloadu Decrypt
- KMS kvota se trenutno ne može povećati na zahtev, zavisi od regiona (u različitim regionima ovi hard limiti su različiti 5500, 10000 ili 30000 zahteva u sekundi ka KMS API-ju).

AWS - S3 Performanse - Uploads

- Performanse pri uploadu se poboljšavaju ako se koristi Multipart Upload
- Preporučljiv je za sve fajlove veće od 100 MB
- Obavezan je za sve fajlove preko 5GB
- Paralelizuje upload (povećava efikasnost)

AWS - S3 Performanse - Downloads

- Koncept analogan multipart uploadu
- S3 Byte range fetches
- Paralelizuje download tako što se specificira byte opseg u kome se fajl izdeli na segmente, a zatim se oni downloaduju istovremeno
- Ukoliko i dođe do greške pri downloadu ona će verovatno biti samo na jednom segmentu čiji download će se onda ponoviti
- Ubrzava download
- Omogućava da se downloaduju samo određeni segmenti (npr treba nam samo zaglavlje nekog fajla).

AWS - S3 Select

- Omogućava da aplikacije sa S3 storage-a iz objekta preuzmu samo onaj podskup podataka koji im trenutno treba
- Koristi se jednostavna SQL sintaksa
- Dramatično utiče na performanse aplikacije
  - npr ako imamo CSV fajlove u zip arhivama, morali bismo obaviti download, unzip i zatim pristup željenim podacima u CSV fajlovima, ali ako se koristi S3 Select moguće je filtriranje uraditi već na S3 i downloadovati samo fragment podataka koji je potreban

AWS - Glacier Select

- Omogućava da aplikacije direktno koriste SQL nad objektima koji se nalaze u Glacier arhivama
- Ovo je jako bitno za performanse, jer neke aplikacije moraju da ispoštuju zakonske zahteve i čuvaju podatke kao arhive, ili se zbog optimizacije troškova čuvanja velike količine podataka podaci brzo prebacuju u Glacier čim nisu svakodnevno neophodni

AWS - S3 deljenje bucketa između AWS naloga

- Moguće je, ali je prethodno potrebno kreirati AWS organization - organizacija predstavlja više AWS accounta koji su objedinjeni pod jednim glavnim nalogom
- Root nalog organizacije omogućava i objedinjenu naplatu servisa (manji troškovi jer se servisi sumiraju pre obračuna cene pa je jedinična cena manja)
- Po preporuci ovaj root nalog AWS organizacije treba koristiti samo za upravljanje i obračun troškova, ne treba u njemu instalirati aplikacije

AWS - S3 deljenje bucketa između AWS naloga

- 3 načina:
  - korišćenjem Bucket Policies i IAM - važi za sve u bucketu. Moguće je samo za programski pristup sadržajima (ne može se koristiti preko AWS console).
  - korisšćenjem Bucket ACL i IAM - za deljenje pojedinačnih objekata, i ovde važi da je samo za programski pristup.
  - Cross Account IAM Roles - ovo je jedini način koji dopušta i programski i pristup preko AWS konzole.

AWS - Cross Account IAM Roles

- Kreira se rola kao i bilo koja druga, ali se za trusted objekat bira drugi AWS nalog (AWS account)
  - mora se uneti Account number
  - kada se rola kreira za nju se mora zakačiti odgovarajuća Policy (u ovom slučaju želimo samo S3 access)
- Da bi drugi account imao mogućnost da iskoristi ovakvu rolu u njemu mora biti kreiran user (ne može se raditi switch role sa root nalogom)
- Nakon switch role, dati user će biti ulogovan na drugi AWS account (onaj čiji nalog želimo da delimo)

AWS - Cross Region Replication

- Da bi cross region replication CRR radio mora biti ukljuceno verzioniranje na bucketu
- Kada se kreira replikacija kreira se novi bucket u drugom regionu i uspostavlja se veza između source i destionation bucketa.Jednom kreiran ovaj bucket se vidi na listi nasih S3 bucketa.
- Moguće je podesiti da se prilikom replikacije menja tip storage-a (npr. replikacija se radi u jeftiniji tier)
- Prilikom kreiranja replikacije svi u tom momentu postojeći objekti (fajlovi) iz source bucketa neće automatski biti replicirani. Tek izmene nastale NAKON kreiranja replikacije će biti preslikane i na destination.
- Ukoliko se kreira delete marker za objekat on SE NE REPLICIRA
- Takođe ako se obriše specifična verzija fajla usource bucketu - brisanje se NE REFLEKTUJE u destination bucketu (ovo je svesna i namerna odluka Amazona)

AWS - S3 Transfer Acceleration

- S3 Transfer Acceleration koristi CloudFront Edge Network kako bi ubrzao upload fajlova u S3 bucket
- Umesto da se fajlovi uploaduju direktno u S3 bucket, koristi se poseban URL kojim se upload usmerava ka Edge Location koja će naknadno preneti fajl u bucket
- Na ovaj način prenos fajla između Edge Location i S3 bucketa se obavlja preko Amazonove backbone mreže
- Amazon je izgradio i Tool kojim se radi poređenje brzine transfera preko različitih Edge lokacija

AWS - Data Sync

- omogućava da se velike količine podataka prebace efikasno na/sa AWS
- koristi se kada imamo on-premise data centar odakle veliku količinu podataka treba redovno da sinhronizujemo sa AWS.
- koristi se sa NFS i SMB kompatibilnim fajl sistemima. Može se koristiti i za EFS to EFS replikaciju.
- na privatnom data centru se instalira AWS Data Sync agent koji zatim
  - prebacuje fajlove na AWS (može se podesiti interval sinhornizacije)
  - čita izmene sa AWS i prebacuje u naš fajlsistem
  - automatski radi enkripciju
  - automatski radi data integrity check (kako uprenosu tako i u mirovanju)

Lorem Ipsum Dolor

AWS - Cloud Front

AWS - Cloud Front Overview

- Cloud Front je AWS Content Delivery Network (CDN)
- Omogućava da se sadržaji isporučuju korisnicima preko distribuirane mreže servera u zavisnosti od geografske lokacije
- Zasniva se na Edge Locations - serverima na kojima se kešira sadržaj
- Umesto direktne komunikacije korisnika sa serverom na kojem je sadržaj hostovan, korisnik uspostavlja vezu prema lokalnoj Edge Location

AWS - Cloud Front Overview

- Edge Location - pristupni server sa keširanim sadržajem - postoji ih više za svaki Availability Zone, raspoređenih po svetu
- Origin - stvarna lokacija na kojoj se originalni sadržaj nalazi
- Distribution - kolekcija Edge Locations

- Cloud Front omogućava isporuku svih sadržaja - zahtevi se automatski rutiraju na najbližu Edge Location, tako da se postižu najbolje performanse
-

AWS - Cloud Front Distributions

- Postoje dva tipa:
  - Web Distribution - za websiteove
  - RTMP - za streaming multimedijalnih sadržaja

AWS - Edge Locations ponašanje

- Edge Locations nisu samo ReadOnly - na njih se može i slati sadržaj (Transfer Acceleration)
- Objekti se na Edge Location zadržavaju u skladu sa definisanim TTL (Time To Live)
- Ukoliko nam zatreba možemo i prinudno invalidirati objekte u Edge Locations (cache invalidation), ALI OVO SE NAPLAĆUJE POSEBNO.

AWS - Kreiranje Cloud Front distribucije

- Bira se Origin - vaš Bucket, EFS, Route 53…
- Opciono bira se Origin Path (npr. ukoliko imamo podfoldere u bucketu, možemo distribuciju zakačiti samo za neku putanju ne za ceo bucket)
- Ukoliko želimo možemo forsirati da svi korisnici moraju pristupati sadržaju preko distribucije - u tom slučaju se uključi opcija Restrict Bucket Access
- Postoje dva načina podešavanja politike keširanja
  - legacy - biramo min max TTL
  - korišćenjem Cache Policy i Origin Cache policy - ovo je preporučeno
    - Ovo je Managed rešenje
- Smooth Streaming omogućava bolji streaming - ali ne sme se uključiti za MS IIS
- Moguće je ograničiti korisnički pruistup tako što se zahteva pristup preko signed URL i signed Cookie

AWS - Kreiranje Cloud Front distribucije

- Cloud Front distribucija se može podesiti tako da za određene evente koristi Lambda funkcije
  - Events: View request, View Response, Origin Request, Origin Response
  - Kada se desi podešeni event trigeruje se odgovarajuća Lambda funkcija
- Može se podesiti na koje tipove zahteva se Cache koristi (npr samo za GET i HEAD, ali ne za POST i PUT, u tom slučaju to bi bio samo READ ONLY Cache)
- Kada se kreira potrebno je određeno vreme da se distribucija aktivira. Dobija se domain name za datu dristirbuciju.
- Kada se želi ukloniti Cloud Front distribucija, neophodno je prvo disableovati pa je tek nakon toga moguće njeno brisanje.

AWS - Signed URLs / Signed Cookies

- Namenjen je za situacije kada na određenom sajtu treba obezbediti “premium access” tj. obezbediti da samo određeni korisnici imaju pravo pristupa nekim ekskluzivnim sadržajima
- Signed URL se dodeljuje striktno pojedinačnom fajlu (ne koristi se za foldere)
- Signed Cookie je za više fajlova

AWS - Signed URLs

- Kada se kreira signed URL za njega se “zakači” i polisa koja najčešće sadrži informacije:
  - vreme do kog dati URL važi
  - IP opsezi sa kojih je pristup dozvoljen
  - Trusted signers - koji AWS nalozi imaju pravo kreiranja signed URLa

AWS - Cloud Front Signed URLs - proces pristupa

- Pristup se obavlja preko Cloud Fronta, a iz cloud fronta se resursu (bucketu, EC2, ELB…) obavlja korišćenjem OAI (Origin Access Identity). Korisnik resursu ne može pristupiti direktno.
- Klijent se loguje na palikaciju koja koristi resurs za koji treba obezbediti “premium pristup”.
- Ta aplikacija koristi SDK da generiše Signed URL za dati resurs
- Signed URL se proseldi korisniku
  - Korisnik pristupa preko tog URL-a (posredstvom Cloud Front-a) tom resursu

AWS - S3 Signed URLs

- Razlikuje se od Cloud Front Signed URL-ova
- koristi se kada se ide na direktan pristup S3 bucketima
- U ovom slučaju se korišćenjem signed URL-a izdaje zahtev koji kao da je poslao IAM User koji je i kreirao signed URL (dakle svi koji pristupaju korišćenjem ovakvog URL-a imaju isto pravo kao i onaj koji ga je kreirao)
- Uvek je vremenski ograničen

AWS - Snowball

- Poseban servis namenjen importu eksportu ogromnih količina fajlova u/iz S3
- Faktički poseban appliance - suštinski ogroman disk (secured casing i sl.)

AWS - Storage Gateway

- Servis koji služi da poveže on-premises softver sa cloud storage-om.
- Na taj način se in-house aplikacije trasnsparentno povežu sa AWS storage-om
- Može biti virtuelni ili fizički uređaj kojim se podaci repliciraju na AWS Storage
- Najčešće se preuzima kao VM image (podržani hipervisori su Hyper-V i VMWare ESXi) koji se instalira on-premise. Nakon toga se kroz proces aktivacije dati gateway “našnira” na storage odgovarajućeg AWS naloga

AWS - Storage Gateway

- Tri tipa:
  - File Gateway (podržava NFS & SMB) - mountuje se u filesistem i fileovi se snimaju u povezane S3 buckete (sve politike definisane na buckete važe i za ovako postavljene fajlove)
  - Volume Gateway (iSCSI) - faktički se čuvaju kopije celih (virtuelnih ili fizičkih) diskova
    - Stored Volumes
    - Cached Volumes
  - Tape Gateway (virtuelni tape device - library)

AWS - Volume Gateway

- Koristeći iSCSI aplikacije “vide” volume:
  - Podaci snimljeni na volume koji je kreiran na gatewayu se asinhrono snimaju na Cloud kao EBS snapshots. Svi snapshoti su inkrementalni i svi se komprimuju kako bi se smanjili troškovi.
  - Stored Volumes - primarna kopija podataka se čuva lokalno, a backup se asinhorno prebacuje na AWS. Low latency storage.
  - Cached Volumes - samo podaci kojima se često pristupa se čuvaju lokalno. Kada se podaci snimaju na ovakav volume, oni se prebacuju na Amazon S3, dok se samo nedavno korišćeni podaci čuvaju na lokalu.

AWS - Athena & Macie

- Athena -
  - serverless, interaktivni servis za pretaživanje koji omogućava da se preko SQL upita direktno pretražuje sadržaj S3 bucketa
- Macie je alat za proveru PII (Personally Identifiable Information)
  - omogućava uvid na Dashboardima, kreira Reporte i Alarme
  - alat koji pomaže da se spreči krađa identiteta