AWS Certified Cloud Practitioner (CLF-C02) විභාග මාර්ගෝපදේශය (Exam Guide) සහ AWS Well-Architected Framework

---

1. Domain 1: Cloud Concepts (වලාකුළු සංකල්ප - විභාග බර තැබීම: 24%)

- 1.1 AWS Cloud හි වාසි සහ මූලික සංකල්ප (Benefits of AWS Cloud):
    - Agility, Elasticity, High Availability, සහ Economies of Scale පිළිබඳ අවබෝධය.
- 1.2 AWS Well-Architected Framework හි නිර්මාණ මූලධර්ම (Design Principles):
    - ප්‍රධාන කුළුණු 6 (6 Pillars): Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, සහ Sustainability.
- 1.3 AWS Cloud වෙත සංක්‍රමණය වීම (Cloud Migration Strategies):
    - AWS Cloud Adoption Framework (AWS CAF) සහ සංක්‍රමණ උපායමාර්ග.
- 1.4 Cloud Economics (වලාකුළු ආර්ථික විද්‍යාව):
    - Fixed costs vs. Variable costs, On-premises හා සසඳන විට පිරිවැය ඉතිරිය සහ Rightsizing.

2. Domain 2: Security and Compliance (ආරක්ෂාව සහ අනුකූලතාව - විභාග බර තැබීම: 30%)

- 2.1 AWS Shared Responsibility Model (බෙදාගත් වගකීම් ආකෘතිය):
    - AWS හි වගකීම් (Security OF the Cloud) සහ පාරිභෝගිකයාගේ වගකීම් (Security IN the Cloud).
- 2.2 AWS Security, Governance, සහ Compliance සංකල්ප:
    - AWS Artifact, AWS CloudWatch, AWS CloudTrail, AWS Config, සහ Encryption ක්‍රම (at rest සහ in transit).
- 2.3 Access Management (පිවිසුම් කළමනාකරණය):
    - AWS Identity and Access Management (IAM), Root Account ආරක්ෂා කිරීම, Least Privilege මූලධර්මය, සහ Multi-Factor Authentication (MFA).
- 2.4 ජාල හා පද්ධති ආරක්ෂණ මෙවලම් (Network Security Tools):

    - Security Groups, Network ACLs, AWS WAF, Shield, සහ Amazon GuardDuty.

3. Domain 3: Cloud Technology and Services (තාක්ෂණය සහ සේවාවන් - විභාග බර තැබීම: 34%)

- 3.1 AWS භාවිතය සහ යෙදවුම් ක්‍රම (Deployment and Operation):
    - AWS Management Console, CLI, SDKs, සහ Infrastructure as Code (IaC).
- 3.2 AWS Global Infrastructure (ගෝලීය යටිතල පහසුකම්):
    - Regions, Availability Zones (AZs), Edge Locations, සහ Local Zones.
- 3.3 ප්‍රධාන AWS සේවාවන් (Core AWS Services):
    - Compute (ගණනය කිරීම් සේවා): Amazon EC2, AWS Lambda, AWS Fargate, Amazon ECS, Amazon EKS, Auto Scaling.
    - Storage (ගබඩා සේවා): Amazon S3, Amazon EBS, Amazon EFS, S3 Glacier.
    - Databases (දත්ත සමුදා සේවා): Amazon RDS, Amazon Aurora, Amazon DynamoDB.
    - Networking (ජාලකරණ සේවා): Amazon VPC, Amazon Route 53, AWS Direct Connect, AWS VPN.
    - AI/ML සහ Analytics: Amazon SageMaker, Amazon Lex, Amazon Athena, AWS Glue, Amazon QuickSight.

4. Domain 4: Billing, Pricing, and Support (ගාස්තු, මිලගණන් සහ සහාය - විභාග බර තැබීම: 12%)

- 4.1 AWS මිලකරණ ආකෘති (Pricing Models):
    - On-Demand, Reserved Instances, Spot Instances, සහ Savings Plans.
- 4.2 පිරිවැය කළමනාකරණ මෙවලම් (Cost Management Tools):
    - AWS Cost Explorer, AWS Budgets, AWS Cost and Usage Report (CUR), සහ Free Tier කොන්දේසි.
- 4.3 තාක්ෂණික සහාය සහ සම්පත් (Technical Resources & Support Options):
    - AWS Support Plans (Developer, Business, Enterprise), AWS Trusted Advisor, සහ AWS Partner Network.

AWS Certified Cloud Practitioner (CLF-C02) විභාගයේ Domain 1: Cloud Concepts (වලාකුළු සංකල්ප) යනු මුළු විභාග ලකුණු ප්‍රමාණයෙන් 24% ක් ආවරණය වන ප්‍රධාන කොටසයි.

1.1 AWS Cloud හි වාසි සහ මූලික සංකල්ප (Benefits of AWS Cloud)

මෙම කොටසේදී සාම්ප්‍රදායික On-premises IT පද්ධති සමග සසඳන විට AWS Cloud භාවිතයෙන් ලැබෙන ප්‍රධාන වාසි අධ්‍යයනය කෙරේ:

- Agility (චලනශීලීබව / කඩිනම්බව):
  - සාම්ප්‍රදායික IT පරිසරයක සර්වර් එකක් මිලදීගෙන සකස් කිරීමට සති ගණනක් හෝ මාස ගණනක් ගතවේ. නමුත් AWS හිදී විනාඩි කිහිපයකින් අවශ්‍ය Cloud සම්පතක් (Compute, Storage) ලබාගෙන පරීක්ෂණ සිදුකළ හැක.
  - උදාහරණය: මෘදුකාංග සංවර්ධකයෙකුට නව App එකක් පරීක්ෂා කිරීමට සර්වර් එකක් අවශ්‍ය වූ විට, භෞතික සර්වර් මිලදී නොගෙන විනාඩි 2 කින් AWS EC2 instance එකක් සාදාගෙන වැඩ නිමවූ පසු එය ක්ෂණිකව terminate (Delete) කළ හැක.
- Elasticity (නම්‍යශීලීබව / ප්‍රසාරණය හා සංකෝචනය):
  - පද්ධතියට පැමිණෙන පරිශීලක ඉල්ලුම (traffic) අනුව ස්වයංක්‍රීයව සර්වර් ප්‍රමාණය වැඩිවීම (scale out) සහ ඉල්ලුම අඩුවන විට නැවත සර්වර් ප්‍රමාණය අඩුවීම (scale in).
  - උදාහරණය: ඔන්ලයින් වෙළඳසැලක (e-commerce store) විශේෂ වට්ටම් සේල් පවතින දිනවලදී විශාල පිරිසක් පැමිණෙන විට සර්වර් ප්‍රමාණය ස්වයංක්‍රීයව වැඩිවන අතර, සේල් එක අවසන් වූ පසු සාමාන්‍ය මට්ටමට සර්වර් ප්‍රමාණය අඩුවෙයි.
- High Availability (ඉහළ පවතිනබව / නොබිඳෙන පැවැත්ම):
  - පද්ධතියේ යම් කොටසක් හෝ දත්ත මධ්‍යස්ථානයක් බිඳවැටුණද, වෙනත් Availability Zone එකක් හරහා අඛණ්ඩව සේවාව ලබාදීමේ හැකියාව.

    ○ උදාහරණය: එක් Data Center එකක විදුලිය විසන්ධි වුවද, වෙනත් AZ එකක ක්‍රියාත්මක වන සර්වර් මගින් App එක කිසිදු බාධාවකින් තොරව පවත්වාගෙන යාම.
- Economies of Scale (පරිමාණයේ ආර්ථික වාසි):
    ○ AWS සතුව ලොව පුරා ලක්ෂ සංඛ්‍යාත පාරිභෝගිකයන් සිටින බැවින්, විශාල පරිමාණයෙන් යටිතල පහසුකම් මිලදී ගැනීමේදී ලැබෙන පිරිවැය ඉතිරිය (Cost savings) අඩු භාවිත ගාස්තු ලෙස පාරිභෝගිකයන්ට ලබාදෙයි.
    ○ උදාහරණය: තනි ආයතනයක් සර්වර් තනිව නඩත්තු කිරීමට යන අධික පිරිවැයට වඩා, AWS වෙතින් "Pay-as-you-go" (භාවිතයට පමණක් ගෙවීම) පදනම මත සේවාව ලබාගැනීම ඉතා ලාභදායී වේ.

1.2 AWS Well-Architected Framework හි නිර්මාණ මූලධර්ම (Design Principles)

වලාකුළු පද්ධතියක් ආරක්ෂිතව, ස්ථාවරව සහ කාර්යක්ෂමව නිර්මාණය කිරීම සඳහා Well-Architected Framework හි ප්‍රධාන කුළුණු 6 ක් (6 Pillars) සහ සාමාන්‍ය නිර්මාණ මූලධර්ම භාවිතා වේ:

ප්‍රධාන කුළුණු 6 (6 Pillars):

1. Operational Excellence (ක්රියාකාරී විශිෂ්ටත්වය): පද්ධති නිවැරදිව පවත්වාගෙන යාම, නිරීක්ෂණය (observability) සහ නිරන්තරයෙන් ක්‍රියාවලි වැඩිදියුණු කිරීම. (උදා: Infrastructure as Code භාවිතයෙන් automatisations සිදුකිරීම)
2. Security (ආරක්ෂාව): දත්ත, පද්ධති සහ සම්පත් ආරක්ෂා කිරීම, Identity Management (IAM) සහ Encryption භාවිතය. (උදා: Data at rest සහ in transit encrypt කිරීම)
3. Reliability (විශ්වාසනීයත්වය): පද්ධතියක් බාධාවකින් තොරව ක්‍රියා කිරීම සහ බිඳවැටීමකින් ස්වයංක්‍රීයව යථා තත්ත්වයට පත්වීම (Automatic recovery). (උදා: සර්වර් අක්‍රිය වූ විට Auto Scaling මගින් අලුත් සර්වර් ස්වයංක්‍රීයව ඇරඹීම)
4. Performance Efficiency (කාර්යසාධන කාර්යක්ෂමතාව): Compute සහ Database සම්පත් කාර්යක්ෂමව භාවිතා කිරීම සහ Serverless වැනි අලුත් තාක්ෂණයන් යොදාගැනීම. (උදා: AWS Lambda වැනි Serverless සේවා භාවිතය)

5. Cost Optimization (පිරිවැය ප්‍රශස්තකරණය): අවම පිරිවැයකින් උපරිම ව්‍යාපාරික අගයක් ලබාගැනීම සහ අපතේ යන සම්පත් අවම කිරීම. (උදා: වැඩ නොකරන සතිඅන්තයේ Dev/Test සර්වර් Stop කර තැබීම)
6. Sustainability (තිරසාරබව): පරිසරයට සිදුවන බලපෑම සහ බලශක්ති අවම කිරීම. (උදා: Rightsizing මගින් අනවශ්‍ය සර්වර් ප්‍රමාණය අඩු කිරීම)

සාමාන්‍ය නිර්මාණ මූලධර්ම (General Design Principles):

- Stop guessing your capacity needs: ධාරිතාව ගැන අනුමාන නොකර අවශ්‍ය ප්‍රමාණයට පමණක් Auto Scaling භාවිතය.
- Test systems at production scale: On-premises මෙන් නොව, Cloud හිදී තාවකාලිකව Production-level පරිසරයක් සාදා පරීක්ෂා කර නැවත Delete කළ හැක.
- Automate to make architectural experimentation easier: ස්වයංක්‍රීයකරණය මගින් වෙනස්කම් පහසුවෙන් සිදුකිරීම.
- Consider evolutionary architectures: කාලයත් සමග පද්ධති යාවත්කාලීන වන පරිදි නම්‍යශීලීව තැබීම.
- Drive architectures using data: දත්ත පදනම් කරගෙන තීරණ ගැනීම.
- Improve through game days: පද්ධති බිඳවැටීම් කෘතිමව නිර්මාණය කර (Game Days) පුහුණු වීම.

1.3 AWS Cloud වෙත සංක්‍රමණය වීම (Cloud Migration Strategies)

ආයතනයක දැනට පවතින On-premises පද්ධති AWS Cloud වෙත ගෙන යාමේදී AWS Cloud Adoption Framework (AWS CAF) සහ විවිධ සංක්‍රමණ උපායමාර්ග (Migration Strategies) භාවිතා කරයි.

- AWS Cloud Adoption Framework (AWS CAF) හි වාසි:
    - ව්‍යාපාරික අවදානම් අඩු කිරීම (Reduced business risk), ESG කාර්යසාධනය වැඩිදියුණු කිරීම, ආදායම වැඩි කිරීම සහ ක්‍රියාකාරී කාර්යක්ෂමතාව ඉහළ නැංවීම.
- සංක්‍රමණ මෙවලම් සහ උපායමාර්ග (Migration Tools & Strategies):
    - AWS Snowball: Petabyte ගණනක විශාල දත්ත ප්‍රමාණයක් අන්තර්ජාලය හරහා යැවීම අපහසු විට, භෞතික ආරක්ෂිත Hardware සාධනයක් (Snowball device) මගින් AWS වෙත දත්ත සංක්‍රමණය කිරීම.

- Database Replication: On-premises Database එකක් බාධාවකින් තොරව AWS Cloud Database (RDS) වෙත සජීවීව පිටපත් (replicate) කිරීම.

1.4 Cloud Economics (වලාකුළු ආර්ථික විද්‍යාව)

Cloud භාවිතයේදී පිරිවැය කළමනාකරණය වන ආකාරය පිළිබඳ මූලයමය සංකල්ප මෙහිදී සාකච්ඡා කෙරේ:

- Fixed Costs vs. Variable Costs:
    - Fixed Costs (CapEx - Capital Expenditure): සාම්ප්‍රදායික IT හිදී සර්වර්, දත්ත මධ්‍යස්ථාන ගොඩනැගිලි සහ විදුලිය සඳහා පෙරලා විශාල මුදලක් ආයෝජනය කිරීමට සිදුවේ.
    - Variable Costs (OpEx - Operational Expenditure): AWS හිදී ඔබ භාවිතා කරන ප්‍රමාණයට සහ වේලාවට පමණක් ගෙවනු ලබයි (Pay-as-you-go).
- Rightsizing (නිවැරදි ප්‍රමාණය තේරීම):
    - Application එකට සැබවින්ම අවශ්‍ය වන CPU, Memory ප්‍රමාණයට හරියටම ගැලපෙන සර්වර් ප්‍රමාණය තෝරාගැනීම මගින් මුදල් අපතේ යාම වැළැක්වීම.
    - උදාහරණය: GB 4 RAM එකක් ප්‍රමාණවත් App එකකට GB 32 RAM සර්වර් එකක් නොගෙන, GB 4 සර්වර් එකක් තෝරා ගැනීම.
- Licensing Strategies (බලපත්‍ර උපායමාර්ග):
    - Bring Your Own License (BYOL): ආයතනය සතුව දැනටමත් පවතින Software Licences (උදා: Windows Server / SQL Server) AWS වෙත රැගෙන යාම.
    - License Included: AWS වෙතින්ම License එක සහිතව සේවාවන් ලබාගැනීම.
- Automation & Managed Services:
    - AWS CloudFormation: Infrastructure as Code මගින් සර්වර් සැකසීම ස්වයංක්‍රීය කර කාලය හා පිරිවැය ඉතිරි කිරීම.
    - Managed Services (Amazon RDS, ECS, EKS, DynamoDB): සර්වර් Patch කිරීම, Backup ගැනීම වැනි සංකීර්ණ වැඩ කොටස් AWS විසින් සිදුකරන බැවින් ආයතනයේ නඩත්තු පිරිවැය (Operational burden) අවම වේ.

Domain 2: Security and Compliance (ආරක්ෂාව සහ අනුකූලතාව)

2.1 AWS Shared Responsibility Model (බෙදාගත් වගකීම් ආකෘතිය)

AWS Cloud පරිසරයක ආරක්ෂාව යනු AWS සහ පාරිභෝගිකයා (Customer) අතර බෙදී යන හවුල් වගකීමකි. මෙය ප්‍රධාන කොටස් දෙකකට බෙදා දැක්විය හැක:

- AWS හි වගකීම් — "Security OF the Cloud":
    - AWS විසින් Cloud සේවාවන් පවත්වාගෙන යන සමස්ත යටිතල පහසුකම්වල (Infrastructure) ආරක්ෂාව තහවුරු කරයි. මීට භෞතික දත්ත මධ්‍යස්ථාන (Data Centers), සර්වර් Hardware, Software, Host Operating Systems, Virtualization Layer (Hypervisor) සහ ජාලකරණය (Networking) ඇතුළත් වේ.
    - උදාහරණය: දත්ත මධ්‍යස්ථාන වෙත අනවසර පුද්ගලයන් ඇතුළුවීම වැළැක්වීම සඳහා ජෛවමිතිය (Biometric scanning) සහ ආරක්ෂක නිලධාරීන් යෙදවීම, අක්‍රිය වන භෞතික Hard Drives ආරක්ෂිතව විනාශ කිරීම, සහ Physical Server Hardware හා Hypervisors යාවත්කාලීන (Patch) කිරීම AWS මගින් සිදුකරයි.
- පාරිභෝගිකයාගේ වගකීම් — "Security IN the Cloud":
    - Cloud පරිසරය තුළ පාරිභෝගිකයා විසින් ගබඩා කරන දත්ත (Customer Data), භාවිතා කරන යෙදවුම් (Applications), සකසන Identity & Access Management (IAM) අවසර, Security Group ෆයර්වෝල් නීති සහ Guest Operating System (EC2 මත දමන OS) ආරක්ෂා කිරීම පාරිභෝගිකයාගේ වගකීමයි.
    - උදාහරණය: Amazon EC2 instance එකක් තුළ Windows/Linux OS එකක් ස්ථාපනය කර ඇත්නම්, එහි Security Patches යාවත්කාලීන කිරීම, දත්ත Encrypt කිරීම, සහ සුදුසු පරිශීලක මුරපද (Passwords) පැනවීම පාරිභෝගිකයා විසින් කළ යුතුය.

(සටහන: Amazon RDS, AWS Lambda වැනි Managed Services භාවිතයේදී AWS විසින් OS Patch කිරීම වැනි වැඩි වගකීම් ප්‍රමාණයක් භාර ගන්නා බැවින් පාරිභෝගිකයාගේ වගකීම තවත් අඩුවේ).

2.2 AWS Security, Governance, සහ Compliance සංකල්ප

- AWS Artifact:
  - AWS හි අනුකූලතා වාර්තා (Compliance reports - උදා: SOC, PCI-DSS, ISO) සහ ආරක්ෂක ගිවිසුම් (Agreements) නොමිලේ ලබාගත හැකි Self-service Portal එකකි.
  - උදාහරණය: මූල්‍ය හෝ බැංකු ක්ෂේත්‍රයේ ආයතනයක් AWS භාවිත කරන විට, රාජ්‍ය හෝ ජාත්‍යන්තර විගණකවරුන්ට (Auditors) පෙන්වීමට අවශ්‍ය PCI-DSS audit report එක AWS Artifact හරහා පහසුවෙන් බාගත (Download) කරගත හැක.
- AWS CloudWatch:
  - AWS පද්ධතිවල කාර්යසාධන දත්ත (Performance metrics) සහ Logs නිරීක්ෂණය (Monitoring) කරන අතර, යම් සීමාවක් ඉක්මවූ විට දැනුම්දීම් (Alarms) නිකුත් කරයි.
  - උදාහරණය: EC2 සර්වර් එකක CPU භාවිතය 85% ඉක්මවූ විට පද්ධති පාලකට Email පණිවිඩයක් යැවීමට හෝ Autoscaling සක්‍රිය කිරීමට CloudWatch Alarm එකක් යෙදිය හැක.
- AWS CloudTrail:
  - AWS ගිණුම තුළ සිදුවන සියලුම API ඇමතුම් (API calls) සහ පරිශීලක ක්‍රියාකාරකම් පිළිබඳ විගණන වාර්තා (Auditing and Event history logs) සටහන් කර ගනී.
  - උදාහරණය: මධ්‍යම රාත්‍රියේ යම් පරිශීලකයෙකු විසින් Amazon S3 Bucket එකක් හෝ Database එකක් Delete කළහොත්, "කුමන පරිශීලකයා විසින්, කුමන වේලාවක, කුමන IP ලිපිනයෙන්" එය සිදුකළේද යන්න CloudTrail logs හරහා සොයාගත හැක.
- AWS Config:
  - AWS සම්පත්වල සැකසුම් වෙනස්වීම් (Configuration history) නිරන්තරයෙන් පරීක්ෂා කරමින් අනුකූලතා නීති (Compliance rules) රකිනවාදැයි නිරීක්ෂණය කරයි.
  - උදාහරණය: යම් සංවර්ධකයෙකු විසින් S3 Bucket එකක Public Access සක්‍රිය කළහොත්, AWS Config rule එකක් මගින් එය නීති විරෝධී (non-compliant) ලෙස හඳුනාගෙන ස්වයංක්‍රීයව නැවත Private තත්ත්වයට පත් කළ හැක (Auto-remediation).

- Encryption ක්‍රම (දත්ත කේතනය කිරීම):
    - Encryption at Rest: ගබඩා කර ඇති දත්ත (S3, EBS volumes, RDS Databases) ආරක්ෂිතව Encrypt කර තැබීම. *(උදා: S3 Bucket එකක තබන ගොනු AWS KMS යතුරු භාවිතයෙන් Encrypt කිරීම).*
    - Encryption in Transit: අන්තර්ජාලය හෝ ජාලය හරහා ගමන් කරන දත්ත ආරක්ෂා කිරීම. *(උදා: Web Browser එක සහ AWS Server එක අතර දත්ත HTTPS/TLS හරහා Encrypt කර හුවමාරු කිරීම).*

2.3 Access Management (පිවිසුම් කළමනාකරණය)

- AWS Identity and Access Management (IAM):
    - AWS සේවාවන් සහ සම්පත් වෙත පිවිසීමට අවසර (Authentication & Authorization) සපයන මධ්‍යම පද්ධතියයි. පරිශීලකයන් (Users), සමූහ (Groups), භූමිකා (Roles) සහ ප්‍රතිපත්ති (Policies) හරහා අවසර පාලනය කරයි.
    - උදාහරණය: ආයතනයක මෘදුකාංග ඉංජිනේරුවෙකුට S3 Buckets බැලීමට පමණක් අවසර දී, Billing හෝ වෙනත් සම්පත් වෙනස් කිරීමට ඇති අවසර අත්හිටුවීම.
- Root Account ආරක්ෂා කිරීම (Protecting AWS Root User):
    - AWS ගිණුම සෑදීමේදී නිර්මාණය වන, සියලුම සම්පත් සඳහා පූර්ණ පාලන බලතල සහිත ප්‍රධාන පරිශීලකයා Root User වේ.
    - ආරක්ෂා කිරීමේ පියවර: Root User සඳහා අන්තර්ජාල ප්‍රවේශ යතුරු (Access keys) නොසෑදීම/මකා දැමීම, අනිවාර්යයෙන් MFA යෙදීම, සහ දෛනික පාලන කටයුතු සඳහා Root Account එක වෙනුවට IAM Users/Roles භාවිත කිරීම.
- Least Privilege මූලධර්මය (Principle of Least Privilege):
    - පරිශීලකයෙකුට හෝ පද්ධතියකට තම නිශ්චිත කාර්යය ඉටුකිරීමට අවශ්‍ය අවම අවසර ප්‍රමාණය (Minimum required permissions) පමණක් ලබාදීමේ ආරක්ෂක මූලධර්මයයි.
    - උදාහරණය: දත්ත සමුදායක් (Database) කියවීමට පමණක් අවශ්‍ය සේවකයෙකුට 'Read-Only' අවසර පමණක් ලබාදී, දත්ත Delete කිරීමට හෝ වෙනස් කිරීමට ඇති අවසර නොදීම.

- Multi-Factor Authentication (MFA):
    - ගිණුමට ප්‍රවේශ වීමේදී මුරපදයට (Password) අමතරව දෙවන ආරක්ෂක පියවරක් (OTP code) ඇතුළත් කිරීමට සැලැස්වීම.
    - උදාහරණය: AWS Console එකට Login වීමේදී Username/Password ඇතුළත් කළ පසු, ජංගම දුරකථනයේ ඇති Authenticator App එකෙන් ලැබෙන අංක 6 ක සංකේතය ඇතුළත් කිරීමට සිදුවීම.

2.4 ජාල හා පද්ධති ආරක්ෂණ මෙවලම් (Network Security Tools)

- Security Groups:
    - EC2 Instances (Virtual Machines) සඳහා ලබාදී ඇති Stateful Virtual Firewall එකකි. Inbound (ඇතුළුවන) සහ Outbound (පිටවන) Network traffic පාලනය කරයි.
    - උදාහරණය: Web Server එකකට Port 443 (HTTPS) හරහා පමණක් Traffic ඇතුළු වීමට ඉඩ දී අන් සියලු Ports බ්ලොක් කර තැබීම.
- Network ACLs (Network Access Control Lists):
    - Subnet මට්ටමේ පවතින Stateless Firewall එකකි. ඇතුළුවන සහ පිටවන Traffic සඳහා Allow මෙන්ම පැහැදිලි Deny Rules යෙදිය හැක.
    - උදාහරණය: යම් කිසි හානිකර IP ලිපිනයකින් (Malicious IP) එන සියලුම ඉල්ලීම් Subnet එකට ඇතුළු වීමට පෙර NACL එකක් මගින් Deny කර සම්පූර්ණයෙන්ම බ්ලොක් කිරීම.
- AWS WAF (Web Application Firewall):
    - Web Applications වෙත පැමිණෙන HTTP/HTTPS ඉල්ලීම් පරීක්ෂා කර, SQL Injection සහ Cross-Site Scripting (XSS) වැනි වෙබ් ප්‍රහාරවලින් ආරක්ෂා කරයි.
    - උදාහරණය: අන්තර්ජාල ප්‍රහාරකයෙකු වෙබ් අඩවියේ පෝරමයක් (Form) හරහා හානිකර SQL කේත යැවීමට උත්සාහ කරන විට AWS WAF මගින් එම Request එක හඳුනාගෙන බ්ලොක් කිරීම.
- AWS Shield:
    - DDoS (Distributed Denial of Service) ප්‍රහාරවලින් පද්ධති සහ යෙදවුම් ආරක්ෂා කරන සේවාවකි. AWS Shield Standard (සියලුම

පාරිභෝගිකයන්ට නොමිලේ ලැබෙන) සහ AWS Shield Advanced ලෙස පවතී.
    - උදාහරණය: වෙබ් අඩවිය අක්‍රිය කිරීමේ අරමුණින් එකවර අධික Fake Traffic ප්‍රමාණයක් එවන විට, Shield මගින් එම ප්‍රහාරය ස්වයංක්‍රීයව සමනය (Mitigate) කර වෙබ් අඩවිය අඛණ්ඩව පවත්වාගෙන යාම.
- Amazon GuardDuty:
    - AWS ගිණුම තුළ සිදුවන අසාමාන්‍ය හෝ සැකකටයුතු ක්‍රියාකාරකම් (Malicious behavior & Threats) නිරන්තරයෙන් නිරීක්ෂණය කරන Intelligent Threat Detection සේවාවකි.
    - උදාහරණය: මීට පෙර කිසිදා භාවිත නොකළ වෙනත් රටක IP ලිපිනයකින් Root User Account එකට Login වීමට උත්සාහ කිරීමක් හෝ EC2 Instance එකක් අනිසි ලෙස Cryptocurrency mining සඳහා යොදාගන්නා බව හඳුනාගෙන Alerts නිකුත් කිරීම.

Domain 3: Cloud Technology and Services (තාක්ෂණය සහ සේවාවන්)

3.1 AWS භාවිතය සහ යෙදවුම් ක්‍රම (Deployment and Operation)

AWS සේවාවන් සමග සම්බන්ධ වීමට සහ Cloud යටිතල පහසුකම් පාලනය කිරීමට ප්‍රධාන ක්‍රම කිහිපයක් භාවිතා කළ හැක:

- AWS Management Console (වෙබ් අතුරුමුහුණත):
    - Graphic User Interface (GUI) එකක් හරහා Web Browser එකකින් AWS සේවාවන් පහසුවෙන් පාලනය කිරීමේ ක්‍රමයයි.
    - උදාහරණය: ආරම්භකයෙකු විසින් බ්‍රවුසරය හරහා AWS Console එකට Login වී, බොත්තම් ක්ලික් කරමින් (point-and-click) තත්පර කිහිපයකින් S3 Storage Bucket එකක් සෑදීම.
- AWS Command Line Interface (CLI):
    - Computer Terminal / Command Prompt එක හරහා Text Commands (විධාන) ටයිප් කරමින් AWS සේවාවන් පාලනය කිරීම.

    - උදාහරණය: System Administrator කෙනෙකු විසින් `aws ec2 describe-instances` ලෙස ටයිප් කර දැනට ධාවනය වන සියලුම Virtual Servers ලැයිස්තුව තත්පරයකින් ලබාගැනීම.
- AWS Software Development Kits (SDKs):
    - Python, Java, JavaScript වැනි Programming Languages මගින් සාදන Software Codes ඇතුළෙන්ම කෙළින්ම AWS සේවාවන් ඇමතීමට (APIs) භාවිතා කරන කට්ටල වේ.
    - උදාහරණය: Python කේතයක් (Boto3) මගින් පරිශීලකයෙකු Upload කරන පින්තූරයක් ස්වයංක්‍රීයව Amazon S3 වෙත යැවීම.
- Infrastructure as Code - IaC (AWS CloudFormation):
    - සර්වර්, ඩේටාබේස් සහ ජාලකරණයන් මැනුවලි නොසාදා, JSON හෝ YAML ගොනුවක (Template) කේත ලෙස ලියා ස්වයංක්‍රීයව සෑදීමේ ක්‍රමයයි.
    - උදාහරණය: CloudFormation Template එකක් ක්‍රියාත්මක කර තනි ක්ලික් කිරීමකින් Test, Staging, සහ Production යන පරිසරයන් තුනෙහිම සමාන සර්වර් සහ ජාල එකවර නිර්මාණය කිරීම.

3.2 AWS Global Infrastructure (ගෝලීය යටිතල පහසුකම්)

ලොව පුරා විසිරී ඇති AWS භෞතික යටිතල පහසුකම් ප්‍රධාන කොටස් 4 කට බෙදේ:

- Regions (කලාප):
    - ලෝකයේ විවිධ භූගෝලීය ප්‍රදේශවල පිහිටුවා ඇති මධ්‍යස්ථාන වේ. එක Region එකක් තුළ අවම වශයෙන් Availability Zones 3 ක් වත් පවතී.
    - උදාහරණය: `us-east-1` (N. Virginia) හෝ `eu-central-1` (Frankfurt) Region එක තෝරාගැනීම.
- Availability Zones - AZs (පවතින කලාප):
    - Region එකක් තුළ එකිනෙකින් කිලෝමීටර කිහිපයක් දුරින් පිහිටි, වෙනස්ම විදුලිය සහ ජාල සපයන භෞතික Data Center එකක් හෝ කිහිපයක එකතුවකි.

- උදාහරණය: එක Data Center එකකට ජල ගැලීමක් වුවද, අනෙක් AZ එකෙහි සර්වර් ක්‍රියාත්මක වන බැවින් App එක නොබිඳී පැවැතීම (High Availability).

- Edge Locations (මායිම් ස්ථාන):

  - Amazon CloudFront (CDN) හරහා පරිශීලකයන්ට ඉතා වේගයෙන් (Low Latency) දත්ත ලබාදීමට ලොව පුරා නගර රැසක පිහිටුවා ඇති Caching Servers වේ.
  - උදාහරණය: ශ්‍රී ලංකාවේ සිටින පරිශීලකයෙකු ඇමරිකාවේ සර්වර් එකක ඇති වීඩියෝවක් නරඹන විට, එය ළඟම ඇති Edge Location එකක Cache වී තත්පරයකින් Play වීම.

- Local Zones (ප්‍රදේශීය කලාප):

  - ප්‍රධාන AWS Region එකක් නොමැති විශාල ජනාකීර්ණ නගර ආසන්නයේ ඇති පරිශීලකයන්ට මිලිසෙකන්ඩ් ගණනක අතිශය අඩු Latency එකක් ලබාදීමට පිහිටුවා ඇති කුඩා Compute/Storage මධ්‍යස්ථාන වේ.
  - උදාහරණය: Los Angeles නගරයේ සිටින සජීවී ක්‍රීඩකයන්ට (Online Gaming / VR) තත්පරයෙන් සියයෙන් පංගුවක ප්‍රමාදයකින් තොරව සේවාව ලබාදීම.

3.3 ප්‍රධාන AWS සේවාවන් (Core AWS Services)

1. Compute Services (ගණනය කිරීම් සේවා)

- Amazon EC2 (Elastic Compute Cloud): අවම වියදමකින් අවශ්‍ය පරිදි සකස් කළ හැකි Virtual Machines (සර්වර්) වේ. *(උදා: Linux හෝ Windows OS එකක් සහිත Virtual Server එකක් මිනිත්තු 2 කින් ලබාගැනීම)*.
- AWS Lambda: Serverless සේවාවකි. සර්වර් කළමනාකරණය නොකර කේතය (Code) පමණක් Upload කර ක්‍රියාත්මක කිරීම. *(උදා: පරිශීලකයෙකු Photo එකක් දැමූ විට එය Resize කිරීමට පමණක් Lambda Code එක run වීම)*.
- Amazon ECS & Amazon EKS: Containers (Docker/Kubernetes) පහසුවෙන් පාලනය කරන සේවා වේ. *(උදා: Microservices ලෙස තනන ලද ඇප් එකක ඩොකර් කන්ටේනර් සිය ගණනක් කළමනාකරණය කිරීම)*.
- AWS Fargate: ECS හෝ EKS සඳහා සර්වර් නඩත්තු නොකර Containers run කරවන Serverless Compute Engine එකකි.

- AWS Auto Scaling: පරිශීලක ඉල්ලුම අනුව EC2 instances ප්‍රමාණය ස්වයංක්‍රියව වැඩි හෝ අඩු කිරීම. *(උදා: රාත්‍රී කාලයේදී සර්වර් 2 ක්ද, දහවල් කාලයේදී සර්වර් 10 ක්ද ස්වයංක්‍රියව පවත්වා ගැනීම)*.

2. Storage Services (ගබඩා සේවා)

- Amazon S3 (Simple Storage Service): Unlimited ප්‍රමාණයෙන් පින්තූර, වීඩියෝ සහ Files ගබඩා කළ හැකි Object Storage සේවාවකි. *(උදා: වෙබ් අඩවියේ User Upload කරන සියලුම PDF සහ Photos S3 Bucket එකක දැමීම)*.
- Amazon EBS (Elastic Block Store): EC2 Instance එකකට අමුණන Virtual Hard Drive (Block Storage) එකකි. *(උදා: EC2 Server එකෙහි OS එක සහ Database ගොනු රඳවන වේගවත් SSD ඩ්‍රයිව් එක)*.
- Amazon EFS (Elastic File System): EC2 සර්වර් කිහිපයකට එකවර සම්ප්‍රේෂණය කළ හැකි Shared Network File System එකකි. *(උදා: සර්වර් 5 කටම එකවර access කළ හැකි පොදු Folder එකක් තැබීම)*.
- S3 Glacier: නිතර ලබාගන්නේ නැති (Archival Data), වසර ගණනාවක් ආරක්ෂිතව අඩු මුදලට තබාගත යුතු දත්ත ගබඩාවකි. *(උදා: වසර 5 ක පැරණි බැංකු ගිණුම් වාර්තා)*.

3. Database Services (දත්ත සමුදා සේවා)

- Amazon RDS (Relational Database Service): MySQL, PostgreSQL, Oracle, MS SQL වැනි ව්‍යුහගත (Relational) Databases පහසුවෙන් නඩත්තු කරදෙන සේවාවයි. *(උදා: පාරිභෝගික නාම සහ මුදල් ගනුදෙනු ලේඛන පවත්වාගෙන යාම)*.
- Amazon Aurora: AWS විසින් සාදන ලද, RDS වලට වඩා 5 ගුණයක් වේගවත් අධි-කාර්යක්ෂම Relational Database එකකි.
- Amazon DynamoDB: අතිශය වේගවත්, ස්වයංක්‍රීයව Scale වන NoSQL (Key-Value) Database සේවාවකි. *(උදා: Online Game එකක ලකුණු පුවරුව (Leaderboard) සහ පරිශීලක Sessions තැන්පත් කිරීම)*.

4. Networking Services (ජාලකරණ සේවා)

- Amazon VPC (Virtual Private Cloud): AWS Cloud එක තුළ ඔබටම වෙන්වූ ආරක්ෂිත හුදකලා අතථ්‍ය ජාලයක් (Isolated Virtual Network) සෑදීම. *(උදා: ආයතනයේ Private සර්වර් පිටතට නොපෙනෙන සේ VPC එකක් තුළ හුදකලා කිරීම)*.

- Amazon Route 53: AWS හි පැමිණෙන Cloud Domain Name System (DNS) සහ Domain Registration සේවාවයි. *(උදා: `example.com` ලෙස ටයිප් කරන විට එය අදාළ IP ලිපිනයට යොමු කිරීම)*.
- AWS Direct Connect: On-premises Data Center එක සහ AWS අතර අන්තර්ජාලය හරහා නොගොස් වෙන්වූ අධිවේගී පුද්ගලික කේබල් සබඳතාවයක් (Dedicated Private Connection) ලබාදීම.
- AWS VPN: අන්තර්ජාලය හරහා ආරක්ෂිතව Encrypted මාර්ගයකින් On-premises ජාලය AWS VPC එක සමග සම්බන්ධ කිරීම.

5. AI/ML සහ Analytics (කෘතිම බුද්ධිය සහ දත්ත විශ්ලේෂණය)

- Amazon SageMaker: Machine Learning Models පහසුවෙන් සාදා, පුහුණු කර (Train), Deploy කිරීමට Developer ලාට සහ Data Scientist ලාට උපකාරී වන Platform එකකි.
- Amazon Lex: සිරි (Siri) හෝ ඇලෙක්සා (Alexa) මෙන් හඬ සහ Text මගින් වැඩ කළ හැකි Chatbots සෑදීමට ඇති AI සේවාවයි. *(උදා: බැංකු වෙබ් අඩවියකට ස්වයංක්‍රීය පාරිභෝගික සහායක Chatbot කෙනෙකු සෑදීම)*.
- Amazon Athena: Amazon S3 හි ඇති දත්ත වලට කෙළින්ම SQL Queries ගසා දත්ත විශ්ලේෂණය කිරීමේ Serverless සේවාවයි.
- AWS Glue: විවිධ ස්ථානවල ඇති දත්ත එකතු කර, සුද්ධ කර, පරිවර්තනය කරන (Extract, Transform, Load - ETL) සේවාවයි.
- Amazon QuickSight: විශ්ලේෂණය කළ දත්ත මගින් අලංකාර ප්‍රස්ථාර සහ Dashboards (Business Intelligence) සාදන සේවාවයි.

Domain 4: Billing, Pricing, and Support (ගාස්තු, මිලගණන් සහ සහාය)

4.1 AWS මිලකරණ ආකෘති (Pricing Models)

AWS හි Compute සම්පත් (සර්වර්) ලබාගැනීමේදී ව්‍යාපාරික අවශ්‍යතාවය සහ පිරිවැය අනුව තෝරාගත හැකි ප්‍රධාන මිලකරණ ක්‍රමවේද 4 ක් පවතී:

- On-Demand Instances:
  - විස්තරය: කිසිදු දිගුකාලීන ගිවිසුමක් හෝ පෙර ගෙවීමක් නොමැතිව, සර්වර් භාවිත කරන වේලාවට (පැයට හෝ තත්පරයට) පමණක් ගෙවීමේ ක්‍රමයයි.

    - උදාහරණය: හදිසියේම දින 3 කට පමණක් පවත්වන පරීක්ෂණයකට (Short-term test/dev) සර්වර් එකක් ලබාගෙන, වැඩ අවසන් වූ පසු Stop/Delete කර භාවිත කළ පැය ගණනට පමණක් ගෙවීම.
- Reserved Instances (RI):
    - විස්තරය: වසර 1 ක් හෝ වසර 3 ක කාලයකට අඛණ්ඩව භාවිත කිරීමට ගිවිසුම්ගත වීම මගින් On-Demand මිලට වඩා 75% දක්වා අධික පිරිවැය ඉතිරියක් (Discount) ලබාගත හැක.
    - උදාහරණය: දවසේ පැය 24 පුරාම, වසර පුරාම අඛණ්ඩව ක්‍රියාත්මක වන ආයතනයේ ප්‍රධාන Database සර්වර් එක සඳහා වසර 3 ක කාලයකට Reserved Instance එකක් තෝරාගැනීම.
- Spot Instances:
    - විස්තරය: AWS සතුව පවතින භාවිත නොකළ (Unused) අතිරික්ත සර්වර් ධාරිතාව 90% දක්වා විශාල වට්ටමකට ලබාදෙන ක්‍රමයයි. නමුත් AWS වෙත වෙනත් පාරිභෝගිකයෙකුගෙන් ඉල්ලුමක් ආවොත්, විනාඩි 2 ක පූර්ව දැනුම්දීමකින් පසු මෙම සර්වර් එක නැවත ලබාගනු ලැබේ.
    - උදාහරණය: සර්වර් එක මැදදී නතර වුවද බාධාවක් නැති, ඕනෑම වේලාවක නැවත ආරම්භ කළ හැකි Big Data Analysis, Batch Processing, හෝ Video Rendering වැනි කටයුතු සඳහා භාවිත කිරීම.
- Savings Plans:
    - විස්තරය: වසර 1 කට හෝ 3 කට නිශ්චිත Compute ගාස්තුවක් (උදා: පැයකට $10 ක්) ගෙවීමට ගිවිසුම්ගත වීමෙන් ලැබෙන නම්‍යශීලී (Flexible) මිලකරණ ආකෘතියයි. EC2, AWS Lambda, සහ AWS Fargate සඳහා මෙය එකසේ අදාළ වේ.
    - උදාහරණය: අනාගතයේදී EC2 සර්වර් එකක OS එක හෝ Region එක වෙනස් කළද, 72% දක්වා වන පිරිවැය වට්ටම අඛණ්ඩව ලබාගැනීම.

4.2 පිරිවැය කළමනාකරණ මෙවලම් (Cost Management Tools)

- AWS Cost Explorer:
    - විස්තරය: පසුගිය කාලයේ සිදු වූ AWS වියදම් සහ භාවිතයන් ප්‍රස්ථාරිකව නිරීක්ෂණය කිරීමටත්, ඉදිරි මාසවල වියදම් කොපමණ විය හැකිදැයි අනාවැකි පලකිරීමටත් (Forecasting) ඇති මෙවලමයි.

    - උදාහරණය: පහුගිය මාස 3 තුළ EC2 සර්වර් සහ S3 Storage සඳහා වෙන් වෙන් වශයෙන් කොපමණ මුදලක් වැය වී ඇත්දැයි බලා, ඉදිරි මාසයේ වියදම ගණනය කරගැනීම.
- AWS Budgets:
    - විස්තරය: මාසිකව හෝ දිනපතා වියදම් කිරීමට අපේක්ෂිත සීමාවන් (Custom Budget Limits) සකසා, එම සීමාව ඉක්මවූ විට හෝ ඉක්මවීමට ආසන්න වන විට (Forecasted) Alerts ලබාදෙන සේවාවයි.
    - උදාහරණය: මාසයකට AWS සඳහා $1000 ක Budget එකක් තබා, වියදම $800 (80%) පසුකරන විට පද්ධති පාලකට Email එකක් මගින් දැනුම්දීම.
- AWS Cost and Usage Report (CUR):
    - විස්තරය: AWS හි සියලුම සේවාවල භාවිතය සහ වියදම් පිළිබඳ අතිශය සවිස්තරාත්මක වාර්තා (Hourly / Daily granularity) ලබාදෙන මූලාශ්‍රයයි.
    - උදාහරණය: Amazon Athena හෝ QuickSight සමග CUR සම්බන්ධ කරමින් ආයතනයේ එක එක Department එක අනුව වියදම් වෙන වෙනම පෙන්වන Dashboards සෑදීම.
- AWS Free Tier කොන්දේසි:
    - විස්තරය: නව පාරිභෝගිකයන්ට AWS සේවාවන් නොමිලේ/අඩු පිරිවැයකින් අත්හදා බැලීමට පහසුකම් සපයයි.
    - කොන්දේසි/වර්ග: Always Free (සමහර සේවා සදාකාලිකවම යම් සීමාවකට නොමිලේ), 12-Month Free (ගිණුම සාදා මුල් මාස 12 තුළ නොමිලේ), සහ Short-term Trials. එසේම නවක පාරිභෝගිකයන්ට Sign-up වීමේදී $100 ක Credits ද, නියමිත අධ්‍යාපනික ක්‍රියාකාරකම් සම්පූර්ණ කිරීමෙන් තවත් $100 ක් ලෙස මුළු $200 දක්වා Credits ලබාගත හැක.

4.3 තාක්ෂණික සහාය සහ සම්පත් (Technical Resources & Support Options)

- AWS Support Plans (තාක්ෂණික සහාය සැලසුම්): AWS විසින් පාරිභෝගික අවශ්‍යතා අනුව වෙනස් වන Support Plans ලබාදෙයි:
    - Developer Support: පරීක්ෂණ සහ සංවර්ධන කටයුතු (Non-production environments) කරන අයට ගැලපේ. වැඩකරන වේලාවන් තුළ (Business hours) Email හරහා සහාය ලැබේ.
    - Business Support: Production මට්ටමේ යෙදවුම් පවත්වාගෙන යන ආයතන සඳහා ගැලපේ. 24/7 Phone, Chat, සහ Email හරහා පැයකට අඩු කාලයකින් (1-hour response) සේවාව ලැබේ.

    - Enterprise Support: විශාල ව්‍යාපාර සහ Mission-critical පද්ධති සඳහා ගැලපේ. කැපවූ Technical Account Manager (TAM) කෙනෙකු ලැබෙන අතර, විනාඩි 15 කින් (15-min response time) ඉතා කඩිනම් සහාය ලැබේ.
- AWS Trusted Advisor:
    - විස්තරය: AWS පද්ධතිවල ආරක්ෂාව (Security), කාර්යසාධනය (Performance), පිරිවැය ප්‍රශස්තකරණය (Cost Optimization), සහ සේවා සීමාවන් (Service Limits) පිළිබඳ ස්වයංක්‍රීය පරීක්ෂාවන් (Automated checks) සිදුකර උපදෙස් දෙන මෙවලමයි.
    - උදාහරණය: භාවිතයට නොගෙන නිකරුණේ පවතින (Idle) EC2 Instances හෝ EBS Volumes හඳුනාගෙන ඒවා Stop කර මුදල් ඉතිරි කරගන්නා ලෙස පෙන්වා දීම.
- AWS Partner Network (APN):
    - විස්තරය: AWS තාක්ෂණය පදනම් කරගෙන මෘදුකාංග (ISVs) සපයන සහ සංකීර්ණ Cloud පද්ධති නිර්මාණය කරදෙන (System Integrators) බලපත්‍රලත් තෙවන පාර්ශවීය ආයතනවල එකතුවයි.
    - උදාහරණය: ආයතනයකට තනිව Cloud Migration එකක් සිදුකර ගැනීමට තාක්ෂණික දැනුම මදි වූ විට, APN Certified Partner ආයතනයක උපදෙස් සහ සහාය ලබාගැනීම.

Shashika Wijerathna

CyberSecurity

Winsys City Campus