

- 1) EBS Volumes never encrypted on default. We can also encrypt using **native data encryption** at **file system level**.
- 2) Best way to scale a solution to intrusion detection is install an agent and send it to **IDS/IPS**.
- 3) S3 encryption at rest: A) SSE - Customer provided keys B) SSE - KMS: **Data key** is managed by **KMS** and we manage the **CMK** C) **Pehle hi encrypt** D) SSE - S3 Managed keys.
- 4) Kinesis to collect data. Analyze using Kinesis **Clients** and Save to Redshift with EMR. Elastic and Parallel always -> EMR
- 5) Always prefer to assign a CNAME record to ELB DNS Name. **Never A Record. Place all web servers behind the ELB and use Route 53 to point to the ELB DNS Name**
- 6) Always a better option to create RDS Instances as part of the Beanstalk and alter it's security group to allow access from hosts in the application subnets. **Separate** is not a good option.
- 7) To quickly adapt applications hosted on-premise, create a CloudFront Distribution to **cache objects from a custom origin**. Select TTL for which objects should exist in cache.
- 8) Create a **public interface** on AWS Direct Connect link. Redistribute BGP and advertise specific routes to the network to AWS.
- 9) Memcached Clusters need to be deployed in different AZ architecture to support extra load.
- 10) AWS Import/Export is a storage service.
- 11) Direct Connect -> BGP, public, internet gateway. Propagate specific routes for on-premises.
- 12) The standard EBS **Instance root volume** limits the total IOPS rate. Change the root volume to be the 500GB, 4000 IOPS.
- 13) HDFS -> encrypted in transit and at rest. Concurrently -> EMR. Use in-memory instead of ephemeral.
- 14) Kinesis best for analyzing anything in **real-time**. Moreover, the retention period is 24 hours - 7 Days.
- 15) Cloudsearch for query processing and Beanstalk to host is a good option.
- 16) Stored mode, data is stored locally. Storage Gateway, give iSCSI, Posix-compliant file system.
- 17) SWF with an auto scaling group of workers and deciders in separate ones. SES reliable email

- 18) Better to scale depending on SQS queue length.
- 19) Introduce SQS and ElastiCache to reduce provisioned read and write throughput..
- 20) CloudTrail trail and store in s3 with **global services option** selected.
- 21) RRS for reproducible data. RRS for pdf and csv files. EMR -> Spot.
- 22) **CPU idle -> We need higher aggregate I/O performance.**
- 23) Multi-AZ always for availability.
- 24) **RDS automated Backups.** For entire disk restores, better to go for **AMI's** instead of EBS Snapshots, which will only capture the data stored in the instances.
- 25) EBS backed AMI. Create a CloudFormation Template of AMI, EC2 and asynchronous replicate transactions using a VPN connection.

PDF 30-50)

- 1)

PDF- 50:

- 1) IPSec: Data Integrity protection, Protection of data in transit over the internet, data encryption across the internet, peer identity authentication between vpn gateway and customer gateway. Nothing **End-End**
- 2) Arn for IAM: arn:aws:iam::123456789012:instance-profile/Webserver.
- 3) arn:aws:service:region:account:resource
- 4) Create RDS Read Replica for the batch analysis.
- 5) Launching RDS Read Replica in Multi-AZ and query it for reporting.
- 6) Configure Web proxy server in the VPC and enforce URL-based rules for outbound access.
- 7) Always IAM Roles for talking between EC2 and S3 or any other services.
- 8) Best hai database backed DB Snapshots and storing read-only in s3, even if shared with a network file system.
- 9) For a large amount of undetermined writes, use SQS to store and capture the writes.
- 10) Always add a route from App and Database tier to NAT Instance. NAT in public.
- 11) SAML IDP gives you temporary security credentials for signing-in using Console.

- 12) IP-Level blocking through NACL.
- 13) Beanstalk **Rebuild Environment** to update log delivery to the EMR Job.
- 14) Allow no inbound and all allow all outbound. Instances with this SG can talk to each other.
- 15) Need to disable the Source/Destination checks on the NAT instance to connect to the internet.
- 16) Customer is responsible for patch management of EC2 OS and **controlling physical access** to compute resources, IAM Life-cycle policies.
- 17) No Charge for using public datasets.
- 18) CloudWatch to terminate instances when utilization is below 5%.
- 19) DynamoDB can scale without limits and need contact support beyond 10000.
- 20) ApplyImmediately to upgrade RDS immediately.
- 21) Elastic IP is unmapped and we have to remap when we restart. EC2-VPC remains associated.
- 22) Cognito push synchronization to notify all devices that new data is available.
- 23) Parent of the IAM user on the bucket is regardless when accessing a bucket in another root account.
- 24) VPN connection does not need Elastic IP ranges but instead needs internal network IP ranges. Needs an Internet-routable IP address of the customer gateway's external interface.
- 25) Passwords can have **any** Basic Latin(ASCII) **characters**.
- 26) Subnet access is allowed for each IAM user for separate zone access of the users.
- 27) Determine port speed when we submit AWS DC Connection Request.
- 28) Need to assign separate Elastic IP and Security Group to each interface. AWS public IP is not an option.
- 29) Unlimited users can open technical support under Enterprise and Premium support plans.
- 30) aws:SourceIP
- 31) PIOPS -> **optimized EBS** volumes and **optimized configuration** stacks.
- 32) **Enhanced** and **Basic** flows for Amazon Cognito.
- 33) ELB can support **only 1 subnet** in each AZ.

- 34) Secure access to DB -> Use **subnet groups**. Each subnet group must have subnets within 2 AZ's within a region.
- 35) AWS Data Pipeline -> when resources have completed successfully or failed they terminate.
- 36) Can't assign private IP because it may have been assigned to another interface in the VPC.
- 37) Check bandwidth, instance type and bandwidth of dedicated instance exceeds PIOPS more than provisioned. Volume size is never a factor.
- 38) Multiple cluster objects in the definition file and associating the cluster to use via the runs on-Field.
- 39) **VPN Cloudhub** provides a simple hub and spoke model that can be used with or without a VPC. Multiple branch offices for remote connectivity.
- 40) We can increase automatic retries to 10 in AWS Data Pipeline. Will fail after 3 failed attempts.
- 41) The CR1 family provides 244GB of RAM.
- 42) JSON written in IAM policy language.
- 43) Create an Internal Load Balancer and register all App Servers with it.
- 44) Redis is a key-value store.
- 45) Use elastic IP and map assign the same EIP to a new instance. ELB does not work in multi-region.
- 46) Use a bootstrapping script to register MAC of instance with the application.
- 47) We can modify DB instances and associate with Security Groups using RDS API
- 48) In ElastiCache, we can run a max of 20 Cache Nodes.
- 49) Pipeline Definition defines the business logic.
- 50) Session persistence allows service to be redirected to the same node as long as it is available.
- 51) Cognito supports **authenticated** and **unauthenticated** identities.
- 52) Temporary security credentials cannot be revoked.
- 53) aws-portal:ViewUsage
- 54)

## LinuxAcademy Test:

- 1) Subnets can only be shared within an Organization. To provide access -> 1) Create a **VPN** b/w VPC and Organization's network 2) Invite to Organization and then use RAM to share subnets.
- 2) To move from one organization to another: 1) **Remove** from org and make it standalone. Then invite into another organization.
- 3) Detailed billing and decomposition across multiple dimensions and aggregation levels: -> **Resource Tagging/ Billing Tags**
- 4) Max VPC's allowed in a **region** are 5.
- 5) Kibana for visualization along with Elasticsearch.
- 6) Web identity federation can be done using Cognito and STS. Federation needs management from a single account and assumes a role to move between accounts. Always try to federate into a single account and switch roles.
- 7) Always to change master account, we need to create a new org, new account and move accounts to the new organization to change master.
- 8) Jismein you need access, usmein create roles.
- 9) Configure DynamoDb with streams and use Lambda to trigger it based on activity.
- 10) Multiple bitrates -> Diff SQS queues to subscribe to SNS and worker instances inside ASG to poll the SQS Queue.
- 11) **Aurora** is ACID compliant and based on MySQL.
- 12) Best to decouple using SQS and Lambda as triggers.
- 13) Single ALB can **offload** SSL certificates using **1 listener** and have multiple active SSL certificates.
- 14) **With Direct Connect we need BGP to propagate specific routes**
- 15) ElastiCache with MySQL or SQL Server, DynamoDB and MongoDB
- 16) Kinesis Use case: 1) Real-Time 2) Persistence of results for data mining 3) Durable, elastic and parallel processing. Analyze data with Kinesis Clients.
- 17) Durable, persistent and accessible from all application servers. NFS to mount on Linux FS.
- 18) Advanced data-types and snapshots are available only in ElastiCache - Redis. In-memory cache. DAX is Dynamodb specific.

- 19) Ad Hoc requests to data using SQL type -> Athena
- 20) Kinesis Data Analytics -> ETL. s3 for raw through Firehose.
- 21) T3 instances -> designed for non-constant usage and cost savings. Use cloudwatch events and Lambda to control the EC2 instance power state.
- 22) Faster than size of data -> IOPS. Scale according to data -> GP2
- 23) Redis for horizontal scaling and multi-AZ.
- 24) We can only use CLI to copy the definitions of existing SG's and create new ones.
- 25) Create an IPSec VPN between on-premises routers and add a route of the subnet in the company router with a tunnel as the next hop.
- 26) Simple: Subnets cannot be stretched. Individual and isolated and use a load balancer.
- 27) Storage gateway best option and use SMB for Windows File Server.
- 28) API Gateway can be integrated with ECS and ALB to provide managed API Service for Docker based microservices.
- 29) Workspaces must point at AD Connector. As a POC, provision AD Connector in AWS and configure as appropriate and private connection via IPSec VPN.
- 30) Transfer acceleration -> transfer of data to S3.
- 31) 1 partition per 10GB. Take the maximum of WCU and RCU partitions.
- 32) DynamoDB charges per GB stored and it is cheaper to store data in s3 rather than DynamoDB
- 33) 1:1:1 configuration on the ASG ensures immediate auto-healing to another AZ if it fails.
- 34) EFS is resilient across AZ. If any instance fails, data is not at all affected.
- 35) Lambda with S3 static will allow for scaling showing it is dynamic rather than static.
- 36) DAX nly helps to offload DDB reads. For writes, decouple by using SQS.
- 37) Prefix lists added to the route table to simplify the configuration of security groups and route tables.
- 38) Unallocated EIPs and EBS volumes cost.
- 39) Enable Private DNS so that default endpoint points to interface endpoint. Still using the default endpoint.
- 40) Check 48
- 41) Launch Templates, Key Pairs and Elastic IP need to be replicated.
- 42) Move to your own DDB Table and allocate your own RCU to meet performance.

- 43) Add trusted signers and generate signed URLs for things that need protection.
- 44) Communication across Public VIF is encrypted because they are using AWS endpoints. VPN IPSec can be created over public VIF to provide encrypted communications.

### 100+ Dumps:

- 1) 5 IAM Users. Same Login ID, Diff Password: Not possible for same login ID.
- 2) Use an elastic network interface to maintain the same MAC, IP and other things. Can be attached and detached.
- 3) Instance Profile Name: 128 characters
- 4) PIOPS: 4GiB - 16TiB. 20000 IOPS per volume
- 5) IAM Policy evaluation is Logical OR.
- 6) IAM is not useful when we have to SSH/RDP.
- 7) RAID 10 best reliability and performance.
- 8) Connecting to a cluster endpoint is no different than connecting directly to an individual cache node. Sabka CNAME is maintained in the DNS
- 9) Disable source/destination check on NAT Instance. Uska ka kuch kaam nahi hai.
- 10) --show-long for listing IAM Role.
- 11) Only one role can be assigned to an EC2 Instance and all applications share the same role and permissions.
- 12) Does not compile the pipeline components to create a set of actionable instances.
- 13) Data Pipeline cannot generate reports.
- 14) No specific. Use (\*)
- 15) IfExists at the end of all operators except NULL
- 16) Must create subnet groups with public and private subnets.
- 17) Instance metadata and Elastic IP not at all related.
- 18) VPC Peering if one VPC want to connect to resources in another VPC
- 19) Direct connect is an alternative to the internet. Hence, cannot connect directly.

- 20) ElastiCache clusters can run in a VPC.
- 21) Dw2.8xlarge has 32 slices.
- 22) We don't have to manage credentials and worry about long-term security risks.
- 23) RAID 10 doubles the amount of I/O required, because we are mirroring all writes to a pair of volumes, limiting how much we can stripe.
- 24) `--source-type cache-cluster --duration 1440`
- 25) Numlreq
- 26) Task Runner package that can be installed on your on-premise host.
- 27) NotAction lets us specify an exception to a list of actions.
- 28) MultiFactorAuthAge
- 29) 100 GiB and 1000 PIOPS
- 30) We can't provide default TTL in Redis for different types of data.
- 31) Cache Security groups are not available inside a VPC.
- 32) Queue Length of 1 per 200 PIOPS.
- 33) Public Cloud pe nahi chahiye toh sidha host on-prem and do a VPN.
- 34) Max ratio of 30, 4-16 and 20000 per volume.
- 35) The nameidentifier cannot be the same as the username stored in AD. And the app requires a different set of claim URI's.
- 36) CloudHSM should have port 22 or port 3389 open to the network.
- 37) C4.8xlarge instance has 10 Gigabit networking performance.
- 38) 8xLarge is available only in multi-node configuration.
- 39) Yes. PIOPS can be used on all RDS instances in a VPC.
- 40) Configure BGP to create a Virtual Interface step.
- 41) Task Runner polls for tasks and then performs the tasks.
- 42) Code memory is only useful for performance checks and not leaks.
- 43) 11211 for Memcached and 6379 for Redis.



- 44) Cloudwatch cannot perform administrative tasks and manage Elasticache.
- 45) Cannot expose Sid in the IAM Api as it is an optional identifier. We can assign a Sid value to each statement in a statement array.
- 46) Cannot launch Elaticache in Dedicated Instance Tenancy.
- 47) Accountid.signin.aws.amazon.com/console
- 48) During CoolDown, other alarms have no effect on the ASG capacity.
- 49) New request only after both instances ka cooldown has passed.
- 50) Accept Binary as parameters:
- 51) **Desired Capacity:**
- 52) We can send an instance's health check directly from our system to CloudWatch.
- 53) Tags are assigned to resources automatically by autoscaling.
- 54) Stop Instance API to release compute resources but preserve the data on the boot partition.
- 55) Cluster Placement Group allows cluster compute resources in clusters.
- 56) Reference the logical ID.
- 57) Cannot have aws:
- 58) Snapshots are only available through the EC2 APIs
- 59) Stack and logical resource name.
- 60) **WaitCondition** and /var/log/
- 61) Logical ID must be unique within the template
- 62) When resources form a Depend On loop
- 63) Define an elastic network interface for eth0 instead of using an existing network interface.
- 64) Cross connect not created within 90 days, then the authority granted expires.
- 65) Route through front-end
- 66) First detach the virtual private gateway and then delete the VPC
- 67) Any data transfer out is billed at the Remote Region ka rate

- 68) Single-mode Optic Fibre
- 69) We cannot detach a primary network interface from an instance.
- 70) First create a Igw and then attach.
- 71) IKE Security is first established.
- 72) No need to configure with multiple subnets.
- 73) AWS will not attach public IP to an instance with more than one ENI
- 74) Wizard mein ban jayega automatically NAT. VPC updates the route table with a private subnet, and adds a route for a public subnet.
- 75) Use a secondary private IP as a failover.
- 76) Instances do not need public IP.
- 77) Projection is a set of attributes that is copied from a table into a secondary index.
- 78) Cannot add secondary indexes through DynamoDB console.
- 79) JSON is used as transport, not a storage format
- 80) Detailed listing of secondary indexes, we should describe Table action.
- 81) Atomic increment or decrement on scalar values.
- 82) Cannot change the zone of an instance after launch.
- 83) Du and stat utilities for measuring disk usage of a file.
- 84) Specific region, not AZ.
- 85) Used KMS master key to generate customer master key
- 86) Each new combination becomes a new metric.
- 87) 20 data points for one putMetric. 8Kb GET, 40Kb POST
- 88) 8 metrics for 1 dimension.
- 89) Region specific. Us-east1.
- 90) List-metric and get-metric
- 91) 15 minutes.

- 92) Increase to 2 and do Route 53 round robin.
- 93) Increase size to 3TB
- 94) Minimize blast radius, create one shared account. Create separate roles for business units and security teams.
- 95) ElastiCache and a dead-letter queue.
  - A) EC2 --user-data
  - B) SSE-customer-key
  - C) KMS --ciphertext-blob parameter

PDF 335 - :

- 1) Add the template to S3 and give the department permission to assume the manager role and add a policy to restrict the permissions and resources it creates.
- 2) Spot Fleet is always a good option. Use reserved to meet reserved capacity demands.
- 3) Use a NAT gateway and associate an elastic IP with the NAT that can be whitelisted.
- 4) 2 backend endpoints and DNS-level failover.
- 5) Block address on peer AC. Create static on VPC-A and VPC-B for VPC-A.
- 6) Delete messages and create a delay queue. Add error handling to message processing code.
- 7) Employ a multi-region solution. Use S3 to switch traffic.
- 8) CloudFront distribution -> WAF on it. Internet gateway and use a shield on it.
- 9) Use CloudWatch Events to trigger **Amazon Systems Manager Run command** to invoke the log collection more frequently and reduce the possibility of log messages being lost in an outage.
- 10) Event patterns in Cloudwatch events to capture API call events.
- 11) VM Import/Export is a good option.
- 12) AWS Config and USF allow launching of EC2 instances using a centralized DevOps team, using an internal ticketing system.
- 13) Configure an Amazon Cloudwatch events rule that invokes Lambda to secure S3. Use S3 bucket permissions for Trusted Advisor and configure AWS Cloudwatch to notify SNS.
- 14) Cron Job on the web server instance.

- 15) Systems Manager to manage patching. Test outside and deploy after approval.
- 16) Create and deploy CloudFormation stacks and reference new lambda versions. Change CloudFront Origin.
- 17) Re-host.
- 18) Failover + RDS Event notification to react to the failure and promote read replica
- 19) AWS SnowBall to migrate existing cluster data to S3. Persistent EMR cluster.
- 20) EC2 instances that are running the .NET. Migrate Cassandra to DynamoDB
- 21) For the S3 bucket, event notification when ec2:runInstance and point to Lambda Function.
- 22) Physical-to-virtual conversion. Transfer server image over AWS Direct Connect and transfer static data to s3.
- 23) Use AWS Config to prevent deleting RDS and EBS resources.
- 24) AMI based software packaging. And use Auto Scaling to deploy the production fleet.
- 25) Convert cron job to AWS Lambda and schedule to run using Cloudwatch events.
- 26) Put in DynamoDB when we do not want real-time
- 27) DMS to replicate and cut-over when data is synchronized.
- 28) EMR S3DistCp has a synchronization mechanism between on premises and Hadoop clusters.
- 29) Implement agents and implement a reverse proxy layer in front of web servers and configure IDS/IPS agents on this reverse proxy layer.
- 30) Use AWS Data Pipeline to schedule a cross region copy once a day. Create a 'LastUpdated' attribute that would represent the timestamp of the last update and use it as a filter.
- 31) Route payment requests through the NAT and whitelist the elastic IP addresses attached.
- 32) Elastic Transcoder and S3 lifecycle policy.
- 33) Route Propagation on the VGW and modify instance VPC route table by adding a route back to the customer's on-premise.
- 34) Develop Identity broker and get federated user credentials.
- 35) TCP Listeners on TCP 443 and configure health checks against all Web Servers.
- 36) Proxy Protocol Support.

- 37) Shared VPC in the central account. Within the private hosted zone, Programmatically associate other VPC's with the hosted zone.
- 38) In-memory caching application running on an EBS-optimized EC2 instance. Install ES cluster to store log files as they are delivered.
- 39) ES and DMS.
- 40) Replace with t2.xLarge and convert the RDS instance to a self-managed MySQL cluster.
- 41) String equals with VPC endpoint and source:Vpce matching.
- 42) Event notification to react to failure and promote.
- 43) Physical-to-virtual conversion on the application server.

C, D, B, B, C, D, D, A, D, A, C, B, (D, E), C, A, B, C, (A, D), C, Skip, D, A, C, A, D, C, A, D, B, A, **B**, A, **C**, A

321, 241, 228, 261, 268, 132, 186, 217, 250, 300, 332, 258, 287, 253, 260, 263, 279, 329

- 8) For Direct Connect **Public** Interface is the answer. Redistribute BGP.
- 10) Propagate specific routes.
- 16) Run simulations in Memory on EC2
- 18) S3 with RRS, CloudSearch and Beanstalk
- 24) Improve Read and Write
- 25) Global Services Option Enabled
- 29) Backup with automated daily DB backups and AMI snapshots.
- 33) Where the answer is not import/export. It is EC2 VM Connector for vCenter
- 60) Use SAML allowing people to sign-in to Console. DO NOT USE SS)
- 67) Physical Access to Compute resources.
- 72) ApplyImmediately
- 73) EC2 Address

76) Elastic IP the company wants to advertise.

85) ELB can support only one subnet in each AZ

86) Subnet group

90) EBS Volume Size does not affect PIOPS Rate

93) VPN CloudHub

109) Elastic Network Interface will have fixed MAC

124) DataSync Attempt does not create a set of actionable instances.

130) GetSessionToken without any special permission

136 confusing. We just need a peer here. No need to block IP

145) NotAction

146) AuthAge

147) Minimum PIOPS MySQL -> 1000

148) Ismein TTL with Elasticache

154) Ratio cannot be higher than 30

194) describe-stack-resource

204) Inside subnet target to NAT is wrong

213) Public Ip is not assigned to an instance with multiple ENIs

214) VPC Wizard: Updates main route table with **private** subnet and creates a

217) Instances do not need public IP

224) DescribeTable

241) Round Robin: Minimize the downtime

248) Dead Letter and Elasticache

250) Systems Manager. Do not select cron jobs

256) CRON JOBS

SimpleMonthly Spend S3. Trusted Advisor.

309) Pre Packaged vs Blue/Green