EC2 & Load Balancer Issues

1. EC2 Instance Not Starting

Troubleshooting Steps:

1. Check instance status in AWS Console (EC2 → Instances).
2. Check if the instance has sufficient permissions to start.
3. Verify instance type and available limits in your AWS account.
4. Check the system logs using EC2 → Actions → Monitor and troubleshoot → Get system log.
5. If a corrupted boot volume is suspected, detach the root volume, attach it to another instance, and inspect logs.

2. EC2 Instance Stuck in "Initializing" State

Troubleshooting Steps:

1. Check CloudWatch metrics for CPU, disk, and memory usage.
2. Verify if instance status checks are failing.
3. Restart the instance and check if it passes health checks.
4. Review /var/log/messages or /var/log/syslog using SSH.
5. If the issue persists, create a new instance from a snapshot.

3. Unable to SSH into EC2 Instance

Troubleshooting Steps:

1. Verify the security group has inbound rules allowing SSH (port 22).
2. Ensure the instance has a public IP or elastic IP assigned.
3. Check that the key pair used matches the one assigned to the instance.
4. Use the EC2 serial console for debugging if SSH is not accessible.
5. Restart the instance and try connecting again.

4. Elastic Load Balancer (ELB) Not Distributing Traffic

Troubleshooting Steps:

1. Ensure target instances are healthy (Load Balancer → Target Groups → Health Status).
2. Check security groups and network ACLs allowing traffic to and from ELB.
3. Verify that listeners are configured properly (e.g., HTTP/HTTPS on correct ports).
4. Ensure proper instance registration in the target group.
5. Check CloudWatch metrics for ELB traffic patterns.

5. EC2 Instance Running Out of Disk Space

Troubleshooting Steps:

1. Run df -h to check disk usage.
2. Identify large files with du -sh /* | sort -h.
3. Clear logs (/var/log/) or move them to S3.
4. Extend the volume via AWS Console (EC2 → Volumes → Modify Volume).
5. Resize the filesystem with sudo resize2fs /dev/xvdf.

6. EC2 Instance Terminated Unexpectedly

Troubleshooting Steps:

1. Check CloudTrail logs for termination events.
2. Verify AWS Auto Scaling settings (if in a group).
3. Check if the instance hit a billing or spot pricing limit.
4. Review termination protection settings in EC2.
5. Restore the instance using an AMI or snapshot.

7. ELB Not Accepting HTTPS Requests

Troubleshooting Steps:

1. Ensure an SSL certificate is attached to the ELB (ACM → Certificates).
2. Verify that the listener is set to HTTPS (443).
3. Check security group rules allowing port 443.
4. Confirm backend instances accept HTTPS traffic.
5. Review logs in CloudTrail and CloudWatch for SSL-related errors.

8. EC2 High CPU Utilization

Troubleshooting Steps:

1. Check CloudWatch metrics for spikes in CPU usage.10
2. Use top or htop to identify high CPU processes.
3. Restart heavy processes or optimize application code.
4. Consider increasing instance type (vertical scaling).
5. Use Auto Scaling (horizontal scaling) if necessary.

9. Auto Scaling Group Not Launching Instances

Troubleshooting Steps:

1. Check the launch template or configuration for errors.
2. Ensure the AMI used is valid and accessible.
3. Verify instance limits for your AWS account.
4. Check if an insufficient subnet/IP issue exists.
5. Review scaling policies and CloudWatch alarms.

10. EC2 Spot Instance Terminated Suddenly

Troubleshooting Steps:

1. Check spot price history (EC2 → Spot Requests).
2. Set a higher maximum bid for spot pricing.
3. Use Spot Fleet or On-Demand instances for reliability.
4. Review AWS Auto Scaling policies to replace terminated instances.
5. Store important data in persistent storage (EBS or S3).

S3 & IAM Issues

11. Access Denied to S3 Bucket

Troubleshooting Steps:

1. Check the bucket policy for Deny statements.
2. Verify IAM role/user permissions (s3:GetObject, s3:ListBucket).
3. Ensure the bucket is public if needed.
4. Confirm the correct AWS region is being used.
5. Check CloudTrail logs for any permission-related events.

12. S3 Bucket Not Allowing Public Access

Troubleshooting Steps:

1. Check Block all public access settings in S3.
2. Modify bucket ACLs to allow public read (GetObject).
3. Update the bucket policy with appropriate permissions.
4. Use pre-signed URLs for secure access if needed.
5. Verify IAM permissions for anonymous access.

13. S3 Object Upload Failing

Troubleshooting Steps:

1. Ensure correct permissions (s3:PutObject).
2. Check bucket encryption settings (if enforced).
3. Verify object size limits (5GB for a single upload).
4. Use multipart upload for large files.
5. Check for AWS SDK errors or misconfigured credentials.

14. IAM User Unable to Assume Role

Troubleshooting Steps:

1. Check IAM role trust policy (sts:AssumeRole).
2. Ensure MFA is enabled if required.
3. Verify the correct session duration is set.
4. Use AWS STS to manually assume the role and troubleshoot.
5. Review CloudTrail logs for any policy denial.

15. IAM Access Key Compromised

Troubleshooting Steps:

1. Immediately disable or delete the key in IAM.
2. Rotate credentials and update all services using the key.
3. Check CloudTrail for suspicious API calls.
4. Enforce MFA for all users.
5. Review security policies and limit excessive permissions.

16. S3 Bucket Versioning Not Working

Troubleshooting Steps:

1. Ensure versioning is enabled (S3 → Bucket → Properties).
2. Check permissions for s3:PutObjectVersion.
3. Verify lifecycle policies are not deleting old versions.
4. Use AWS CLI aws s3api list-object-versions to confirm.
5. Check CloudTrail logs for versioning changes.

17. EC2 Instance Role Not Able to Access S3

Troubleshooting Steps:

1. Verify IAM role attached to the instance (EC2 → IAM Role).
2. Ensure correct permissions (s3:ListBucket, s3:GetObject).
3. Confirm instance metadata service (IMDSv2) is accessible.
4. Run aws s3 ls from the instance to test.
5. Review CloudTrail logs for permission errors.

18. S3 Bucket Lifecycle Rules Not Deleting Objects

Troubleshooting Steps:

1. Ensure lifecycle rules are correctly configured.
2. Check the prefix and tag filters in the policy.
3. Verify IAM permissions (s3:DeleteObject).
4. Manually delete an object to test.
5. Check AWS Config for any policy conflicts.

19. S3 Transfer Acceleration Not Working

Troubleshooting Steps:

1. Ensure acceleration is enabled (S3 → Bucket → Properties).
2. Use the correct endpoint (.s3-accelerate.amazonaws.com).
3. Check AWS region compatibility.
4. Test with AWS CLI aws s3 cp --endpoint-url.
5. Verify CloudFront settings if used with S3.

20. AWS CLI Authentication Failing

Troubleshooting Steps:

1. Run aws configure and check credentials.
2. Ensure ~/.aws/credentials file exists and is valid.
3. Verify IAM permissions.
4. Check environment variables (AWS_ACCESS_KEY_ID).
5. Update AWS CLI to the latest version.

RDS, DynamoDB & Database Issues

21. RDS Instance Not Connecting

Troubleshooting Steps:

1. Verify that the RDS instance is in the "available" state (RDS → Instances).
2. Check security groups and allow inbound traffic on the correct port (e.g.,3306 for MySQL, 5432 for PostgreSQL).
3. Ensure the database credentials are correct.
4. Verify that the database's parameter group and subnet group are properly configured.
5. Test connection using telnet <RDS_ENDPOINT> <PORT> or nc -zv <RDS_ENDPOINT> <PORT>.

22. RDS High CPU Utilization

Troubleshooting Steps:

1. Check CloudWatch metrics for CPU utilization (RDS → Monitoring).
2. Identify slow queries using Performance Insights.
3. Check SHOW PROCESSLIST; (MySQL) or pg_stat_activity (PostgreSQL) for long-running queries.
4. Scale up the instance or optimize queries and indexes.
5. Enable read replicas to distribute the load.

23. DynamoDB Table Not Scaling

Troubleshooting Steps:

1. Check CloudWatch metrics for ReadCapacityUnits and WriteCapacityUnits.
2. Verify that Auto Scaling is enabled in DynamoDB → Tables → Capacity.
3. If manually provisioned, increase capacity.
4. Optimize queries to reduce the number of read/write requests.
5. Use DAX (DynamoDB Accelerator) to improve read performance.

24. RDS Connection Timeout

Troubleshooting Steps:

1. Confirm the database is running (RDS → Instances → Status).
2. Check VPC security groups and ensure inbound rules allow access.
3. Verify subnet group and whether the database is in the correct availability zone.
4. Try connecting from another instance within the same VPC.
5. Ensure that Public Access is enabled if accessing from outside AWS.

25. RDS Database Storage Full

Troubleshooting Steps:

1. Check RDS → Monitoring → Free Storage Space.
2. Increase allocated storage (Modify Instance → Storage).
3. Identify large tables with SELECT table_schema, table_name, round(sum(data_length + index_length) / 1024 / 1024, 2) FROM information_schema.tables GROUP BY table_schema, table_name;
4. Delete old or unnecessary data.
5. Enable automatic storage scaling to prevent future issues.

26. DynamoDB Throttling Errors (Provisioned Throughput Exceeded)

Troubleshooting Steps:

1. Check CloudWatch logs for ThrottledRequests.
2. Increase read/write capacity (DynamoDB → Tables → Capacity).
3. Enable Auto Scaling to prevent future throttling.
4. Use exponential backoff in API requests.
5. Consider enabling DAX (DynamoDB Accelerator) for read-heavy workloads.

27. RDS Multi-AZ Failover Not Working

Troubleshooting Steps:

1. Check if Multi-AZ is enabled (RDS → Modify Instance).
2. Ensure the standby instance is available (RDS → Events).
3. Manually force a failover (Actions → Failover).
4. Verify DNS endpoint resolution (nslookup <RDS_Endpoint>).
5. If needed, restart the primary instance and test failover again.

28. Unable to Restore RDS Snapshot

Troubleshooting Steps:

1. Check snapshot status (RDS → Snapshots → Status).
2. Ensure the snapshot is not encrypted with a missing KMS key.
3. Choose a compatible instance type when restoring.
4. Verify that the correct VPC and security group settings are used.
5. Check CloudTrail logs for permission-related errors.

29. DynamoDB Backup and Restore Issues

Troubleshooting Steps:

1. Verify backup status (DynamoDB → Backups).
2. Ensure proper IAM permissions (dynamodb:CreateBackup, dynamodb:RestoreTableFromBackup).
3. Check if the restore region is supported.
4. If restoring fails, try exporting to S3 and re-importing manually.
5. Use Point-in-Time Recovery (PITR) for automated rollback.

30. RDS Read Replica Lagging Behind Primary

Troubleshooting Steps:

1. Check replication status (SHOW SLAVE STATUS; for MySQL, pg_stat_replication for PostgreSQL).
2. Increase instance size if the replica is underpowered.
3. Tune replication settings (rds_replica_transaction_apply_delay).
4. Reduce write load on the primary instance.
5. Restart the replica instance and monitor performance.

AWS Lambda, API Gateway, and CloudFront Issues

31. AWS Lambda Timeout Error

Troubleshooting Steps:

1. Check the function’s timeout settings (Lambda → Function → Configuration → General settings).
2. Increase the timeout if necessary (default is 3 seconds).
3. Optimize the function code (e.g., avoid unnecessary loops, optimize database queries).
4. Check CloudWatch logs (Lambda → Monitor → View Logs in CloudWatch) for performance bottlenecks.
5. If calling external APIs, ensure they respond within the timeout limit.

32. Lambda Function Exceeds Memory Limit

Troubleshooting Steps:

1. Check memory settings in the Lambda configuration (Lambda → Function → Configuration → General settings).
2. Increase memory allocation incrementally and test performance.
3. Optimize the function by reducing payload size and avoiding redundant computations.
4. Use CloudWatch logs to identify which part of the function consumes the most memory.
5. Consider using AWS Step Functions for large workloads.

33. API Gateway Returning 403 Forbidden

Troubleshooting Steps:

1. Verify that the API Gateway resource policies allow access (API Gateway → Permissions).
2. Check if IAM roles and permissions are set up correctly (IAM → Policies).
3. If using Lambda, ensure the function’s execution role has lambda:InvokeFunction permissions.
4. Review API Gateway logs in CloudWatch to identify the exact issue.
5. If using AWS WAF, check if any rules are blocking the request.

34. API Gateway Throttling Requests (429 Error)

Troubleshooting Steps:

1. Check the API Gateway rate limits (API Gateway → Stages → Throttling).
2. Increase rate and burst limits if necessary.
3. If using Lambda, ensure the concurrency limit isn’t exceeded (Lambda → Concurrency).
4. Implement retries with exponential backoff in your application.
5. Consider using AWS AppSync or AWS Step Functions for high-throughput workloads.

35. CloudFront Returning 502 Bad Gateway

Troubleshooting Steps:

1. Check the origin server's health in CloudFront (CloudFront → Origins → Health).
2. Verify that the origin is responding to requests (use curl or Postman to test).
3. Increase the timeout setting (CloudFront → Behavior → Origin Response Timeout).
4. Check if SSL/TLS settings are misconfigured (CloudFront → Distribution → SSL Settings).
5. If using Lambda@Edge, ensure the function isn’t causing an error in the response.

36. CloudFront Serving Stale Content

Troubleshooting Steps:

1. Invalidate the cache manually (CloudFront → Invalidations → Create Invalidation).
2. Reduce TTL settings (CloudFront → Behavior → Cache Policy).
3. Ensure the origin server returns correct cache headers (Cache-Control: no-cache).
4. Enable Origin Shield to reduce outdated cached responses.
5. If using S3, check bucket settings for Object Lock or Versioning.

37. API Gateway Returning 504 Gateway Timeout

Troubleshooting Steps:

1. Check if the backend service (Lambda, EC2, RDS) is responding within the timeout limit.
2. Increase the Integration Response Timeout in API Gateway settings.
3. Optimize the backend service's response time (e.g., reduce DB query times).
4. If using VPC Link, ensure the target resource is accessible from the API Gateway.
5. Check CloudWatch logs to identify slow responses.

38. AWS Lambda Function Deployment Failing

Troubleshooting Steps:

1. Ensure the deployment package is under the allowed size limit (50MB for direct upload, 250MB for S3).
2. If using a ZIP file, verify the structure (should contain index.js or handler.py).
3. Check IAM execution role permissions for Lambda (IAM → Roles → Lambda Execution Role).
4. If using layers, confirm that dependencies are correctly packaged.
5. Deploy using AWS SAM or Serverless Framework for better dependency management.

39. Lambda Cold Start Issues

Troubleshooting Steps:

1. Use Provisioned Concurrency to keep instances warm (Lambda → Configuration → Concurrency).
2. Reduce package size by removing unnecessary dependencies.
3. Use AWS SDK connections outside the function handler to persist between invocations.
4. Optimize initialization logic to minimize execution delays.
5. If possible, switch to a different runtime that has better cold start performance (e.g., JavaScript over Java).

40. Lambda Logs Not Appearing in CloudWatch

Troubleshooting Steps:

1. Ensure the Lambda function's execution role has CloudWatchLogs:CreateLogGroup, CreateLogStream, and PutLogEvents permissions.
2. Verify that logs are being generated (Lambda → Test → View Logs).
3. Check CloudWatch log groups manually (CloudWatch → Log Groups → Lambda).
4. If logs are missing, add explicit logging in the function (console.log() for Node.js, print() for Python).
5. Ensure that the CloudWatch log retention policy isn't automatically deleting logs.

AWS CI/CD, Security, and Miscellaneous Issues

41. AWS CodePipeline Stuck in Progress

Troubleshooting Steps:

1. Check AWS CodePipeline execution history (CodePipeline → Pipelines →Execution History).
2. Identify the stage causing the issue (Source, Build, Deploy).
3. Check AWS CodeBuild logs for errors (CodeBuild → Build history → Logs).
4. Verify IAM role permissions (IAM → Roles → Check Pipeline Role for required policies).
5. Restart the failed stage or retry the pipeline execution.

42. CodeBuild Failing Due to Dependency Errors

Troubleshooting Steps:

1. View build logs in CodeBuild → Build history → Logs.
2. If using npm, Python, or Maven, ensure dependencies are correctly listed in package.json, requirements.txt, or pom.xml.
3. Check if the build container has access to the internet (VPC → NAT Gateway → Ensure internet access).
4. Run aws codebuild batch-get-builds to get more error details.
5. Use a custom build image with pre-installed dependencies if necessary.

43. AWS CodeDeploy Deployment Stuck in Pending

Troubleshooting Steps:

1. Check instance status in EC2 → Instances to ensure they are running.
2. Verify that the CodeDeploy agent is installed (sudo service codedeploy- agent status).
3. Restart the agent (sudo service codedeploy-agent restart).
4. Ensure IAM permissions allow codedeploy:CreateDeployment.
5. Manually trigger the deployment again and monitor logs.

44. AWS Secrets Manager Secrets Not Rotating

Troubleshooting Steps:

1. Check Secrets Manager rotation status (Secrets Manager → Secrets → Rotation).
2. Ensure the Lambda function assigned for rotation has correct permissions (secretsmanager:RotateSecret).
3. Check CloudWatch logs for errors related to rotation.
4. Test manual rotation by clicking Rotate secret now.
5. If automatic rotation fails, update the Lambda rotation function and retry.

45. CloudFormation Stack Failing to Create

Troubleshooting Steps:

1. Check CloudFormation → Stack Events for error messages.
2. Validate template syntax (aws cloudformation validate-template – template-body file://template.yml).
3. Ensure required IAM roles exist before running the stack.
4. Verify that resources (e.g., S3 buckets, EC2 instances) are available.
5. If rollback happens, enable Rollback on failure to debug the issue.

46. CloudTrail Not Logging Events

Troubleshooting Steps:

1. Verify CloudTrail is enabled (CloudTrail → Trails → Status).
2. Check if logs are being written to the specified S3 bucket (S3 → Bucket → Check for log files).
3. Ensure the IAM role for CloudTrail has permissions to write to S3.
4. If using an organization trail, confirm it is properly configured (AWS Organizations → Service Control Policies).
5. Restart CloudTrail logging (aws cloudtrail start-logging --name <trail- name>).

47. AWS KMS Key Access Denied

Troubleshooting Steps:

1. Check KMS key policy (KMS → Customer Managed Keys → Key Policy).
2. Ensure IAM role or user has kms:Decrypt and kms:Encrypt permissions.
3. Verify that the principal using the key is listed in the key policy.
4. Check if the key is enabled (KMS → Key → Status).
5. If cross-account access is needed, update the resource policy to allow external access.

48. AWS SNS Notifications Not Being Delivered

Troubleshooting Steps:

1. Verify that the SNS topic is active (SNS → Topics → Check Subscription Status).
2. Ensure the correct endpoint (email, SMS, Lambda, etc.) is subscribed.
3. Check if the recipient email/SMS provider is blocking messages.
4. Use AWS SNS → Delivery Status Logging to check failed messages.
5. Resubscribe to the topic if needed and test with a simple message.

49. AWS Config Not Recording Changes

Troubleshooting Steps:

1. Check if AWS Config is enabled (Config → Settings).
2. Ensure the required AWS resources (S3, EC2, IAM, etc.) are included in the rules.
3. Verify IAM permissions (config:PutEvaluations, config:GetComplianceDetailsByResource).
4. Check AWS Config logs in CloudWatch for errors.
5. Manually trigger resource evaluation (aws configservice start-config- rules-evaluation).

50. AWS Elastic Beanstalk Deployment Failing

Troubleshooting Steps:

1. Check Elastic Beanstalk logs (EB → Environment → Logs).
2. Verify that the instance type and resources meet application requirements.
3. Ensure the correct runtime and platform version is selected.
4. Check environment health (EB → Environment → Health).
5. If needed, redeploy a previous working version from EB → Application Versions.

AWS Networking, ECS, and EKS Issues

51. VPC Peering Not Working

Troubleshooting Steps:

1. Verify that the VPC peering connection is in an "Active" state (VPC → Peering Connections).
2. Update route tables to include routes for the peered VPC (VPC → Route Tables → Edit Routes).
3. Check security groups and network ACLs to allow traffic between the VPCs.
4. Ensure that DNS resolution is enabled for private IP addresses (VPC → Peering Connection → DNS Settings).
5. Test connectivity using ping or telnet between instances in both VPCs.

52. EC2 Instance Can't Reach Internet via NAT Gateway

Troubleshooting Steps:

1. Verify the instance is in a private subnet (EC2 → Instances → Subnet).
2. Check that the NAT Gateway is associated with a public subnet (VPC → NAT Gateways).
3. Ensure the route table for the private subnet has a route to the NAT Gateway (VPC → Route Tables).
4. Check security groups and network ACLs for outbound rules allowing internet access.
5. Test by running curl google.com or ping 8.8.8.8 from the private instance.

53. ECS Task Stuck in Pending State

Troubleshooting Steps:

1. Check if there are enough available EC2 instances in the ECS cluster (ECS → Clusters → Instances).
2. Verify that the ECS service IAM role has required permissions (IAM → Roles → AmazonECSServiceRole).
3. Ensure the container image exists in the registry (ECR → Repositories → Check Image).
4. Check if the task definition is valid (ECS → Task Definitions → Check Revision).
5. Inspect ECS service logs for errors (CloudWatch → Logs → /aws/ecs/cluster-name).

54. EKS Worker Nodes Not Joining Cluster

Troubleshooting Steps:

1. Ensure that worker nodes have the correct IAM role (IAM → Roles →AmazonEKSWorkerNodeRole).
2. Verify that the worker node security group allows inbound traffic from the EKS control plane.
3. Check if the nodes are registered in the cluster (kubectl get nodes).
4. If using AWS Fargate, ensure that the pod execution role has correct permissions.
5. Restart the worker nodes and check logs for errors.

55. Kubernetes Pod CrashLoopBackOff in EKS

Troubleshooting Steps:

1. Get pod logs using kubectl logs <pod-name>.
2. Describe the pod for additional details (kubectl describe pod <pod-name>).
3. Check if the container is running out of memory (kubectl top pod).
4. Ensure the container image is correct and accessible (ECR → Repositories).
5. If necessary, delete the pod and let it restart (kubectl delete pod <pod-name>).

56. ALB Not Routing Traffic to ECS Tasks

Troubleshooting Steps:

1. Ensure that the target group is correctly attached to the ALB (EC2 → Load Balancers → Target Groups).
2. Verify that ECS tasks are registered in the target group (Target Group → Registered Targets).
3. Check health check settings (Target Group → Health Check).
4. Inspect ALB access logs (S3 → Check ALB logs if logging is enabled).
5. Test connectivity to the ECS tasks manually using curl or telnet.

57. Lambda Function Execution Role Issues

Troubleshooting Steps:

1. Check IAM role permissions (IAM → Roles → Lambda Execution Role).
2. Verify that required policies are attached (AWSLambdaBasicExecutionRole, AWSLambdaVPCAccessExecutionRole).
3. If accessing other AWS services, ensure the necessary service permissions are added.
4. Check AWS CloudTrail for permission denial logs.
5. Update and attach the correct role to the Lambda function.

58. API Gateway Returning 502 Bad Gateway

Troubleshooting Steps:

1. Check if the Lambda function or backend service is running (Lambda → Function → Monitor Logs).
2. Verify that the correct endpoint is configured in API Gateway (API Gateway → Stages → Check Endpoints).
3. Enable logging and check execution logs (CloudWatch → Logs → API Gateway Logs).
4. Test API Gateway manually using Postman or curl.
5. If the backend is an EC2 instance, ensure it has an open security group rule.

59. S3 Event Notification Not Triggering Lambda

Troubleshooting Steps:

1. Verify that S3 event notifications are enabled (S3 → Properties → Event Notifications).
2. Check if the Lambda function has the correct execution role (IAM → Roles → AWSLambdaS3ExecutionRole).
3. Test manually by uploading a file to the S3 bucket and checking Lambda logs (CloudWatch → Logs).
4. Ensure the Lambda function's permission policy allows S3 to invoke it (Lambda → Configuration → Permissions).
5. Delete and recreate the S3 event notification.

60. AWS Step Function Stuck in Running State

Troubleshooting Steps:

1. Check execution history in AWS Step Functions (Step Functions →Executions).
2. Identify which step is causing the delay (Step Functions → Execution Graph).
3. Check logs for the failing step (CloudWatch → Logs).
4. If using Lambda, ensure the function has sufficient timeout limits.
5. Manually retry the step or adjust timeout settings.

AWS ECS, EKS, and Container Issues

61. ECS Task Stuck in Pending State

Troubleshooting Steps:

1. Ensure the ECS cluster has sufficient EC2 instances (ECS → Clusters → Instances).
2. Verify that the ECS task definition is valid and correctly configured (ECS → Task Definitions → Check Revision).
3. Confirm that there are enough resources (CPU, memory) to run the task.
4. Check the IAM roles for correct permissions (IAM → Roles → AmazonECSServiceRole).
5. Review ECS service logs for any potential errors (CloudWatch → Logs →/aws/ecs/<cluster-name>).

62. ECS Service Not Scaling as Expected

Troubleshooting Steps:

1. Verify the scaling policy is configured correctly in the ECS service (ECS → Services → Check Scaling Policies).
2. Ensure that the EC2 instances in the cluster have sufficient resources.
3. Confirm that there are no limits set on scaling in the Auto Scaling group (EC2 → Auto Scaling → Groups).
4. Check for any failed tasks or unhealthy instances in the ECS service.
5. Review CloudWatch alarms and metrics to ensure scaling is triggered based on CPU or memory utilization.

63. Fargate Task Running Out of Memory

Troubleshooting Steps:

1. Increase the memory allocation in the Fargate task definition (ECS → Task Definitions → Edit Memory).
2. Check for memory leaks in the application logs (CloudWatch → Logs → /aws/ecs/).
3. Review the task's CPU and memory resource limits to ensure they match the workload requirements.
4. Ensure the application inside the container is optimized for memory usage.
5. Scale out by running more tasks or increase the memory limit in the ECS service.

64. EKS Pod Stuck in CrashLoopBackOff

Troubleshooting Steps:

1. Check the pod's logs using kubectl logs <pod-name> for error details.
2. Use kubectl describe pod <pod-name> to see events and identify potential configuration issues.
3. Inspect the resource limits in the pod's configuration (kubectl get pod <pod-name> -o yaml).
4. Ensure the application inside the pod is healthy and has no dependency issues.
5. Restart the pod or delete and let it reschedule automatically.

65. EKS Nodes Not Joining the Cluster

Troubleshooting Steps:

1. Check the IAM role attached to the worker nodes (IAM → Roles → AmazonEKSWorkerNodeRole).
2. Ensure that the worker node security group allows inbound traffic from the EKS control plane.
3. Verify the VPC subnets are correctly configured for EKS.
4. Use kubectl get nodes to check if the nodes are registered.32
5. Restart the worker nodes and check logs for errors (/var/log/cloud- init.log on EC2 instances)

66. EKS Ingress Controller Not Routing Traffic

Troubleshooting Steps:

1. Ensure that the ingress controller is installed and properly configured in the EKS cluster.
2. Check the ingress resource (kubectl get ingress) for correct configuration.
3. Verify that the associated service has the correct annotations for the ingress controller (kubectl describe service <service-name>).
4. Review the security groups to make sure they allow inbound HTTP/HTTPS traffic.
5. Check the logs of the ingress controller to debug routing issues (kubectl logs <ingress-controller-pod>).

67. EKS IAM Role Not Attaching to Service Account

Troubleshooting Steps:

1. Ensure the correct service account exists and is associated with the Kubernetes service (kubectl get serviceaccount).
2. Verify that the service account has the necessary IAM permissions (IAM → Roles → EKSServiceAccountRole).
3. Ensure the service account is linked to the correct IAM role using the eks.amazonaws.com/role-arn annotation.
4. Confirm that the OIDC identity provider is configured for the EKS cluster (EKS → Identity Providers).
5. Review the kubectl describe serviceaccount for any missing annotations or role bindings.

68. ECS Logs Not Appearing in CloudWatch

Troubleshooting Steps:

1. Ensure the ECS task definition includes the correct CloudWatch log configuration (ECS → Task Definitions → Check Log Configuration).
2. Verify that the ECS task has the appropriate IAM permissions to publish logs (IAM → Roles → AmazonECSTaskExecutionRole).
3. Confirm that CloudWatch Logs are enabled in the ECS service (CloudWatch → Logs → Log Groups).
4. Check the log stream for the task's specific log group (CloudWatch → Logs → /aws/ecs/).
5. Check for any errors in the IAM role permissions related to CloudWatch.

69. Docker Image Pull Failure in ECS

Troubleshooting Steps:

1. Verify that the Docker image is correctly uploaded to Amazon ECR (ECR → Repositories → Image Availability).
2. Ensure ECS has the appropriate IAM permissions to pull from ECR (IAM → Roles → AmazonECSTaskExecutionRole).
3. Check for image version mismatches in the ECS task definition (ECS → Task Definitions).
4. Validate that the image URL is correct and follows the format aws_account_id.dkr.ecr.region.amazonaws.com/repository_name.
5. Check network settings, ensuring the ECS container has internet access if using an external Docker registry.

70. ECS Service Not Registering with ALB

Troubleshooting Steps:

1. Ensure that the ECS service is linked to the correct target group (ECS → Services → Load Balancer).
2. Check if the security groups for the ALB and ECS instances allow traffic between them.
3. Verify that the target group health checks are configured properly (EC2 → Load Balancers → Target Groups → Health Check).
4. Ensure that the ECS task definition is correctly set to route traffic to the

ALB (ECS → Task Definitions → Ports Configuration).

5. Review the ALB access logs for errors in routing.

AWS Monitoring, Security, and Miscellaneous Issues

71. ALB Not Routing Traffic to ECS Tasks

Troubleshooting Steps:

1. Confirm that the ALB is associated with the correct target group (EC2 → Load Balancers → Target Groups).
2. Check the health check settings for the target group (EC2 → Target Groups → Health Checks).
3. Verify the ECS service is running and tasks are in the "running" state.
4. Check security group settings to ensure inbound traffic is allowed.
5. Use curl or telnet to test connectivity from the ALB to the ECS tasks.

72. VPC Peering Not Working

Troubleshooting Steps:

1. Verify that the VPC peering connection is in an "Active" state (VPC → Peering Connections).
2. Check the route tables in both VPCs to ensure routes are added for peering.
3. Confirm security group and network ACLs are configured to allow communication between VPCs.
4. Check if DNS resolution settings are enabled for peered VPCs (VPC → Peering Connection → DNS Settings).
5. Test the connection with ping or telnet from an instance in each VPC.

73. EC2 Instance Can't Reach Internet via NAT Gateway

Troubleshooting Steps:

1. Verify the NAT Gateway is in a public subnet and the route table of private subnets points to the NAT Gateway.36
2. Ensure that the security group and network ACLs allow outbound internet traffic.
3. Check if the instance has an Elastic IP assigned for internet access.
4. Ensure that the NAT Gateway has sufficient capacity.
5. Test by running curl google.com or ping 8.8.8.8 from the EC2 instance.

74. S3 Bucket Policy Not Allowing Access

Troubleshooting Steps:

1. Verify that the S3 bucket policy allows access for the specific IAM role or user (S3 → Permissions → Bucket Policy).
2. Check if there are any conflicting permissions with ACLs or IAM roles.
3. Ensure the correct Principal is specified in the policy.
4. Verify that the requestor's IP address or VPC endpoint is not blocked.
5. Review the AccessAnalyzer findings for any blocked access.

75. VPC Security Group Misconfiguration

Troubleshooting Steps:

1. Verify that the correct ports (e.g., 22 for SSH, 80 for HTTP) are open for the EC2 instance (EC2 → Security Groups → Inbound Rules).
2. Check for conflicting inbound and outbound rules that could block traffic.
3. Ensure that the security group is associated with the correct instances (EC2 → Instances → Security Groups).
4. Review the security group for any rules restricting IP addresses or CIDR blocks.
5. Test connectivity from a remote location using telnet or curl.

76. CloudWatch Logs Not Appearing

Troubleshooting Steps:

1. Verify that the log group and log stream exist (CloudWatch → Logs → Log groups).
2. Check if the application or service has the correct IAM permissions (IAM → Policies → Ensure logs:CreateLogGroup, logs:CreateLogStream, logs:PutLogEvents).
3. Confirm that the log retention period is set correctly (CloudWatch → Logs → Select Log Group → Retention settings).
4. Restart the application or Lambda function to trigger logging.
5. Use the AWS CLI to manually push test logs (aws logs put-log-events).

77. AWS Config Not Recording Changes

Troubleshooting Steps:

1. Check if AWS Config is enabled in the region (AWS Config → Settings).
2. Ensure that AWS Config rules are correctly configured (AWS Config → Rules).
3. Verify that the IAM role for AWS Config has the required permissions (IAM → Roles → AWSConfigRole).
4. Check S3 bucket permissions if AWS Config is storing logs in S3 (S3 → Permissions).
5. Manually trigger a compliance check (AWS Config → Rules → Evaluate).

78. AWS GuardDuty Not Detecting Threats

Troubleshooting Steps:

1. Verify that GuardDuty is enabled (GuardDuty → Settings → Status).
2. Ensure that GuardDuty has the necessary permissions to access CloudTrail and VPC Flow Logs.
3. Check CloudTrail logs for security-related events (CloudTrail → Event History).
4. Simulate a threat by executing a curl command to a known malicious domain and verify detection.
5. Use AWS Security Hub to cross-check findings (Security Hub → Findings).

79. AWS WAF Not Blocking Malicious Traffic

Troubleshooting Steps:

1. Ensure that WAF is associated with the correct CloudFront distribution or ALB (WAF → Web ACLs).
2. Check WAF logs to see if rules are matching (WAF → Web ACLs → Logging and Metrics).
3. Increase the rule priority to make it effective before other rules.
4. Test rules using AWS WAF's test feature (WAF → Web ACLs → Test Rules).
5. Manually block an IP using an IP set and verify if traffic is blocked.

80. AWS Secrets Manager Not Rotating Secrets

Troubleshooting Steps:

1. Verify that automatic rotation is enabled (Secrets Manager → Secret Details → Rotation Configuration).
2. Check Lambda function permissions for rotation (IAM → Roles → Rotation Function Role).
3. Ensure the database or service allows credential rotation.
4. Manually trigger a rotation (Secrets Manager → Select Secret → Rotate).
5. Check CloudWatch logs for rotation function execution errors.

AWS Cost Management & Billing Issues

81. AWS Organizations SCP Not Enforcing Policies

Troubleshooting Steps:

1. Ensure that SCPs are enabled for the organization (Organizations → Settings → Enable SCPs).
2. Check if the policy is attached to the correct Organizational Unit (OU).
3. Validate that no other policy is overriding the SCP.
4. Use IAM Policy Simulator to test SCP effects (IAM → Policy Simulator).
5. Review CloudTrail logs for denied API actions due to SCPs.

82. AWS S3 Replication Not Working

Troubleshooting Steps:

1. Ensure that versioning is enabled on both source and destination buckets (S3 → Bucket Properties → Versioning).
2. Check IAM role permissions for replication (IAM → Roles → S3 Replication Role).
3. Verify that replication rules are correctly configured (S3 → Replication Rules).
4. Check CloudTrail logs for replication errors (CloudTrail → Event History).
5. Test by manually uploading a new file to see if replication triggers.

83. AWS Shield Advanced Not Mitigating DDoS Attacks

Troubleshooting Steps:

1. Confirm that Shield Advanced is enabled (Shield → Overview → Protected Resources).
2. Ensure that the protected resources (ALB, CloudFront, Route 53) are correctly added.
3. Check CloudWatch metrics for attack detection (CloudWatch → Metrics → DDoS Events).
4. Review WAF rules and rate limits (WAF → Web ACLs).
5. Contact AWS Support if experiencing an active attack.

84. AWS Step Functions Execution Stuck

Troubleshooting Steps:

1. Check the execution history (Step Functions → Execution History).
2. Identify the state where it got stuck and inspect the output.
3. Validate if Lambda functions or services invoked by Step Functions are responding correctly.
4. Increase timeout settings if necessary.
5. Restart execution with valid input data.

85. AWS Elastic Beanstalk Deployment Failing

Troubleshooting Steps:

1. Check Elastic Beanstalk logs (Elastic Beanstalk → Logs → Request Logs).
2. Verify if environment variables are correctly set (Elastic Beanstalk →Configuration → Environment Properties).
3. Ensure the EC2 instance running Beanstalk has the necessary permissions.
4. Check if the application code has dependencies missing (Elastic Beanstalk → Events).
5. Rebuild the application package and redeploy.

86. AWS CloudFormation Stack Failing to Create

Troubleshooting Steps:

1. Check the error message in CloudFormation → Events.41
2. Validate the template syntax (AWS CLI → aws cloudformation validate- template).
3. Ensure IAM roles used in the template have necessary permissions.
4. Verify resource limits (e.g., max EC2 instances, S3 bucket name uniqueness).
5. Delete failed stack and retry.

87. AWS Cost Explorer Showing Unexpected High Costs

Troubleshooting Steps:

1. Review cost breakdown by service (Cost Explorer → Service Breakdown).
2. Check if any new resources were provisioned unexpectedly (AWS Config → Resource Changes).
3. Identify any sudden data transfer spikes (CloudWatch → Metrics → Network Usage).
4. Enable cost alerts and budgets (AWS Budgets → Create Budget).
5. Review AWS Trusted Advisor for cost optimization recommendations.

88. AWS ECS Tasks Not Starting

Troubleshooting Steps:

1. Check ECS service event logs (ECS → Cluster → Service Events).
2. Ensure the IAM task execution role has required permissions (IAM → Roles → Task Execution Role).
3. Verify that the container image is available in ECR or public registry.
4. Confirm that the task placement strategy allows new tasks.
5. Increase available CPU or memory resources.

89. AWS Glue Job Failing

Troubleshooting Steps:

1. Check Glue job logs (Glue → Jobs → Logs).
2. Validate IAM role permissions for accessing data sources (IAM → Roles → Glue Job Role).
3. Verify that the Python/Scala script has the correct dependencies.
4. Ensure that the source and target data stores are accessible.
5. Increase job timeout if necessary.

90. AWS Auto Scaling Not Adding Instances

Troubleshooting Steps:

1. Check Auto Scaling activity history (EC2 → Auto Scaling Groups →Activity History).
2. Verify that the launch template or configuration is correct.
3. Ensure that the target scaling policy is set correctly.
4. Check if there are sufficient instance quotas in the region.
5. Confirm that health checks are passing for existing instances.

AWS Monitoring, Security, and Miscellaneous Issues

91. AWS CloudTrail Logs Not Capturing Events

Troubleshooting Steps:

1. Verify that CloudTrail is enabled (CloudTrail → Trails → Check Status).
2. Ensure that logging is turned on (CloudTrail → Edit Trail → Enable Logging).
3. Check the S3 bucket policy to allow CloudTrail to write logs.
4. Validate IAM permissions for CloudTrail
 (IAM → Policies → Ensure cloudtrail:PutEventSelectors and cloudtrail:UpdateTrail).
5. Check CloudTrail Insights to identify potential issues.

92. AWS GuardDuty Not Detecting Threats

Troubleshooting Steps:

1. Confirm that GuardDuty is enabled (GuardDuty → Settings).
2. Check if threat intelligence feeds are enabled (GuardDuty → Settings → Data Sources).
3. Verify that CloudTrail, VPC Flow Logs, and DNS logs are being monitored.
4. Ensure the GuardDuty findings are not being filtered out (GuardDuty →Findings → Filters).
5. Check IAM permissions for GuardDuty to access necessary logs.

93. AWS WAF Blocking Legitimate Traffic

Troubleshooting Steps:

1. Check WAF logs in CloudWatch to identify blocked requests (CloudWatch → Logs → Select WAF Log Group).
2. Review the WebACL rules and ensure no overly restrictive conditions exist (WAF → WebACLs → Rules).
3. Modify or disable any rule that incorrectly blocks legitimate traffic.44
4. Whitelist trusted IPs or user agents.
5. Test traffic flow using AWS WAF logging.

94. AWS Organizations SCP Not Applying to Accounts

Troubleshooting Steps:

1. Ensure the SCP is attached to the correct AWS Organizational Unit (OU).
2. Verify that the SCP is enabled (AWS Organizations → Policies → Service Control Policies).
3. Check IAM role permissions for affected accounts (IAM → Policies → Check Permissions).
4. Refresh AWS IAM policy cache using aws organizations describe-policy.
5. Remove and reapply the SCP if needed.

95. AWS Backup Failing for RDS Snapshots

Troubleshooting Steps:

1. Check backup policies in AWS Backup (AWS Backup → Backup Plans).
2. Ensure the RDS instance has automated backups enabled (RDS → Modify → Backup Retention Period).
3. Validate IAM permissions for AWS Backup (IAM → Policies → Ensure backup:StartBackupJob).
4. Check AWS Backup logs for errors (AWS Backup → Jobs → Select Failed Job → Logs).
5. Retry the backup manually and monitor CloudWatch logs for issues.

96. AWS SNS Notifications Not Being Sent

Troubleshooting Steps:

1. Check the SNS topic subscription status (SNS → Topics → Subscriptions).
2. Verify that the SNS topic has the correct IAM permissions (IAM → Policies → Ensure sns:Publish).
3. Confirm that the endpoint (email, Lambda, SQS) is active and reachable.
4. Check CloudWatch logs for SNS errors (CloudWatch → Logs → Select SNS Log Group).
5. Resend a test message via AWS CLI (aws sns publish).

97. AWS EventBridge Rule Not Triggering

Troubleshooting Steps:

1. Verify that the rule is enabled (EventBridge → Rules → Check Status).
2. Ensure the rule target (Lambda, SQS, SNS) exists and has the correct permissions.
3. Check CloudWatch metrics to see if the rule was invoked.
4. Use AWS CloudTrail to check if the event was generated.
5. Manually trigger a test event using AWS CLI (aws events put-events).

98. AWS Systems Manager (SSM) Session Manager Not Connecting to EC2

Troubleshooting Steps:

1. Ensure SSM Agent is installed and running on the instance (sudo systemctl status amazon-ssm-agent).
2. Verify that the instance has the correct IAM role (IAM → Roles → Ensure ssm:StartSession).
3. Check VPC endpoints if using a private instance (VPC → Endpoints → Ensure SSM Endpoint Exists).
4. Review SSM logs in CloudWatch (CloudWatch → Logs → /aws/ssm).
5. Restart the SSM agent (sudo systemctl restart amazon-ssm-agent).

99. AWS Glue Job Failing

Troubleshooting Steps:

1. Check job logs in CloudWatch (CloudWatch → Logs → /aws- glue/jobs/output).
2. Verify that the IAM role assigned to the job has correct permissions
(IAM → Roles → Ensure s3:PutObject, glue:StartJobRun).
3. Confirm that the Glue Data Catalog tables are correctly defined.
4. Ensure the script does not have syntax errors (Glue → Jobs → Script Editor).
5. Increase the worker type or memory allocation if the job runs out of resources.

100. AWS Cost Anomalies Detected

Troubleshooting Steps:

1. Check AWS Cost Explorer for unusual spikes (AWS Billing → Cost Explorer).
2. Identify specific services causing the cost increase (AWS Billing → Cost & Usage Reports).
3. Review recent deployments and scaling changes.
4. Enable AWS Budgets and configure alerts (AWS Billing → Budgets).
5. Investigate possible security breaches (AWS IAM → Check Unusual Activity).

All DevOps & Cloud notes in one place

Follow

www.linkedin.com/in/jotheeshwaran-v

for real-world DevOps labs, cloud architecture breakdowns, interview-ready notes, trending tools, production scenarios, certifications, and career growth insights — curated for 2026 engineers.