gart.

DevOps
Infrastructure Audit Report

19.04.2024

gart.

Infrastructure Audit results:

1. Security and Compliance

Identity and Access Management (IAM)

- Only one user has Multi-Factor Authentication (MFA) enabled; more than ten users show no activity for over 150 days, suggesting a need for account review and potential deactivation.
- Credentials lack regular rotation policies for both passwords and access keys.
- Least privilege access policies are not adequately implemented.

Security Groups and Network ACLs

- Network ACLs (NACL) allow all inbound and outbound traffic, which violates the principle of least privilege.
- Numerous security groups are potentially unused and require further investigation or removal.

Encryption

- RDS instances have encryption enabled, but several EBS volumes lack encryption.
- Limited S3 buckets have encryption enabled, showing inconsistency in the application of security practices across services.

- Logging and Monitoring

- CloudTrail is enabled for management events, but CloudWatch lacks alarms for PROD services, and VPC Flow Logs are not enabled in several critical VPCs.

Compliance

- Utilization of AWS Config and regular compliance checks with AWS Trusted Advisor are recommended practices that need emphasis.

2. Cost Management

Resource Utilization and Right-Sizing

- There is a need to review and adjust resource allocation to ensure efficient use and cost savings, including the potential adoption of Reserved Instances or Savings Plans.

gart.

Cost Allocation Tags

- Implementing a comprehensive tagging strategy could improve cost allocation and management.

Budgets and Alerts

- The configuration of AWS Budgets and billing alerts will aid in managing expenses and preventing overruns.

3. Reliability and Performance

High Availability and Disaster Recovery

- Critical services like RDS and ECS are not fully utilizing multi-AZ deployments which is crucial for high availability and disaster recovery.
- Automated snapshots are enabled for RDS but are missing for other services like EC2 and ECS.

Performance Efficiency

- Auto-scaling is partially implemented; expanding its use will help match workload demands more effectively.
- Regular performance reviews are needed to identify and resolve bottlenecks.

Service Limits

- Monitoring and proactive management of service limits are necessary to avoid disruptions.

4. Networking

VPC Configuration

- The co-location of production and development VPCs within a single AWS account raises concerns about security and operational isolation.
- Application and database layers are appropriately isolated in private subnets, minimizing direct internet exposure.

DNS and Domain Management

- No Route 53 hosted zones are configured, indicating a potential gap in DNS management and health checking capabilities.

Connectivity

- Although VPNs are not utilized, the setup of bastion hosts with restricted access provides a secure entry point into the environments.

5. Data Management

Data Storage and Backup

- Lifecycle policies are only enabled for selected S3 buckets, and their application needs broadening to include other relevant data storage.
- Regular testing of backups is limited to RDS, with a need to evaluate the necessity and frequency of backups for other resources.

Database Services

- Regular backups and performance optimization strategies are well-implemented for RDS instances.

gart.

Recommendations based on Audit results

1. Security and Compliance Improvements

- Enable Multi-Factor Authentication (MFA) for all users to strengthen security measures.
- Implement credential rotation policies for IAM users to ensure that access keys and passwords are changed regularly.
- Review and refine IAM policies to enforce least privilege access to minimize potential security breaches.
- Audit and rationalize security groups and NACLs to remove unused or unnecessary rules and ensure that both inbound and outbound traffic is restricted to what is strictly necessary.
- Enable encryption on all EBS volumes and S3 buckets using AWS KMS keys to protect data at rest across all services.
- Configure CloudWatch alarms for all critical production services to ensure performance and security issues are promptly addressed.
- Enable VPC Flow Logs for all VPCs to monitor and record network traffic for security analysis and troubleshooting.
- Regularly use AWS Config and AWS Trusted Advisor to continuously assess, audit, and evaluate AWS resource configurations for compliance with best practices.

2. Cost Management Improvements

- Perform a detailed review of resource utilization to identify underutilized resources and either decommission them or resize them to save costs.
- Adopt Reserved Instances and Savings Plans for predictable workloads to capitalize on cost savings over time.
- Implement a comprehensive tagging strategy to accurately allocate costs to various teams or projects, enhancing visibility and accountability.
- Set up and configure AWS Budgets with corresponding alerts to actively monitor and manage expenditures against predefined budget limits.
- Move FARGATE services to ARM CPU architecture to improve performance and safe up to 25% of compute budget.
- Move Dev environment to ECS EC2 approach. I allow to use spot istances instead of FARGATE compute.

3. Reliability and Performance Improvements

- Adopt Multi-AZ deployments for critical services like RDS and ECS to enhance fault tolerance and ensure continuous availability.

- Establish robust backup and disaster recovery plans, including the regular testing of these strategies to confirm recovery objectives are met.

- Expand the use of Auto Scaling to automatically adjust resources in response to changing demand, thus improving operational efficiency and cost-effectiveness.
- Conduct regular performance audits to identify bottlenecks and optimize configurations accordingly.

4. Networking Improvements

- Segregate production and non-production environments into separate VPCs or accounts to enhance security and reduce the risk of accidental exposure or data leakage.
- Utilize AWS PrivateLink to securely connect services across different environments.
- Implement Route 53 for DNS management and health checks to ensure high availability and resilience of domain name system services.
- Connectivity
- Review and enhance the security of bastion hosts, ensuring they have the minimal necessary access rights and are monitored effectively.

5. Data Management Improvements

- Expand lifecycle policies to all applicable S3 buckets for automated data archiving and expiration, reducing costs and improving data lifecycle management.
- Regularly test backups for all critical data, not just RDS, to ensure they meet recovery objectives.

By addressing these areas, the AWS infrastructure can achieve better security, performance, and cost efficiency, while also enhancing overall reliability and compliance.