Logging, Monitoring, and Audit Trails

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Data Retention Policies

What are your data retention policies for logs and monitoring data?

How long do you retain logs, and what is the process for archiving or deleting old logs?

2.How do you control access to your logging and monitoring tools?

Are there specific roles and permissions defined for accessing logs and monitoring dashboards?

3. Incident Response

How do your logging and monitoring systems support your incident response process?

Do you have automated alerts and notifications set up for critical incidents?

4. Log Aggregation and Centralization

How are logs aggregated and centralized from different sources (e.g., application logs, infrastructure logs, network logs)?

Do you use a centralized logging platform or multiple logging solutions?

5. Compliance and Regulatory Requirements

How do you ensure that your logging and monitoring practices comply with relevant regulatory requirements and industry standards?

Are there any specific compliance frameworks (e.g., GDPR, HIPAA) that you adhere to in your logging and monitoring processes?

6. Log Encryption and Security

Are your logs encrypted both in transit and at rest?

What security measures are in place to protect the integrity and confidentiality of your logs?

7. Scalability and Performance

How do you ensure that your logging and monitoring infrastructure scales with your application and user growth?

Have you encountered any performance bottlenecks in your current logging and monitoring setup? If so, how have you addressed them?

8. Integration with Other Tools

How well do your logging and monitoring tools integrate with other tools and platforms in your environment (e.g., CI/CD pipelines, incident management tools)?

Are there any planned integrations to enhance your current logging and monitoring capabilities?

9. Real-time Monitoring and Dashboards

Do you have real-time monitoring and dashboards set up for critical metrics and logs?

API Gateway and Load Balancing:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. API Security

What measures are in place to secure API endpoints and prevent unauthorized access?

How do you handle API authentication and authorization?

2. Rate Limiting and Throttling

Do you implement rate limiting and throttling to prevent abuse of your APIs?

How do you ensure that rate limiting policies are enforced per tenant?

3. API Gateway Configuration and Management

What API gateway solution are you using (e.g., AWS API Gateway, Kong, NGINX)?

How do you manage and configure your API gateway for different environments (e.g., development, staging, production)?

4. Scalability and Performance

How do you ensure your API gateway and load balancers scale with increasing traffic?

What monitoring and performance metrics do you track to ensure optimal performance?

5. Health Checks and Failover

How do you configure health checks for your API endpoints and load balancers?

What is your failover strategy in case an API instance or load balancer fails?

6. Traffic Routing and Management

How do you handle traffic routing for different versions of your APIs (e.g., canary deployments, blue-green deployments)?

Do you use any traffic shaping or management techniques to prioritize certain types of traffic?

7. Logging and Monitoring

How do you log API requests and responses for monitoring and troubleshooting purposes?

What tools do you use for monitoring the health and performance of your API gateway and load balancers?

8. Latency and Response Time

How do you ensure low latency and quick response times for API requests?

What optimizations have you implemented to reduce latency?

9. Integration with CI/CD Pipelines

How do you integrate your API gateway and load balancers with your CI/CD pipelines?

Are there automated tests and deployments in place for your API infrastructure?

10. Documentation and Developer Experience

How do you provide API documentation and developer portals for your APIs?

What tools or platforms do you use to enhance the developer experience for consuming your APIs?

11. Error Handling and Retries

How do you handle errors and retries for API requests?

Are there specific strategies in place to handle transient errors and ensure request reliability?

12. Cross-Origin Resource Sharing (CORS)

How do you manage CORS policies for your APIs?

Are there specific configurations in place to handle cross-origin requests securely?

13. API Versioning

How do you manage different versions of your APIs?

What strategies do you use to deprecate old API versions and introduce new ones?

14. API Usage Analytics

How do you track and analyze API usage?

What metrics do you use to understand the usage patterns and performance of your APIs?

15. Cost Management

How do you manage and optimize the costs associated with your API gateway and load balancers?

Are there any cost-saving measures you have implemented or are considering?

Network Policy Enforcement, Latency

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Network Policy Enforcement:

1. Network Policy Management

• How do you manage and update your Kubernetes network policies?

• Are there automated tools or scripts in place to ensure consistency across clusters?

2. Security Auditing

• How do you audit your network policies to ensure they are correctly implemented and effective?

• Are there regular reviews or automated scans to identify potential policy violations or misconfigurations?

3. Traffic Encryption

• Is traffic between services within your cluster encrypted?

• How do you ensure encryption for traffic between tenants to prevent eavesdropping?

4. Third-Party Integrations

• How do you handle network policies for third-party integrations?

• Are there specific policies or configurations required for these integrations to ensure they comply with your security standards?

5. DDoS Protection

• What measures are in place to protect against Distributed Denial of Service (DDoS) attacks?

• How do you ensure that DDoS protection mechanisms do not interfere with legitimate tenant traffic?

Latency:

1. Latency Monitoring

• How do you monitor latency across your network and application components?

• Are there specific tools or dashboards in place to track and visualize latency metrics?

2. Latency Optimization

• What strategies are in place to optimize latency for your applications?

• Have you implemented any latency-reducing techniques such as lazy loading, caching, or data compression?

3. Latency in Multi-Region Deployments

• How do you handle latency in multi-region deployments?

• Are there specific configurations or optimizations in place to ensure low latency across different geographic regions?

4. Impact of Network Policies on Latency

• How do your network policies impact application latency?

• Are there any trade-offs between enforcing strict security policies and maintaining low latency?

5. Edge Computing

• Have you considered implementing edge computing to reduce latency?

• What are the potential benefits and challenges you foresee with edge computing in your environment?

6. Service Mesh Impact

• How does Istio or any other service mesh impact your overall latency?

• Are there specific configurations or optimizations within Istio to minimize latency?

7. Latency in CI/CD Pipelines

• How do you ensure that latency is minimized during the deployment process?

• Are there specific checks or tests in place to measure and optimize latency as part of your CI/CD pipelines?

8. Network Latency Analysis

• Do you perform regular network latency analysis to identify and address bottlenecks?

• What tools or methods do you use for detailed network latency analysis?

Additional Considerations:

1. Incident Response and Latency

• How does your incident response process address latency issues?

• Are there specific protocols in place to quickly identify and resolve latency-related incidents?

2. Quality of Service (QoS)

• Do you implement QoS policies to prioritize certain types of traffic?

• How do these policies impact latency for different tenants or applications?

Security

1. Security Configurations

• What security measures are in place for Amazon EKS, such as role-based access controls (RBAC) and encryption?

2. Audit and Monitoring

• What audit mechanisms are used to track and verify compliance with data isolation and security policies?

• How do you log and monitor access to the Kubernetes environment?

3. Vulnerability Management

• What processes are in place to identify and mitigate vulnerabilities within the Amazon EKS environment?

• How are vulnerabilities tracked and addressed, such as CVE management and software updates?