Observing Cloud Resources

*SRE Assessment Template*

# Categorize Responsibilities

| **Prometheus and Grafana Screenshots** | | |
| --- | --- | --- |
| Provide a screenshot of the Prometheus node\_exporter service running on the EC2 instance. Use the following command to show that the system is running: sudo systemctl status node\_exporter | | |
|  | | |
| **Host Metric**  **(CPU, RAM, Disk, Network)** | **Dashboard** | |
| *CPU* |  | |
| *Network* |  | |
| *RAM* |  | |
| *DISK IO* |  | |
| **Responsibilities** | | |
| 1. The development team wants to release an emergency hotfix to production. Identify two roles of the SRE team who would be involved in this and why. | | |
| * **TeamLead:** The Team lead is responsible for leading the response to an incident and coordinating the efforts of all teams involved. In the case of an emergency hotfix, the Incident Commander from the SRE team would take charge of the situation, ensuring that the hotfix is properly planned, executed, and monitored. They would work closely with the development team to understand the nature of the issue, assess the impact, and prioritize the fix. The Incident Commander would also communicate updates and progress to stakeholders, ensuring transparency and alignment throughout the process. * **Release Engineer**: The Release Engineer plays a crucial role in managing the deployment of software changes to production environments. In the case of an emergency hotfix, the Release Engineer from the SRE team would be responsible for ensuring a smooth and controlled release of the hotfix. They would work closely with the development team to package the fix, perform any necessary testing, and coordinate the deployment process. The Release Engineer would also monitor the deployment, verifying its success and addressing any issues that may arise during or after the release. | | |
| 2. The development team is in the early stages of planning to build a new product. Identify two roles of the SRE team that should be invited to the meeting and why. | | |
| * **System Architect**: The SRE Architect is responsible for designing the overall architecture of the system with a focus on reliability, scalability, and performance. They have a deep understanding of system design principles and can provide valuable insights into building a highly available and resilient product. By involving the SRE Architect in the early planning stages, the development team can benefit from their expertise in designing a system that can handle anticipated traffic loads, ensure fault tolerance, and meet the desired reliability goals. They can help identify potential architectural challenges, propose appropriate technologies, and guide the team in making informed decisions to build a robust product. * **Infrastructure Engineer**: The Infrastructure Engineer brings expertise in designing and implementing the underlying infrastructure required to support the new product. Additionally, the Infrastructure Engineer can provide insights into best practices for security, monitoring, and disaster recovery. They can help identify potential risks and suggest mitigation strategies to ensure the reliability and resilience of the infrastructure. | | |
| 3. The emergency hotfix from question 1 was applied and is causing major issues in production. Which SRE role would primarily be involved in mitigating these issues? | | |
| the SRE role primarily involved in mitigating the issues caused by the emergency hotfix would be the Team Lead. The Team Lead is responsible for responding to incidents, identifying the root cause, and taking appropriate actions to mitigate the impact and restore normal operations. They work closely with other SRE roles to troubleshoot and resolve the issues. It's important for the team lead to coordinate and communicate effectively with the rest of the team to ensure a swift and effective response to the incident. | | |

# 

# Team Formation and Workflow Identification

| **API Monitoring and Notifications** | | |
| --- | --- | --- |
| Display the status of an API endpoint: Provide a screenshot of the Grafana dashboard that will show at which point the API is unhealthy (non-200 HTTP code), and when it becomes healthy again (200 HTTP code). | | |
|  | | |
| Create a notification channel: Provide a screenshot of the Grafana notification which shows the summary of the issue and when it occurred. | | |
|  | | |
| Configure alert rules: Provide a screenshot of the alert rules list in Grafana. | | |
|  | | |

# 

# Applying the Concepts

| **Graph 1** | | |
| --- | --- | --- |
|  | | |
| 4a. Given the above graph, where does it show that the API endpoint is down? Where on the graph does this show that the API is healthy again? | | |
| *API endpoint is down at 3:27PM (second vertical dashed line) and healthy again at 3:35 PM (third vertical dashed line)* | | |
| 4b. If there was no SRE team, how would this outage affect customers? | | |
| * *Service Disruption: The API server acts as a gateway for customers to interact with the product or service. If the API server goes down, customers may experience a complete disruption in accessing the functionality provided by the product.* * *Loss of Functionality: The API server is responsible for processing requests and providing responses to customers. When it goes down, customers may lose access to specific functionalities or services that rely on the API server.* * *Data Inconsistency: If the API server is responsible for managing and storing data, a server outage can lead to data inconsistencies.* * *Reputation and Trust: A prolonged API server outage can damage the reputation and trust of the product or service provider.* | | |
| 4c. What could be put in place so that the SRE team could know of the outage before the customer does? | | |
| * Monitoring and Alerting: Implement a robust monitoring system that continuously tracks the health and performance of critical components in real-time. This includes monitoring metrics such as response time, error rates, and resource utilization. Set up alerts to notify the SRE team immediately when any predefined thresholds are breached or anomalies are detected. * Incident Management: Establish an incident management process that includes clear escalation paths and defined roles and responsibilities. When an incident occurs, ensure that the SRE team is promptly notified through automated alerting mechanisms. This can be achieved by integrating monitoring tools with incident management systems like PagerDuty or OpsGenie. * Automated Remediation: Implement automated remediation mechanisms that can detect and resolve common issues without human intervention. * Synthetic Transactions: Set up synthetic transactions or periodic health checks that simulate user interactions with the system. These transactions can be scheduled to run at regular intervals and verify the availability and functionality of critical components. If any issues are detected during these synthetic transactions, alerts can be triggered to notify the SRE team, allowing them to investigate and resolve the problem before customers are affected. | | |

| **Graph 2** | | |
| --- | --- | --- |
|  | | |
| 5a. Given the above graph, which instance had the increase in traffic, and approximately how many bytes did it receive (feel free to round)? | | |
| *Instance 10.0.0.68:9100 is the instance had increased in traffic, and about 3500 bytes then 4500 bytes received.* | | |
| 5b. Which team members on the SRE team would be interested in this graph and why? | | |
| * SRE Network Engineer: The SRE Network Engineer specializes in network infrastructure and performance. They would be particularly interested in network traffic graphs to monitor and analyze the flow of data within the system. By examining network traffic patterns, they can identify potential bottlenecks, congestion points, or anomalies that may impact the overall performance and reliability of the system. This information helps them optimize network configurations, troubleshoot issues, and ensure efficient network utilization. * SRE Incident Responder: The SRE Incident Responder is responsible for handling and responding to incidents in real-time. They would be interested in network traffic graphs to quickly identify any sudden changes or anomalies in network traffic that may indicate a potential incident or security breach. By monitoring network traffic graphs, they can detect any unusual patterns, investigate the root cause, and initiate appropriate incident response procedures to minimize the impact on the system and customers. | | |

# 

# 