LMOGC: Logging, Monitoring and Observability in Google Cloud

Course Code: LMOGC
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The ***Logging, Monitoring and Observability in Google Cloud*** training course teaches participants techniques for monitoring, troubleshooting, and improving infrastructure and application performance in Google Cloud.

Learn how to monitor, troubleshoot, and improve your infrastructure and application performance. Guided by the principles of Site Reliability Engineering (SRE), this course features a combination of lectures, demos, hands-on labs, and real-world case studies. In this course, you'll gain experience with full-stack monitoring, real-time log management and analysis, debugging code in production, and profiling CPU and memory usage.

SKILLS COVERED

This course teaches participants the following skills:

- Plan and implement a well-architected logging and monitoring infrastructure
- Define Service Level Indicators (SLIs) and Service Level Objectives (SLOs)
- Create effective monitoring dashboards and alerts
- Monitor, troubleshoot, and improve Google Cloud infrastructure
- Analyze and export Google Cloud audit logs
- Find production code defects, identify bottlenecks, and improve performance
- Optimize monitoring costs

WHO SHOULD ATTEND?

This class is intended for the following participants:

- Cloud architects, administrators, and SysOps personnel
- Cloud developers and DevOps personnel

PREREQUISITES

To get the most out of this course, participants should have:

- Google Cloud Platform Fundamentals: Core Infrastructure or equivalent experience
- Basic scripting or coding familiarity
- Proficiency with command-line tools and Linux operating system environments

MODULES

Module 1: Introduction to Google Cloud Monitoring Tools

- Understand the purpose and capabilities of Google Cloud operations-focused components: Logging, Monitoring, Error Reporting, and Service Monitoring
- Understand the purpose and capabilities of Google Cloud application performance management focused components: Debugger, Trace, and Profiler

Module 2: Avoiding Customer Pain

- Construct a monitoring base on the four golden signals: latency, traffic, errors, and saturation
- Measure customer pain with SLIs

- Define critical performance measures
- Create and use SLOs and SLAs
- Achieve developer and operation harmony with error budgets

Module 3: Alerting Policies

- Develop alerting strategies
- Define alerting policies
- Add notification channels
- Identify types of alerts and common uses for each
- Construct and alert on resource groups
- Manage alerting policies programmatically

Module 4: Monitoring Critical Systems

- Choose best practice monitoring project architectures
- Differentiate Cloud IAM roles for monitoring
- Use the default dashboards appropriately
- Build custom dashboards to show resource consumption and application load
- Define uptime checks to track aliveness and latency

Module 5: Configuring Google Cloud Services for Observability

- Integrate logging and monitoring agents into Compute Engine VMs and images
- Enable and use Kubernetes Monitoring
- Extend and clarify Kubernetes monitoring with Prometheus
- Expose custom metrics through code and with the help of OpenCensus

Module 6: Advanced Logging and Analysis

- Identify and choose among resource tagging approaches
- Define log sinks (inclusion filters) and exclusion filters
- Create metrics based on logs
- Define custom metrics
- Use Error Reporting to link application errors to Logging
- Export logs to BigQuery

Module 7: Monitoring Network Security and Audit Logs

- Collect and analyze VPC Flow logs and Firewall Rules logs.
- Enable and monitor Packet Mirroring.
- Explain the capabilities of Network Intelligence Center.
- Use Admin Activity audit logs to track changes to the configuration or metadata of resources.
- Use Data Access audit logs to track accesses or changes to user-provided resource data.
- Use System Event audit logs to track GCP administrative actions.

Module 8: Managing Incidents

- Define incident management roles and communication channels
- Mitigate incident impact
- Troubleshoot root causes
- Resolve incidents
- Document incidents in a post-mortem process

Module 9: Monitoring Network Security and Audit Logs

- Collect and analyze VPC Flow logs and Firewall Rules logs.
- Enable and monitor Packet Mirroring.
- Explain the capabilities of Network Intelligence Center.
- Use Admin Activity audit logs to track changes to the configuration or metadata of resources.

- Use Data Access audit logs to track accesses or changes to user-provided resource data.
- Use System Event audit logs to track GCP administrative actions.

Module 10: Optimizing Stackdriver Costs

- Understand Stackdriver billing
- Analyze Stackdriver resource utilization
- Implement best practices for Stackdriver cost control

END OF PAGE