Dynatrace Day 4: Advanced Monitoring & Integration – Detailed Notes

# 26. Network Monitoring

Dynatrace provides insights into the network layer to understand dependencies and identify latency or bandwidth bottlenecks.  
  
- Flow Analysis and Traffic Inspection:  
 - Monitors traffic between processes, services, and external endpoints.  
 - Visualizes packet flow direction and volume using Smartscape and service flow.  
 - Detects dropped packets, retransmissions, and connection errors.  
  
 Example: A spike in TCP retransmissions between two services can indicate degraded performance or a flaky network link, which Dynatrace can trace back to affected service calls.  
  
- Network Dependencies and Latency Insights:  
 - Shows how network issues impact service response time.  
 - Enables drill-down into slow external service calls.  
 - Correlates network metrics with CPU/memory to pinpoint performance bottlenecks.  
  
 Diagram: Smartscape map showing services A → B → C with network latency arrows highlighting delay on link B → C.

# 27. Log Monitoring Using Dynatrace

- Log Ingestion Methods:  
 - OneAgent automatically collects logs from standard paths.  
 - Logs can be pushed from FluentD, AWS CloudWatch, Syslog, etc., using the log ingestion API.  
  
- Log Processing and Analytics:  
 - Supports dynamic parsing with DQL (Dynatrace Query Language).  
 - Create log metrics, dashboards, and anomaly detection rules.  
  
- Log Management Best Practices:  
 - Use tags to organize logs.  
 - Exclude noisy log types.  
 - Apply retention policies to control cost.  
  
 Example: Create a rule to monitor `ERROR` level log entries for all services tagged with `Environment=Production`.

# 28. Log Analytics

- Searching Logs and Extracting Fields:  
 - Filter logs using text search, regex, and DQL fields.  
 - Extract custom fields for grouping and metric conversion.  
  
- Building Log-Based Metrics and Alerts:  
 - Define metrics from log content (e.g., count of ERRORs).  
 - Set thresholds and trigger alerts when limits are breached.  
  
 Example: Extract "statusCode" from log lines and build a metric to monitor 5xx status codes per minute.

# 29. Diagnostic Tools

- Memory Dumps and CPU Sampling:  
 - Capture heap dumps for memory leak analysis.  
 - Perform CPU sampling to identify hotspots and long-running methods.  
  
- Thread and Heap Analysis:  
 - Visualize blocked or deadlocked threads.  
 - Analyze object allocation and GC pressure.  
  
- Problem Investigation with PurePath:  
 - Trace request lifecycle across services.  
 - Identify bottlenecks, errors, and abnormal behaviors.  
  
 Diagram: PurePath trace showing timing distribution across service A, DB, and external API with latency breakdown.

# 30. Reports & Alerts

- Custom Alerts and Problem Thresholds:  
 - Define static and dynamic rules on any metric.  
 - Leverage Davis AI for adaptive thresholds.  
  
- Alerting Profiles and Routing:  
 - Group alerts by severity, tag, or service.  
 - Route to email, Slack, ServiceNow, PagerDuty.  
  
- Scheduled and Ad Hoc Reports:  
 - Automate delivery of dashboards as PDFs.  
 - Export data from Data Explorer and DQL queries.  
  
 Example: Send weekly uptime and error reports to application owners.

# 31. Autosys Integration & Monitoring

- Use Cases for Autosys Monitoring:  
 - Monitor job execution time, failures, and scheduling delays.  
 - Correlate job failures with resource bottlenecks or application exceptions.  
  
- Job-Level Visibility and Correlation:  
 - Ingest Autosys logs and job status via APIs or log forwarding.  
 - Visualize impact on downstream services using PurePath.  
  
 Example: Job failure correlating with out-of-memory condition on the DB server.

# 32. Automation with APIs

- Configuration API Overview:  
 - Manage alerting profiles, management zones, dashboards, tags, and monitors.  
 - CRUD operations for environments and entities.  
  
- Automating Tagging, Dashboarding, Alerting:  
 - Auto-apply tags based on metadata.  
 - Create dashboards and alert rules via CI/CD scripts.  
 - Use Terraform or Ansible for infrastructure-as-code workflows.  
  
 Example: Use GitHub Actions to apply updated dashboards to all staging environments nightly.

# 33. Extending Dynatrace

- Custom Extensions (SDK):  
 - Use Extension Framework 2.0 for monitoring custom devices, protocols.  
 - Create plugin scripts to ingest data not natively supported.  
  
- Integration with Third-Party Systems:  
 - ServiceNow: CMDB sync, incident and event creation.  
 - Splunk: Export events or logs to SIEM.  
 - Prometheus/Grafana: Ingest metrics or visualize Dynatrace data externally.  
  
 Diagram: Architecture showing Dynatrace sending incidents to ServiceNow and metrics to Grafana.