INFOSOFT IT SOLUTIONS

Training | Projects | Placements

ELASTIC STACK [ELK]

Introduction to Elastic Stack

- Overview of Elastic Stack components (Elasticsearch, Logstash, Kibana)
- Use cases and benefits of Elastic Stack

Elasticsearch

- Introduction to Elasticsearch
- Installation and setup
- Basic concepts: Index, Type, Document, Shard, Replica
- CRUD Operations
- Query DSL (Domain Specific Language)
- Aggregations and Analytics
- Index management and optimization

Logstash

- Introduction to Logstash
- Installation and configuration
- Data ingestion techniques
- Filters and plugins

Kibana

- Introduction to Kibana
- Installation and setup
- Visualization and dashboard creation
- Discovering and exploring data
- Search and filter capabilities
- Timelion for time series data

Beats

- Overview of Beats (Filebeat, Metricbeat, etc.)
- Installation and configuration
- Data shipping and monitoring
- Use cases and integration with other Elastic Stack components

Advanced Topics

- Scaling Elasticsearch clusters
- Security and authentication
- Monitoring and alerting

Advanced Elasticsearch

- Data modeling and schema design
- Advanced query optimizations
- Index lifecycle management (ILM)
- Cross-cluster search and federated search
- Resiliency and fault tolerance strategies

Advanced Logstash

- Advanced filtering techniques (grok patterns, conditionals)
- Performance tuning and pipeline optimizations
- Handling complex data transformations
- Using plugins for custom integrations
- Scaling Logstash for high-volume data pipelines

Advanced Kibana

- Custom plugin development
- Canvas for creating custom visualizations
- Vega and Vega-Lite visualizations
- Timelion scripting for advanced time series analysis
- Dashboard embedding and reporting

Beats and Advanced Data Shipping

- Creating custom Beats modules
- Integrating with cloud services (AWS, GCP, Azure)
- Monitoring infrastructure and application metrics
- Using Beats for security event collection (Filebeat, Auditbeat)

Security and Compliance

- Securing Elasticsearch clusters (SSL/TLS, authentication)
- Role-based access control (RBAC) and permissions
- Audit logging and compliance reporting
- Implementing GDPR and CCPA compliance

Machine Learning with Elastic Stack

- Introduction to machine learning in Elastic Stack
- Anomaly detection and forecasting
- Integrating machine learning jobs with Kibana
- Real-time analytics and alerting with machine learning

Advanced Cluster Management

- Multi-cluster management with Elastic Cloud Enterprise (ECE)
- Cross-cluster replication (CCR) for disaster recovery
- Performance monitoring and optimization
- Advanced shard allocation and rebalancing strategies

DevOps and CI/CD Integration

- Using Elastic Stack in DevOps pipelines
- Continuous delivery of configuration changes
- Automated testing and validation with Elastic Stack
- Integrating with CI/CD tools like Jenkins, GitLab CI

Real-time Data Ingestion and Processing

- Building real-time data pipelines with Elasticsearch
- Handling streaming data with Beats and Logstash
- Processing IoT data and sensor data streams
- Benchmarking and optimizing real-time ingestion