AWS Advanced Topics and Best Practices

By Aditya Putra

me@adityaputra.com
https://github.com/adityaputra/praktisimengajar-cloudcomputing

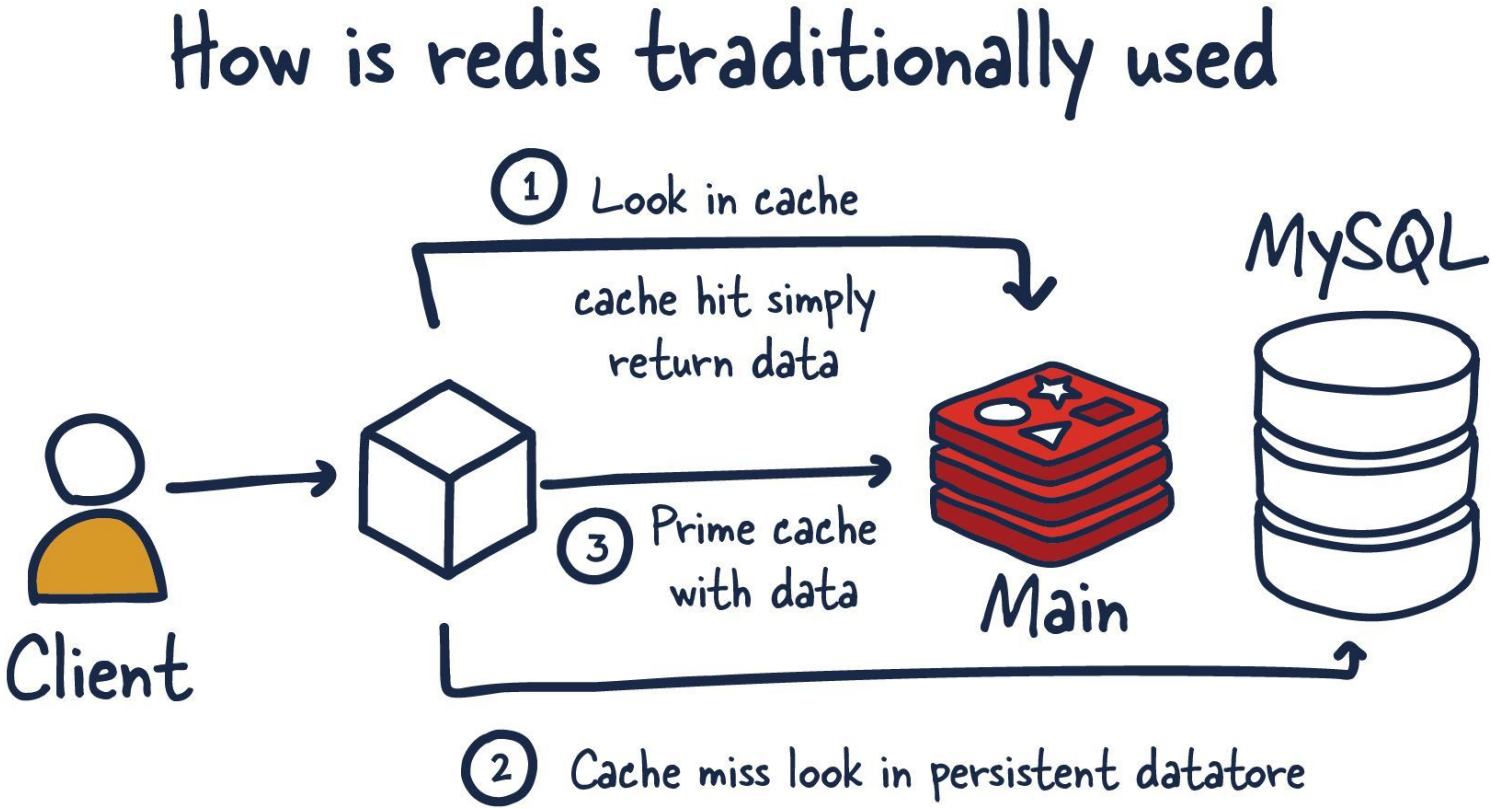
What we’re learning today

- AWS Elasticache, OpenSearch, ElasticSearch
- Logs and metrics aggregation
- IaC: Terraform and AWS CloudFormation
- CI/CD: Github actions and AWS CodeDeploy
- Best practices for cost optimization and security in the cloud

AWS Elasticache

- Fully managed, in-memory data caching service
- Supports Redis and Memcached caching engines
- Improves application performance and scalability
- Offloads database workload and reduces latency
- Accelerates response times and scales applications
- Features automatic data replication for durability
- Integrates with AWS services for seamless integration
- Provides security with encryption and access control
- Enhances user experience and reduces database load

Cache engine



AWS OpenSearch / ElasticSearch

- Managed service for Elasticsearch
- Distributed search and analytics engine
- Scalable and near real-time data analysis
- Ingest, index, and search large volumes of data
- Seamless integration with AWS services
- Automatic scaling and high availability
- Powerful search queries and data visualization
- Extensible with plugins and customization options
- Commonly used for log analytics and monitoring
- Simplifies deployment and management

Logs

Logs refer to textual records of events, activities, and errors generated by applications, operating systems, and other components. They contain valuable information for understanding system behavior, diagnosing problems, and auditing activities.

Metrics

Metrics are quantitative measurements of system performance, resource utilization, and other relevant data points. They provide a numerical representation of system behavior and help track trends, identify anomalies, and trigger alerts.

Showcase

Logs and Metrics Aggregation

Logs and metrics aggregation is a critical aspect of monitoring and managing the health and performance of systems, applications, and infrastructure.

Collecting, centralizing, and analyzing logs and metrics from various sources to gain insights, troubleshoot issues, and optimize performance.

Tools for logs and metric aggregation

- AWS CloudWatch
- Newrelic
- Datadog
- Elasticsearch, Logstash, Kibana, Prometheus, Grafana

Showcase

IaC: Infrastructure as Code

IaC is a methodology for managing and provisioning infrastructure resources through machine-readable definition files, rather than manual configuration.

It enables the automation and versioning of infrastructure deployment, making it repeatable, consistent, and easily manageable.

Benefits of IaC

- Automates infrastructure provisioning
- Treats infrastructure as software
- Eliminates manual errors
- Enables version control and collaboration
- Tools: AWS CloudFormation, Terraform, Ansible
- Fast, consistent, and scalable deployments
- Benefits: speed, reproducibility, scalability
- Supports DevOps practices
- Improves infrastructure management

Common tools

- Terraform
- Ansible
- AWS CloudFormation

Write

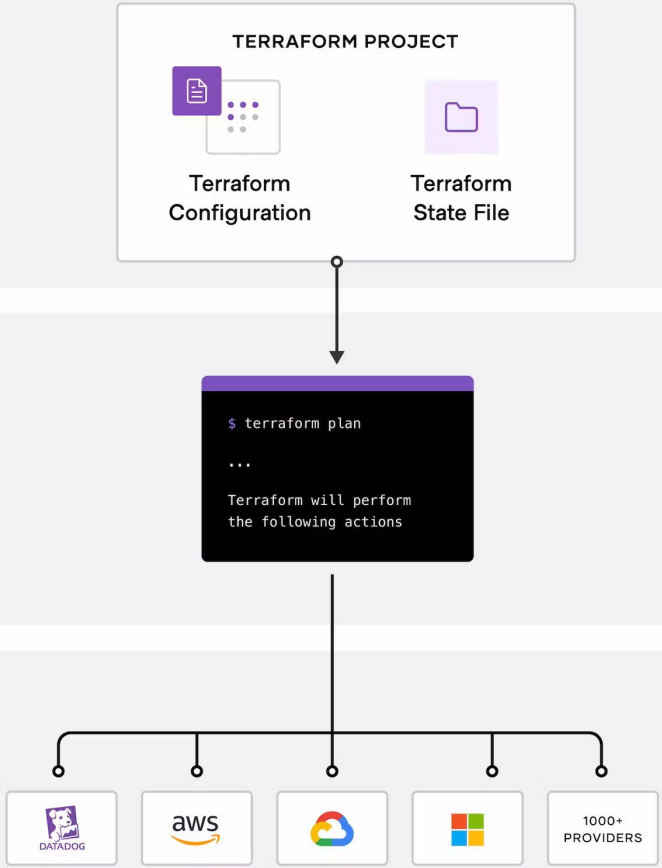
Define infrastructure in configuration files

Plan

Review the changes Terraform will make to your infrastructure

Apply

Terraform provisions your infrastructure and updates the state file.



Demo

AWS cost optimization

- Monitor and analyze costs regularly.
- Right-size resources based on workload needs.
- Utilize reserved instances or savings plans.
- Consider spot instances for non-critical workloads.
- Implement auto-scaling for dynamic resource allocation.
- Leverage serverless computing for pay-as-you-go pricing.
- Optimize cloud storage by deleting unused data and using lower-cost tiers.
- Use reserved capacity for services like databases.
- Implement cost tagging for accurate cost allocation.
- Continuously review and optimize cloud architecture and usage.

AWS security best practices

- Use strong IAM controls and least privilege access.
- Secure network traffic and apply encryption.
- Implement robust monitoring and logging.
- Regularly apply security patches and updates.
- Follow secure coding practices and perform security testing.
- Establish backup and disaster recovery procedures.
- Conduct security audits and ensure compliance.
- Develop an incident response plan.
- Provide security education and awareness.
- Maintain ongoing vigilance and stay informed about emerging threats.

Questionnaire

https://forms.gle/nFc4wdypwmxBhyTA7

What will we do next?

Let’s keep in touch and good luck for your IT career!