Best Practices for Operating in the AWS Cloud

The AWS Well-Architected Framework Abbreviated

PINNACLE
SOLUTIONS, INC.

Rise to a Higher Level of Clarity | thepinnaclesolutions.com | 866.MOVE.FWD

General Design Principles

The Well-Architected Framework identifies a set of general design principles to facilitate good design in the cloud.

Stop guessing your capacity needs: Guessing capacity before deployment can mean expensive idle resources or limited capacity. Cloud computing allows you to use only needed capacity, and scale up and down automatically.

Test systems at production scale: Create a production-scale test environment on demand, complete your testing, and then decommission the resources. Pay only during usage, making testing a fraction of the cost.

Automate to make architectural experimentation easier: Create and replicate systems at low cost, without manual effort. Track changes, audit impact, and revert parameters.

Allow for evolutionary architectures: Automation and testing on demand lowers the risk of impact from design changes so that businesses can take advantage of innovations as a standard practice.

Drive architectures using data: Collect data to learn how your architectural choices affect the behavior of your workload so you can improve your architecture choices.

Improve through game days: Host game days simulating events in production to reveal where improvements can be made and develop organizational experience in dealing with events.

1 Operational Excellence

Design Principles

Best practices involve the ability to run and monitor systems to deliver business value and improve supporting processes and procedures.

Perform operations as code: Define operations procedures as code and automate execution of procedures by triggering them in response to events. This limits human error and enables consistent responses to events.

Annotate documentation: Automate the creation of annotated documentation after every build. This documentation can be used by people and systems, and can act as an input to your operations code.

Make frequent, small, reversible changes: Design workloads to allow regular updates to components, and make changes in small increments that can be reversed.

Refine operations procedures frequently: Look for opportunities to improve and evolve your operations procedures with your workload. Regularly review and validate the effectiveness of all procedures and ensure teams are familiar with them.

Anticipate failure: Perform “pre-mortem” exercises to identify potential sources of failure and understand their impact. Test your response procedures to ensure they’re effective and teams are familiar with their execution.

Learn from all operational failures: Share lessons learned across teams and the organization to drive improvement.

Prepare. Operate. Evolve.

Effective preparation establishes shared goals and common standards for workload design and management and is key to operational excellence and business success. Design workloads with mechanisms to monitor and gain insight into application, platform, and infrastructure components. Validate that workloads, or changes, are ready to be moved to production and that there are sufficient trained personnel to effectively support the workload. Prepare for events and failures and test response procedures.

Successful operation is measured by achievement of business and customer outcomes. Define expected outcomes and metrics used to measure success. Establish baselines and then collect and analyze your metrics to determine operations success and how it changes over time. Operational excellence also requires efficient and effective management of both planned and unplanned operational events. Routine operations and responses to unplanned events should be automated.

Evolution is required to sustain operational excellence. Successful evolution of operations is founded in: frequent small improvements; providing safe environments and time to experiment, develop, and test improvements; and environments in which learning from failures is encouraged.

Key AWS Services

Prepare: AWS Config and AWS Config rules can be used to create standards for workloads and to determine if environments are compliant with those standards before being put into production.

Operate: Amazon CloudWatch allows you to monitor the operational health of a workload.

Evolve: Amazon Elasticsearch Service (Amazon ES) allows you to analyze your log data to gain actionable insights quickly and securely.

2

Security

Design Principles

Best practices involve the ability to protect systems, information, and assets, and deliver business value through risk assessments and mitigation strategies.

Implement a strong identity foundation: Use the principle of least privilege, enforce separation of duties, and centralize privilege management.

Enable traceability: Monitor, alert, and audit actions and changes in real time. Integrate logs and metrics with systems to automatically respond and take action.

Apply security at all layers: Apply a defense-in-depth approach with security controls at all layers.

Automate security best practices: Automated security mechanisms allow you to securely scale. Define and manage secure architectures as code in version-controlled templates.

Protect data in transit and at rest: Classify your data into sensitivity levels and use encryption, tokenization, and access control.

Keep people away from data: Reduce the need for direct access or manual processing of data to lessen the risk of loss or modification of sensitive data.

Prepare for security events: Run incident response simulations and use automation tools to increase your detection, investigation, and recovery speed.

Manage. Protect. Respond.

Identity and access management are key parts of an information security program. Use granular policies and enforce strong password practices, such as avoiding re-use, and multi-factor authentication. Do not share credentials, and grant user access with a least-privilege approach.

Detective controls are an essential part of governance frameworks and can be used to support a quality process, a legal or compliance obligation, and for threat identification and response efforts. It is critical that you analyze logs and respond to them so you can identify potential security threats and take appropriate action.

Your infrastructure protection should include multiple layers of defense including: boundary protection, monitoring points of ingress and egress, and comprehensive logging, monitoring, and alerting.

Data protection practices such as data classification and encryption help protect data by providing a way to categorize data based on levels of sensitivity and rendering data unintelligible to unauthorized access.

It’s also essential to implement and practice procedures to respond to and mitigate the potential impact of security incidents. You should also automate the isolation of instances and the capturing of data and state for forensics.

Key AWS Services

Identity and Access Management: IAM, MFA, and AWS Organizations enable you to control access and centrally manage and enforce policies for multiple AWS accounts.

Detective Controls: AWS CloudTrail, AWS Config, Amazon GuardDuty, and CloudWatch monitor your resources and configurations for malicious or unauthorized behavior, and can trigger responses with CloudWatch Events.

Infrastructure Protection: Amazon VPC, CloudFront, AWS Shield, AWS WAF, and Application Load Balancer securely deliver and protect data and applications.

Data Protection: Amazon ELB, EBS, S3, and RDS, Macie, and AWS KMS classify and protect data in transit and at rest.

Incident Response: Create a clean environment for investigations and trigger automated responses with AWS CloudFormation and CloudWatch Events.

3 Reliability

Design Principles

Best practices involve the ability to recover from and mitigate infrastructure or service disruptions, and dynamically acquire compute resources for demand.

Test recovery procedures: Use automation to simulate failures or recreate scenarios that previously led to failures to expose failure pathways that you can rectify before a real failure scenario.

Automatically recover from failure: Monitoring key performance indicators allows you to trigger automatic notifications and tracking of failures when a threshold is breached. Automated recovery processes can work around or repair a failure. Sophisticated automation allows you to anticipate and remediate failures before they occur.

Scale horizontally to increase aggregate system availability: Replace one large resource with multiple small resources to reduce the impact of a single failure on the overall system. Distribute requests among resources to ensure they don’t share a common point of failure.

Stop guessing capacity: Monitor demand and system utilization and automate addition and removal of resources to maintain the optimal level to satisfy demand without over- or under-provisioning.

Manage change in automation: Changes that need to be managed are changes to automation. Changes to infrastructure should be automated.

Foundations. Change Management. Failure Mangagement.

AWS has most foundational requirements already incorporated. Because the cloud is designed to be limitless, AWS fulfills the requirement for sufficient networking and compute capacity, leaving you free to change resource size and allocation. AWS does set service limits to protect you from over-provisioning resources, and you need to have processes in place to monitor and change these limits to meet your business needs. If you are using a hybrid model, it's important to have a design for how your AWS and on-premises resources will interact as a network topology.

When you are aware of how change affects a system, you can proactively plan and quickly identify trends that could lead to capacity issues or SLA breaches. With AWS, you can monitor the behavior of a system and automate the response to changes in demand, increasing reliability. Monitoring can alert your team when KPIs deviate from expected norms, and automatic logging of changes allows you to audit and quickly identify actions that might have impacted reliability.

In any system of reasonable complexity, failures will occur. With AWS, when a metric crosses a threshold you can trigger an automated action to remedy the problem. You can also replace a failed resource with a new one and carry out analysis on the failed resource out of band.

Key AWS Services

Foundations: AWS IAM, Amazon VPC, AWS Trusted Advisor, and AWS Shield enable you to control access, see into service limits, and safeguard web applications on AWS.

Change Management: Use AWS CloudTrail, AWS Config, Amazon Auto Scaling, and Amazon CloudWatch to record and adjust your resources and configurations.

Failure Management: AWS CloudFormation, Amazon S3, Amazon Glacier, and AWS KMS provide everything from templates to create and provision resources to storage and management capabilities.

4

Performance Efficiency

Design Principles

Best practices involve the ability to use computing resources efficiently, and to maintain that efficiency as demand and technologies change.

Democratize advanced technologies: Rather than having your IT team learn how to host and run a new technology, simply consume it as a service. This keeps your team focused on product development instead of resource provisioning and management.

Go global in minutes: Provide lower latency and a better customer experience at minimal cost by deploying your system in multiple Regions around the world in a few clicks.

Use serverless architectures: Remove the need to run and maintain servers to carry out traditional compute activities, eliminating the operational burden of servers and lowering transactional costs.

Experiment more often: Virtual and automatable resources allow you to quickly carry out comparative testing using different types of instances, storage, and configurations.

Mechanical sympathy: Use the technology approach that aligns best to what you are trying to achieve.

Selection. Review. Monitoring. Tradeoffs.

Well-architected systems use multiple solutions and enable different features for optimal performance. The wrong solution and features can lead to lower performance.

The optimal compute solution depends on design, usage patterns, and configuration settings. Take advantage of elasticity mechanisms to ensure your solution is scalable. The optimal storage solution depends on access method, patterns of access, throughput required, access and update frequency, and availability and durability constraints.

The optimal database solution depends on requirements for availability, consistency, partition tolerance, latency, durability, scalability, and query capacity. The optimal network solution varies depending on latency, throughput reqirements, and location.

Review your architecture's performance-constraints so you can look for new releases that alleviate these constraints. Monitor your architecture so you can proactively remediate issues. When thresholds are breached, an alarm should trigger an automated action to work around badly performing components. Test your alarm solution to ensure it correctly recognizes issues.

Actively consider tradeoffs - such as consistency, durability, and space for time and latency - to optimize performance.

Key AWS Services

Selection:
Compute - Auto Scaling is key to ensuring you have enough instances to meet demand and maintain responsiveness. *Storage* - Use Amazon EBS and S3 to store and securely transfer files. *Database* - Amazon RDS and Amazon DynamoDB allow you to optimize for your use case. *Network* - Use Amazon Route 53, Amazon VPC, and AWS Direct Connect for latency-based routing and reduced network distance or jitter.

Review: Find new updates on AWS Blog and What's New.

Monitoring: Integrate your monitoring solution with Amazon CloudWatch and trigger actions with AWS Lambda.

Tradeoffs: Improve performance and read replicas with ElastiCache, CloudFront, AWS Snowball, and Amazon RDS.

5 Cost Optimization

Design Principles

Best practices involve the ability to run systems to deliver business value at the lowest price point.

Adopt a consumption model: Pay only for the computing resources that you require and increase or descrease usage depending on business requirements.

Measure overall efficiency: Measuring the business output of the workload and delivery costs will help you monitor the gains made from increasing output and reducing costs.

Stop spending money on data center operations: AWS does the heavy lifting of racking, stacking, and powering servers, allowing you to focus on your customers and projects instead of infrastructure.

Analyze and attribute expenditure: The cloud makes it easier to identify the usage and cost of systems. IT costs can be attributed to individual workload owners, which helps measure return on investment and gives workload owners the opportunity to optimize their resources and reduce costs.

Use managed and application level services to reduce cost of ownership: Managed and application level services remove the operational burden of maintaining servers for tasks such as sending email or managing databases. The scale of the cloud puts these managed services at a lower cost per transaction.

Awareness. Balance. Optimization.

The ease of use and virtually unlimited on-demand capacity requires a new way of thinking about expenditures.

With AWS, you can accurately attribute costs to teams or individual product owners. This allows you to know which products are truly profitable so you can make more informed decisions about where to allocate budget.

Use Cost Explorer to track your spend and use AWS Budgets to get notifications of usage or costs that are not inline with your forecasts. You can set up billing alerts to notify you of predicted overspending.

You can use cost allocation tags to track cost and usage of cost centers, workloads, owners, and resources. Combining tags with entity lifecycle tracking can allow you to identify orphaned resources or projects that no longer generate value to your business.

Auto Scaling, demand, buffer, and time-based approaches allow you to automatically provision resources to match demand.

Continuously review your existing architectural decisions to ensure they are the most cost-effective. Assess how new services can help you save money, and decommission unneccessary resources, services, and systems.

Key AWS Services

Expenditure Awareness: AWS Cost Explorer and AWS Budgets monitors usage and spend.

Cost-Effective Resources: Use Cost Explorer, Amazon CloudWatch, Trusted Advisor, Amazon Aurora, AWS Direct Connect, and Amazon CloudFront to size resources, remove database licensing costs, and optimize data transfer.

Matching Supply and Demand: Use Auto Scaling to adjust resources with demand without overspending.

Optimizing Over Time: AWS Trusted Advisor inspects your environment and finds opportunities to save you money.

The Review Process

The architecture review process identifies any critical issues that might need addressing or areas that could be improved.

The review of architecture needs to be done in a consistent manner, with a blame-free approach. It should be a light-weight, conversational process. The outcome is a set of actions that should improve the experience of a customer using the workload.

Use the Well-Architected Framework to continually review architecture. This approach allows team members to update answers as the architecture evolves and improve the architecture as you deliver features.

Reviews should be applied at key milestones in the product lifecycle, early on in the design phase to avoid one-way doors - decisions that are hard or impossible to reverse - and before the go live date.

After a review, you should have a list of issues that you can prioritize based on your business context. Take into account the impact on day-to-day work of your team. Addressing issues early could free up time for creating business value.

As you carry out multiple reviews, you might identify thematic issues - i.e. one group of teams has clusters of issues in a particular pillar or topic. Look at all your reviews in a holistic manner and identify any mechanisms, training, or principle engineering talks that could help address those thematic issues.

Best Practices for Operating in the AWS Cloud

The AWS Well-Architected Framework Abbreviated

For more information on how Pinnacle Solutions can with your cloud journey, please contact us: thepinnaclesolutions.com/contact or call 317-423-9143.

PINNACLE SOLUTIONS, INC.