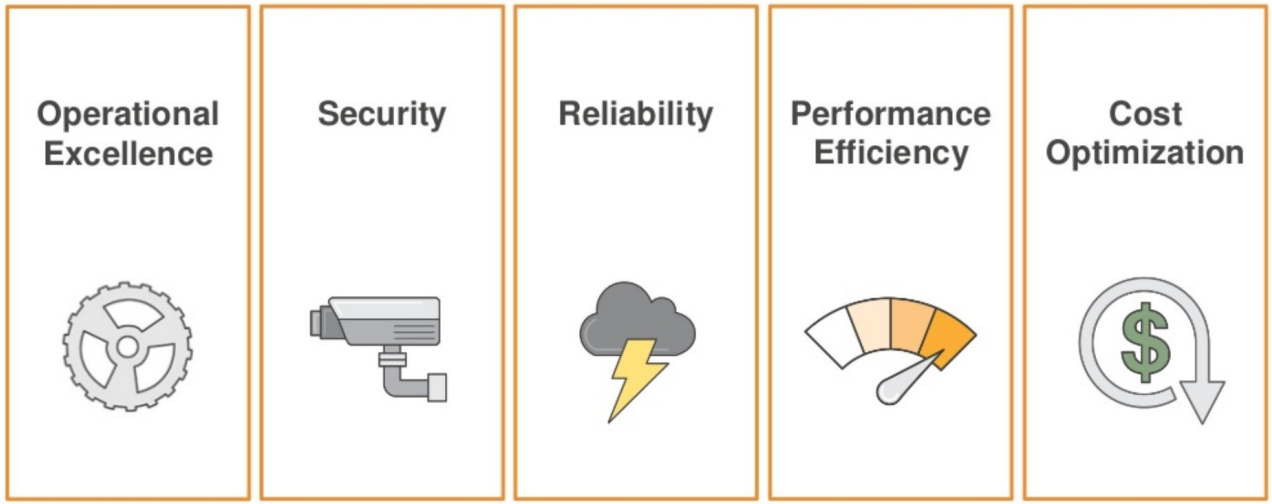
7.1 AWS Management Tools Overview

- Provisioning
  - AWS CloudFormation
  - AWS Service Catalog
  - Elastic Beanstalk
- Operations Management
  - AWS Systems Manager
  - AWS CloudTrail
  - AWS Config
- Configuration Management
  - AWS OpsWorks (Chef, Puppet)
- Monitoring and Logging
  - AWS CloudWatch

7.2 AWS Well Architected Framework

- Questions developed by AWS experts to helps customers analyze their environment
- The framework does not provide, implementation details, architectural patterns or relevant case studies
- The framework enables customers to:
  - Assess their environments against AWS best practices
  - Improve their infrastructure practices and deployments
  - Understand the business impact of architectural decisions

7.3 AWS Well Architected Framework Pillars



7.4 Operational Excellence:

- Align with business objectives
- Give alerts and respond to them in an automated manner
- Perform operations with code
- Make incremental changes
- Learn from failures
- Test for responses to unexpected events
- Document current procedures

7.5 Security

- Protect information, systems and assets
- Do risk assessments
- Have mitigation strategies
- Secure at all layers
- Enable traceability
- Implement a principle of least privilege
- Automate best practices

7.6 Reliability

- Automatically recover from infrastructure or service disruptions
- Scale horizontally to increase availability
- Use multiple availability zones
- Choose instance type based on application needs
- Stop guessing about capacity
- Test recovery procedures

7.7 Performance Efficiency

- Make efficient use of resources
- Enable latency-based routing
- Adopt latest technologies and architectures
- Experiment often

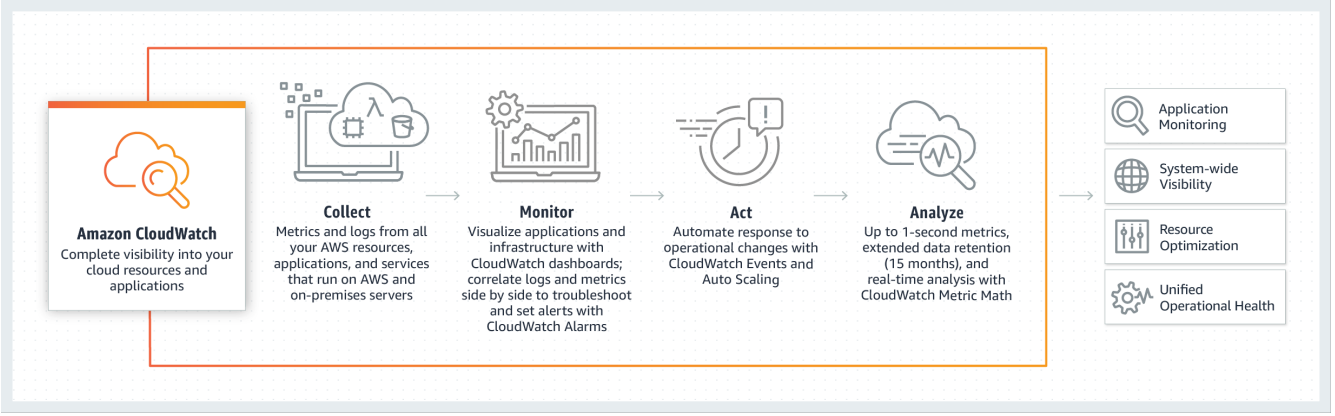
7.8 Cost Optimization

- Avoid unneeded costs
- Assess resource utilization
- Analyze and attribute expenditure
- Match supply and demand
- Optimize over time
- Delete unused resources
- Use consolidated billing, spot instances, and reserved instances
- Rightsize before/after migrations.

7.9 What is CloudWatch

- Amazon CloudWatch enables users to monitor their AWS resources and applications that run on AWS and/or on-premise servers
- CloudWatch collects monitoring and operational data in the form of logs, metrics, alarms, and events from AWS services, user and third party applications (e.g. Microsoft IIS server, MongoDB, Nginx, etc.)
- This service provides users with a unified view of enlisted AWS resources
- AWS CloudWatch documentation can be found here: https://docs.aws.amazon.com/cloudwatch

7.10 How CloudWatch Works



Source: AWS Documentation

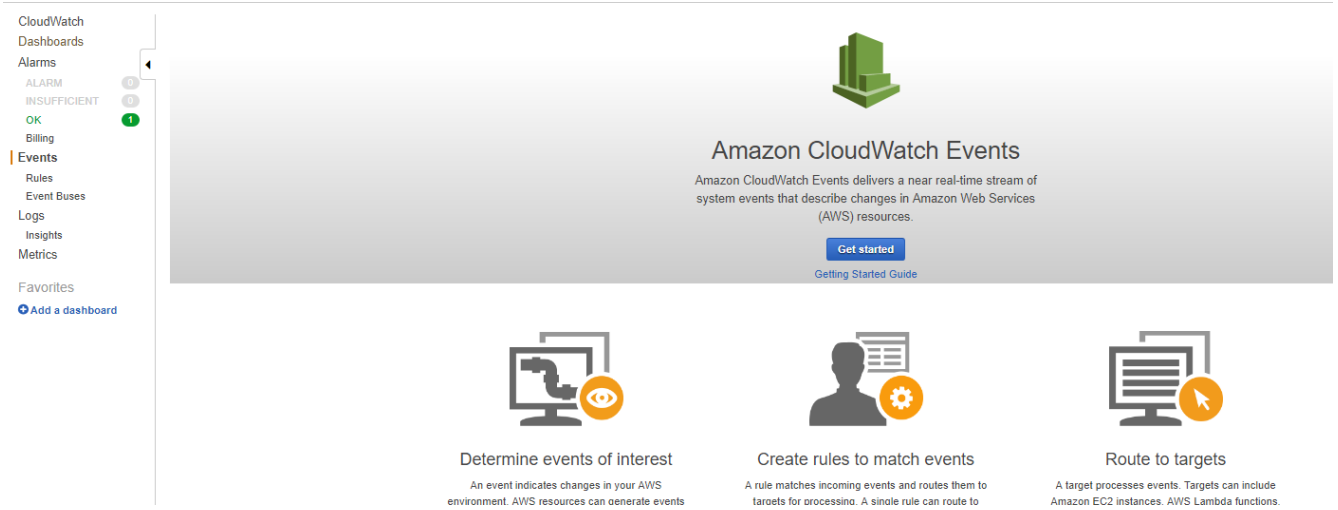
7.11 Use Cases

- Infrastructure monitoring and troubleshooting
  - Monitor key metrics and logs, visualize your application and infrastructure stack, create alarms, and correlate metrics and logs to understand and resolve root cause of performance issues
- Resource optimization
  - Use CloudWatch Alarms to automate capacity and resource planning through Auto Scaling
- Application monitoring
  - Trigger automated CloudWatch Alarms and Lambda workflows to improve customer experience
- Log analytics
  - Explore, analyze, and visualize your logs instantly to address operational issues and improve applications performance

7.12 Log Management

- CloudWatch as a log management solution offers users the following services:
  - Store log data from multiple sources in a central location
  - Enforce retention policy on those logs so they are available for a specific period
  - Offer a searching facility to look inside the logs for important information
  - Generate alerts based on metrics users define on the logs
    - Alerts can be sent off using the SNS service

7.13 Amazon CloudWatch in the AWS Management Console



7.14 CloudWatch AWS Services Integration

- CloudWatch is natively integrated with 70+ AWS services, including EC2, DynamoDB, S3, ECS, Lambda, CloudTrail, Amazon API Gateway, etc.
- Predefined metrics are generated and published at a minute interval
  - For a complete list of AWS Services and their CloudWatch metrics, visit https://amzn.to/2T6xm07

7.15 Monitoring EC2 Instances

- AWS EC2 users are automatically registered for Amazon CloudWatch and EC2 Basic Monitoring at no additional charge
- Users can upgrade to Detailed Monitoring when creating a new EC2 instance or for existing instances
- Amazon CloudWatch also automatically monitors metrics of
  - Elastic Load Balancers (EBS)
    - Request count and latency
  - EBS volumes
    - Read/write latency

7.16 Collecting Metrics and Logs from EC2 Instances and On-Premises Servers with the CloudWatch Agent

- CloudWatch Logs Agent can be installed manually or either through CloudFormation or Chef
- CloudWatch Agent, when installed on your EC2 or on-premise servers, enables you to do the following:
  - Collect system-level metrics from Amazon EC2 instances beyond standard metrics
  - Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS
  - Retrieve custom metrics from your applications or services using the **StatsD** and **collectd** protocols
    - StatsD is supported on both Linux and Windows
    - collectd is supported only on Linux servers
- For more details, visit https://amzn.to/2xtw722 and https://bit.ly/2mYhkaY

7.17 CloudWatch Alarms

- CloudWatch alarms enable users to set up system triggers to respond to specific events
- For example, you can set up Auto Scaling to add or remove EC2 instances in line with the inbound traffic profile
  - This elastic QoS can help optimize costs and improve resource utilization

7.18 Alarms in the AWS Management Console Examples

Source: AWS Documentation

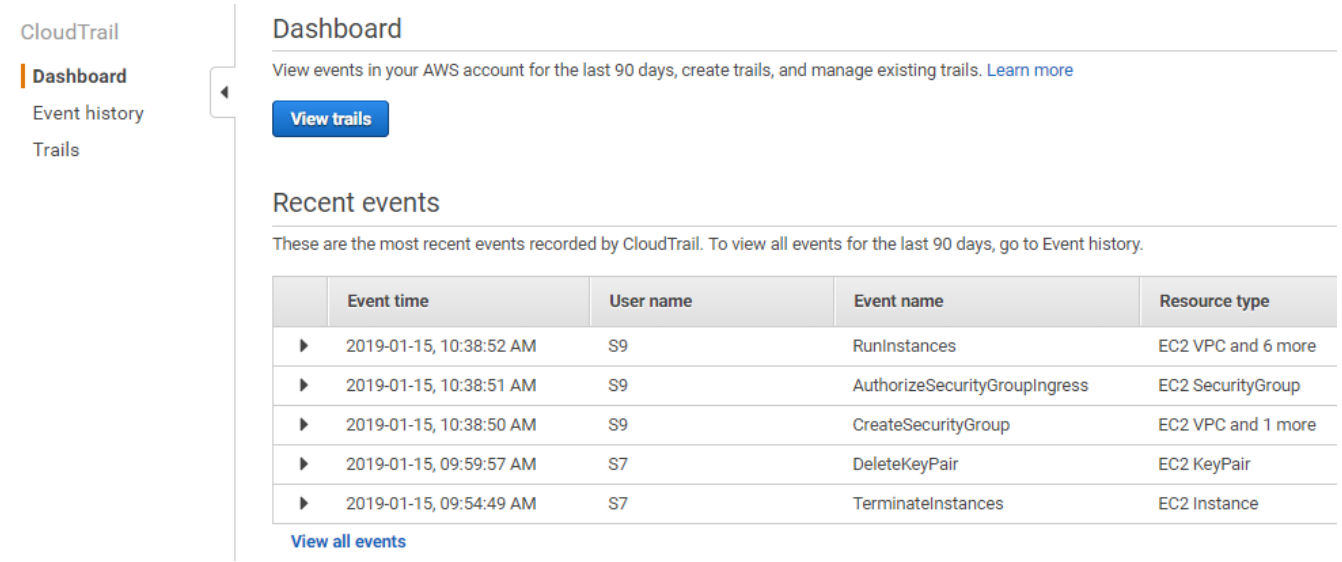
7.19 Amazon CloudWatch Events

- Through Amazon CloudWatch events you can respond to state changes in your AWS resources or when a particular threshold is exceeded
  - For example,
    - CloudWatch will provide monitoring of EC2 instances with respect of operational performance, including such metrics as CPU utilization, I/O operations, network traffic (in/out), and response latencies. It can also be configured to monitor HTTP status codes in Apache logs, etc.
    - CloudWatch generates an event when the state of an EC2 instance changes from pending to running or when Auto Scaling launches an instance
- For collecting custom log data, you need to install and configure CloudWatch agents that will be sending your logs to the CloudWatch Logs service and then create your specific metric filter there

7.20 AWS CloudTrail

- The AWS CloudTrail is a web service that enables governance, compliance, operational auditing, and risk auditing of user AWS accounts
- This service continuously monitors user activity and resource usage and provides visibility into related user actions across AWS infrastructure, AWS Management Console, API calls from AWS SDKs and CLI, etc.
- CloudTrail captures actions made directly by the user or on behalf of the user by an AWS service
- When a particular activity occurs in your AWS account, that activity is automatically recorded in event logs making event history available for subsequent security analysis, resource change tracking, troubleshooting, and incident investigations
  - The system, where applicable, records the source IP address and time from where the call related to the activity was made

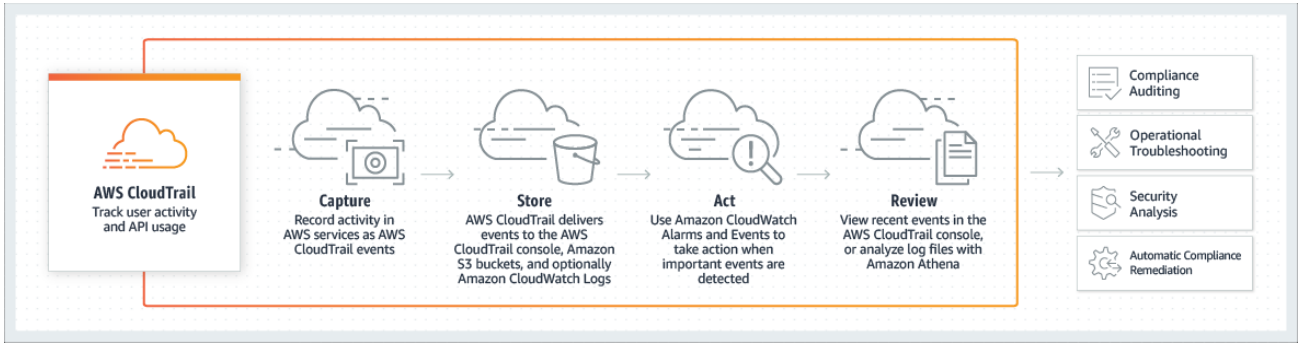
7.21 CloudTrail Dashboard in the AWS Management Console



7.22 CloudTrail Integration with CloudWatch

- CloudTrail is integrated with Amazon CloudWatch Logs for log data search
- Integration with CloudWatch Events service enables users to set up workflows triggered in response to events that can potentially pose security threat
  - An example of such an event is an attempt to make a private S3 bucket public

7.23 How CloudTrail Works



Source: AWS Documentation

7.24 CloudTrail Use Cases

- Compliance
  - CloudTrail dramatically simplified compliance audits for out-of-compliance events and fast responses to auditing requests
  - CloudTrail ensures compliance with internal policies and regulatory standards by providing a history of activity in your AWS account. For more information, visit https://bit.ly/2Reo6K4
- Security Analysis
  - You can analyze user behavior patterns by ingesting AWS CloudTrail events history into your log management and analytics solutions
- Data Exfiltration Detection (an act of unauthorized copying, transfer or retrieval of data)
  - Done via S3 object-level API events recorded in CloudTrail
  - You can also configure an action in response to such events using Amazon CloudWatch Events and AWS Lambda
- Operational Issue Troubleshooting
  - Done using AWS API call history produced by AWS CloudTrail
  - For example, you can quickly identify changes done to Amazon VPC security groups

7.25 Trusted Advisor

- AWS on-line expert service that can analyze you AWS environment and offers recommendations that can help you reduce cost, tighten security, increase performance, improve fault tolerance, and optimally provision resources following AWS best practices
- There are two tiers of Trusted Advisor service:
  - **Free** - available to all AWS customers
    - This type performs only core checks
  - **Business or Enterprise** - based on support plans

7.26 Trusted Advisor Dashboard

Recommended Actions

Security Groups - Specific Ports Unrestricted — *Refreshed: 2 minutes ago*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

140 of 291 security group rules allow unrestricted access to a specific port.

MFA on Root Account — *Refreshed: 2 minutes ago*
Previous status: Yellow

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

MFA is not enabled on the root account.

VPC Elastic IP Address — *Refreshed: 2 minutes ago*
Previous status: Green

Checks for usage that is more than 80% of the VPC Elastic IP Address Limit.

1 of 16 items have usage that is more than 80% of the service limit.

RDS Subnets per Subnet Group — *Refreshed: 2 minutes ago*
Previous status: Green

Checks for usage that is more than 80% of the RDS Subnets per Subnet Group Limit.

1 of 4 items have usage that is more than 80% of the service limit.

IAM Use — *Refreshed: 2 minutes ago*

7.27 Summary

- In this chapter, we reviewed the elements of AWS monitoring capabilities and ways to manage AWS resources and user applications