AWS Architecting and SysOps

Monitoring and Deploying AWS Resources, Part 1

June-July 2019

Contents

Amazon CloudWatch

Monitoring services and exploring metrics on AWS

Monitoring

Amazon CloudWatch

AWS Systems Manager

Amazon CloudTrail

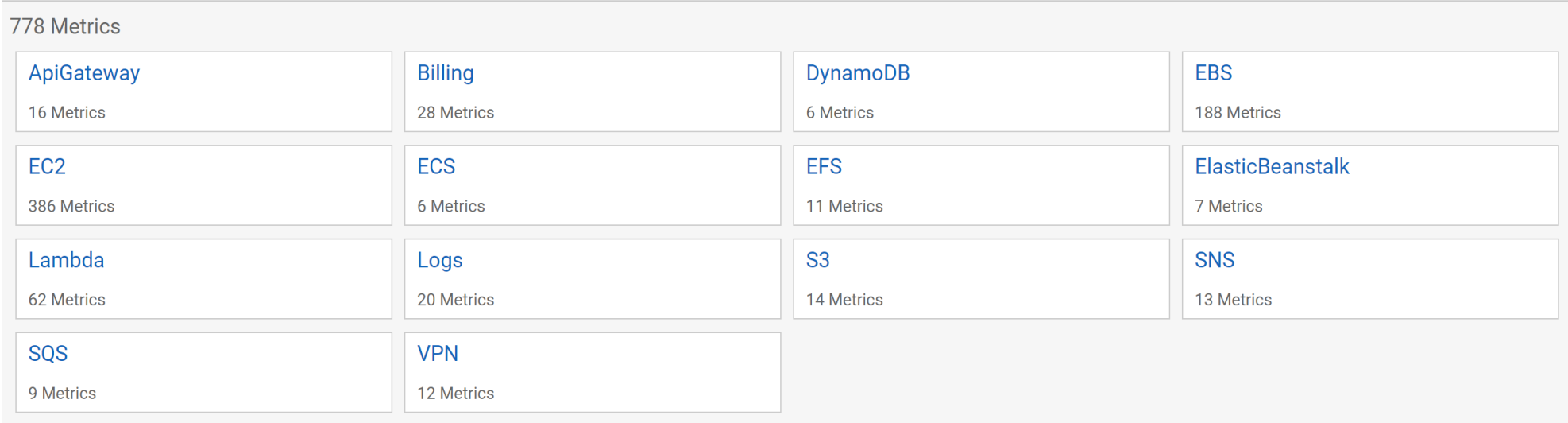
CloudWatch

- A monitoring and management service built for developers, system operators, site reliability engineers (SRE), an IT managers
- Provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health
- Collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers
- You can use CloudWatch to set high resolution alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to optimize your applications, and ensure they are running smoothly
- Easy to get started as you pay for what you use

CloudWatch metrics

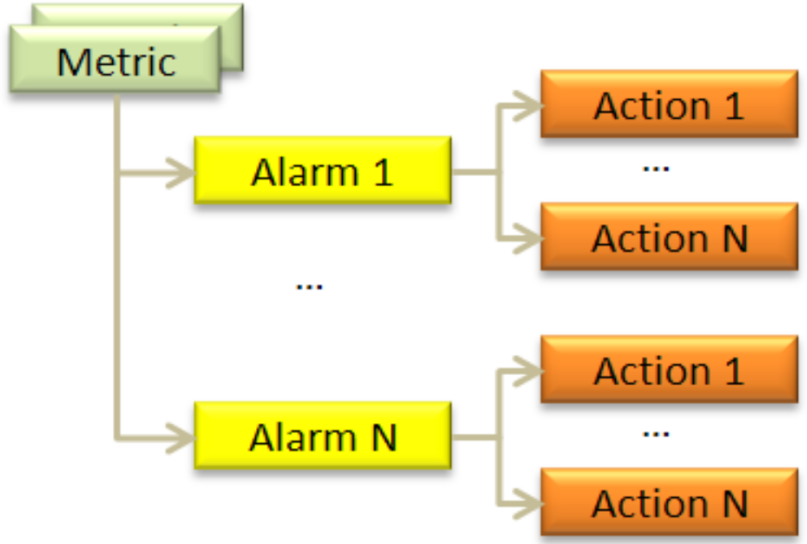
- Metrics are data about the performance of your systems
- By default, several services provide free metrics for resources
  - EC2 instances, EBS volumes, RDS DB instances
- You can also enable detailed monitoring some resources or publish your own application metrics
- CloudWatch loads all the metrics in your account for search, graphing, and alarms

➢ Metric data is kept for 15 months enabling you to view both up-to-the-minute data and historical data



CloudWatch alarms

- Allows you to watch metrics and to receive notifications when the metrics fall outside of the levels (high or low thresholds) that you configure
- You can attach multiple alarms to each metric and each one can have multiple actions
- The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods
- The action can be:
  - ✓EC2 action
  - ✓EC2 Auto Scaling action
  - ✓A notification sent to an SNS topic



CloudWatch alarms

- CloudWatch Alarm is always in one of three states

✓OK – the metric is within the range you have defined as acceptable

✓ALARM – when the metric breaches a threshold, it transitions to this state

✓INSUFFICIENT_DATA – when the data needed to make the decision is missing or incomplete

- CloudWatch alarms transitions between the 3 states depending on the metric

➢Important: CloudWatch does not

- ➢Test or validate the actions that you specify
- ➢Detects any error resulting from an attempt to invoke nonexistent actions

Make sure that your actions exist!!

CloudWatch dashboard

- CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, even those resources that are spread across different Regions
- You can use CloudWatch dashboards to create customized views of the metrics and alarms for your AWS resources
- With dashboards, you can create the following:
  - ✓ A single view for selected metrics and alarms to help you assess the health of your resources and applications across one or more regions
  - ✓ Select the color used for each metric on each graph, so that you can easily track the same metric across multiple graphs
  - ✓ An operational playbook that provides guidance for team members during operational events about how to respond to specific incidents
  - ✓ A common view of critical resource and application measurements that can be shared by team members for faster communication flow during operational events

CloudWatch logs

- Allow you to monitor and troubleshoot systems and applications using existing system, application, and custom log files
  - Monitor logs for specific phrases, values, or patterns
  - EC2 instances, CloudTrail events, and other sources like Lambda
- You can then retrieve the associated log data from CloudWatch logs
- The key is to install an small agent in each of the resources you want to monitor
- CloudWatch now includes an installable agent for all AWS OS at no additional charge

Use cases for CloudWatch logs

- Track the number of errors that occur in the application logs and send a notification whenever the rate of errors exceeds a specified threshold
  - Uses the log data for monitoring; no code changes required
- Monitor application logs for specific literal terms
  - such as “NullReferenceException”

  or something that may indicate that your application is having an issue
- Create alarms in CloudWatch and receive notifications of particular API activity as captured by CloudTrail
  - Use the notification to perform troubleshooting
- Store log data in highly durable storage
  - Change the log retention settings so that any log events older that this setting are automatically deleted

CloudWatch logs components

- CloudWatch log agents
  - Automated way to send log data to CloudWatch logs from EC2 instances
  - Agent components:
  - ✓A plugin to the CLI that pushes log data to CloudWatch logs
  - ✓A script (daemon) that initiates the process to push data to CloudWatch logs
  - ✓A cron job that ensures that the daemon is always running
- Log group
  - A group of log streams that share the same retention time, monitoring, and access control settings
  - Each log stream must belong to one log group

CloudWatch logs insights

- Fully managed, highly scalable, log analytics capabilities
- Debug operational issues by analyzing and visualizing your logs
- Fully integration with CloudWatch so you can gain full operational visibility
- Run fast and interactive queries at enterprise scale
  - Design to return results in seconds regardless of you log volume or query complexity
- Realtime insights provides you with the flexibility to scale your applications, find and solution operational issues quickly so you can continue to innovate rapidly
- You can have programmatic access using CLI, APIs, and SDKs

Logs insights: work with any log type

- Use logs from AWS services or on-premises applications
- Instantly query any log being sent to CloudWatch
- No setup required
- Automatic log field discovery:

1. Creates system fields for all logs:

✓@timestamp: time when the log event was added into CloudWatch
✓@message: the data row event as sent to CloudWatch
✓@logStream: name of the source that generated the log event

2. Automatically discovers additional log fields for logs coming from:

✓AWS services, such as Lambda, CloudTrail, Route 53, and VPC flow logs
✓Any application or custom log that produces log events in JSON format

Log insight queries

- Easy-to-learn query language with simple query commands
- Log insights offers in-product help via sample questions, command descriptions, and query autocompletion
- Query commands
  - fields: retrieve a list of files
  - filter: retrieve log events that match search criteria
  - stats: calculate aggregate statistics
  - sort: sort results based on a field in ascending or descending order
  - limit: retrieve a limited number of log events
  - parse: extra data from a log field, creating an ephemeral field
- Write queries with aggregations, filters, and regular expressions
  - ✓ Identify trends and patterns in your logs
  - ✓ Detect anomalies activities
  - ✓ Visualize query results and time series data
- Add results to CloudWatch dashboards

CloudWatch pricing

- Pricing, as usual, depends on the region and the services used
- Metrics
  - EC2 detailed monitoring
- APIs
  - Charged per number of statistics
- Dashboard
  - Price per dashboard / month
- Alarms
  - Standard of high resolution
- Logs
  - Only data transfer OUT at same price as EC2
- Events
  - Per million of events

More Monitoring Tools

Operational auditing and monitoring centralization

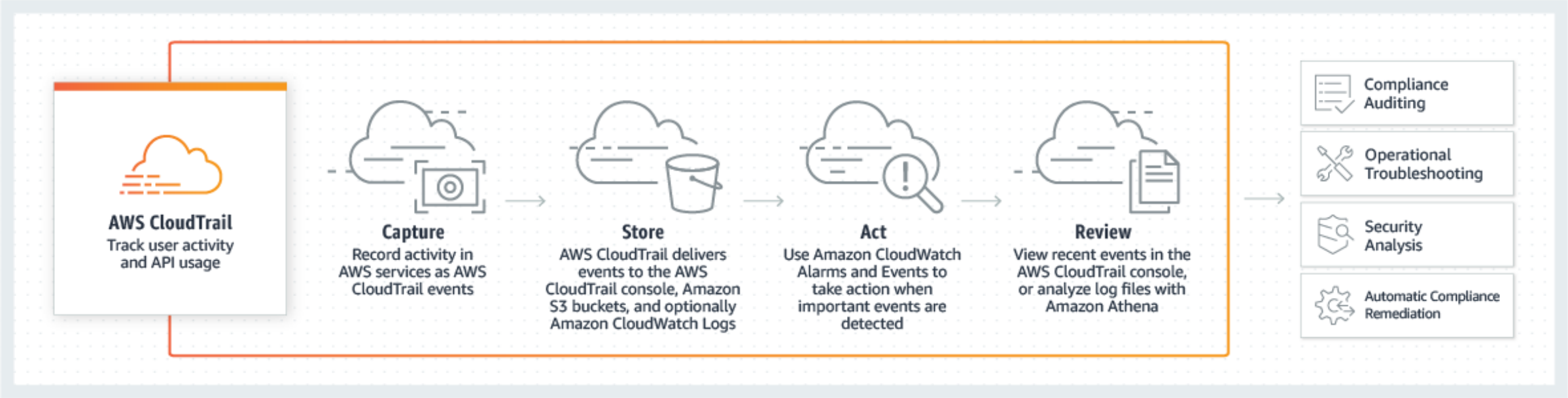
CloudTrail

- AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account
- You can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure
- CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services
- Customers who need to track changes to resources, answer simple questions about user activity, demonstrate compliance, troubleshoot, or perform security analysis should use CloudTrail

CloudTrail Features

- Since account creation, you have access to last 90 days of your account activity for create, modify, and delete operations of supported services
- Service works without activation or configuration
- You can view, search, and download your recent activity
- Log file integrity validation to detect whether the log files were unchanged, modified, or deleted since CloudTrail delivered them to your Amazon S3 bucket
- AWS CloudTrail encrypts all log files delivered to your specified Amazon S3 bucket using Amazon S3 server-side encryption (SSE)
- Data events provide insights into the resource (“data plane”) operations performed on or within the resource itself
- Management events provide insights into the management (“control plane”) operations performed on resources in your AWS account

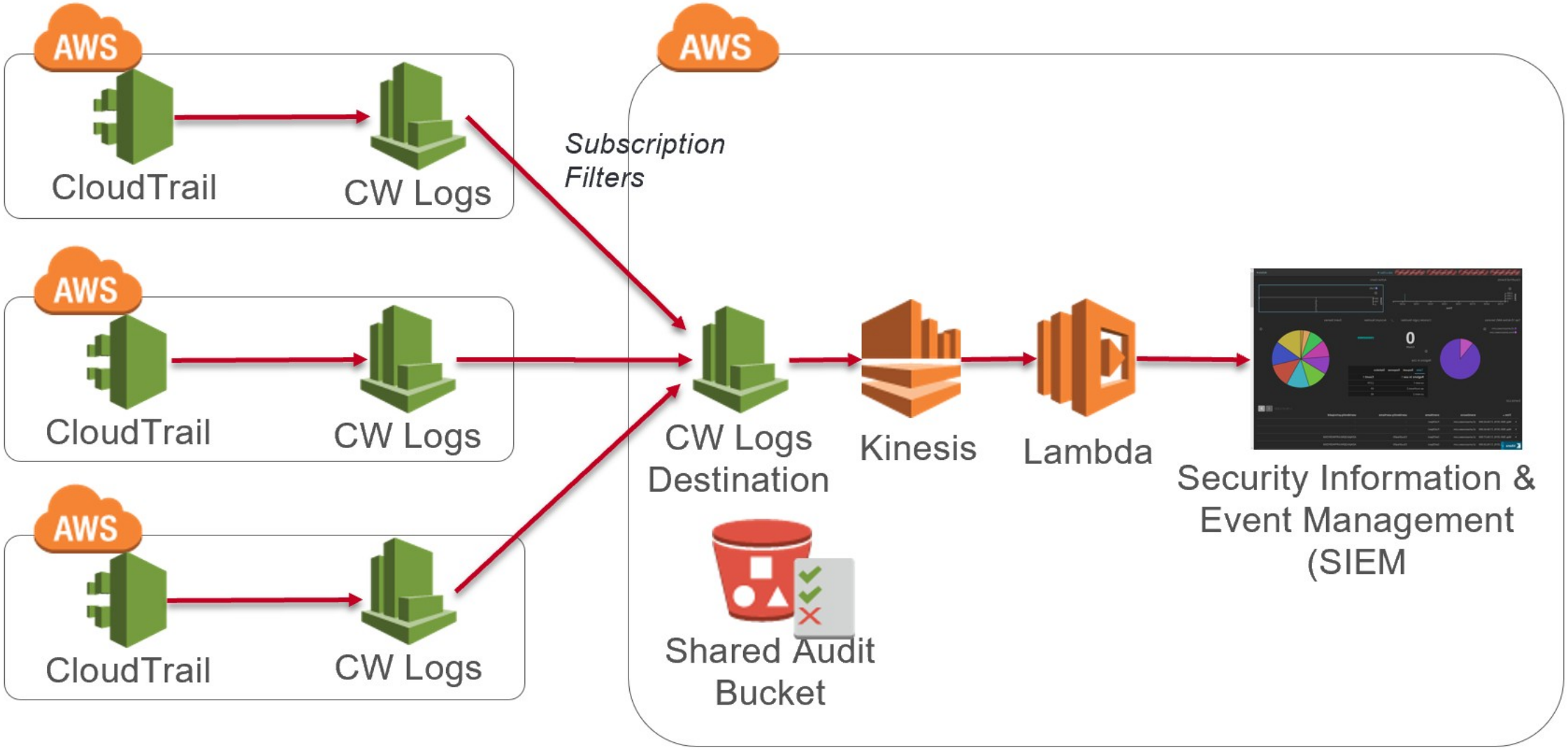
How CloudTrail works



CloudTrail Integration

- AWS Lambda
  - You can take advantage of the Amazon S3 bucket notification feature to direct Amazon S3 to publish object-created events to AWS Lambda
  - When CloudTrail writes logs to your S3 bucket, Amazon S3 can invoke your Lambda function to process the access records logged by CloudTrail
- Amazon CloudWatch Logs
  - AWS CloudTrail integration with Amazon CloudWatch Logs enables you to send management and data events recorded by CloudTrail to CloudWatch Logs
  - CloudWatch Logs allows you to create metric filters to monitor events, search events, and stream events to other AWS services, such as AWS Lambda and Amazon Elasticsearch Service
- Amazon CloudWatch Events
  - AWS CloudTrail integration with Amazon CloudWatch Events enables you to automatically respond to changes to your AWS resources
  - With CloudWatch Events, you are able to define actions to execute when specific events are logged by AWS CloudTrail

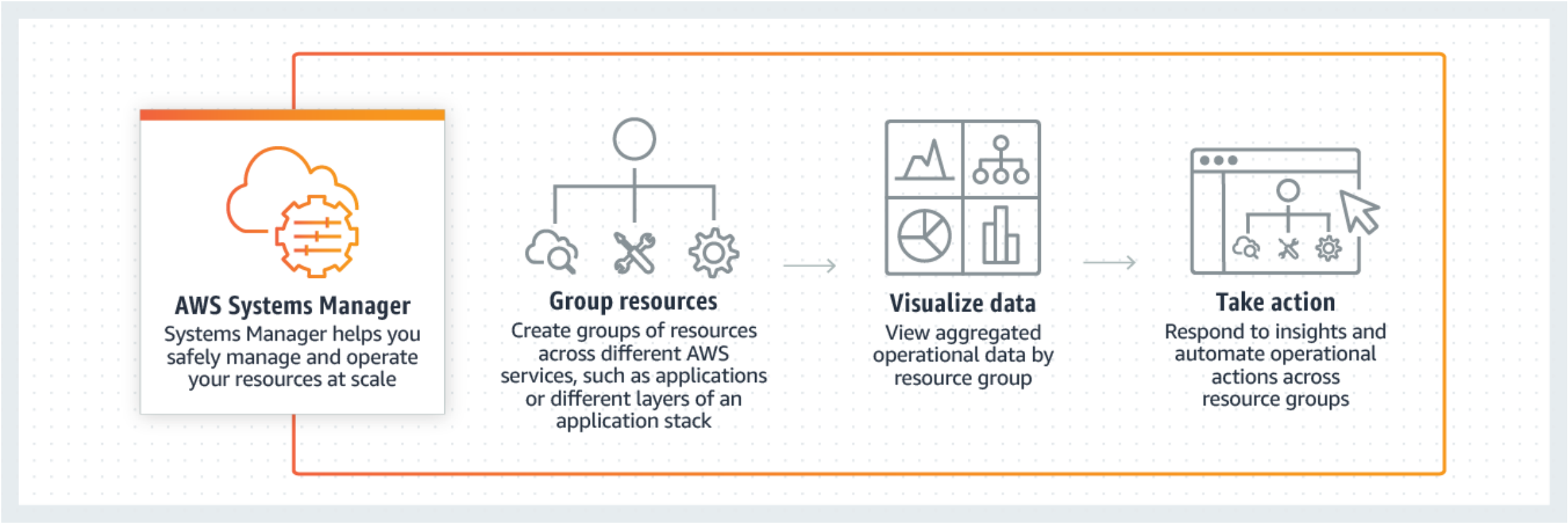
CloudTrail logs centralization



Systems Manager

- A unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources
- With Systems Manager, you can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources
- It simplifies resource and application management, shortens the time to detect and resolve operational problems, and makes it easy to operate and manage your infrastructure securely at scale

Systems Manager



Systems Manager Features

- OpsCenter
  - Provides a central location where operations engineers and IT professionals can view, investigate, and resolve operational issues related to any AWS resource
  - Aggregates and standardizes operational issues, referred to as OpsItems
- OpsItem give access to information
  - Event, resource and account details
  - Past OpsItems with similar characteristics
  - Related AWS Config changes
  - AWS CloudTrail logs and other quick-links to access logs and metrics
  - Amazon CloudWatch alarms
  - Stack information
  - List of runbooks and recommended runbooks
- Resource groups
  - A way to create a logical group of resources associated with a particular workload such as different layers of an application stack
  - Resource groups can be created, updated, or removed programmatically through the API

Systems Manager Features

- Insights Dashboard
  - AWS Systems Manager automatically aggregates and displays operational data for each resource group through a dashboard
  - Eliminates the need for you to navigate across multiple AWS consoles to view your operational data
- Inventory
  - Collects information about your instances and the software installed on them, helping you to understand your system configurations and installed applications
  - You can collect data about applications, files, network configurations, Windows services, registries, server roles, updates, and any other system properties
  - Gathered data enables you to manage application assets, track licenses, monitor file integrity, discover applications not installed by a traditional installer, and more
- Automation
  - AWS Systems Manager allows you to safely automate common and repetitive IT operations and management tasks across AWS resources
  - You can create documents that specify a specific list of tasks or use community provided docs

Systems Manager Features

- Run Command
  - Provides you safe, secure remote management of your instances at scale without logging into your servers, replacing the need for bastion hosts, SSH, or remote PowerShell
  - Has a simple way of automating common administrative tasks across groups of instances such as registry edits, user management, and software and patch installations
  - All actions taken with Systems Manager are recorded by AWS CloudTrail, allowing you to audit changes throughout your environment
- Session Manager
  - Provides a browser-based interactive shell and CLI for managing Windows and Linux EC2 instances, without the need to open inbound ports, manage SSH keys, or use bastion hosts
- Patch Manager
  - Helps you select and deploy operating system and software patches automatically across large groups of Amazon EC2 or on-premises instances
  - Through patch baselines, you can set rules to auto-approve select categories of patches to be installed, such as operating system or high severity patches, and you can specify a list of patches that override these rules and are automatically approved or rejected

Systems Manager Features

- Maintenance Window
  - AWS Systems Manager lets you schedule windows of time to run administrative and maintenance tasks across your instances
  - You can select a convenient and safe time to install patches and updates or make other configuration changes, improving the availability and reliability of your services and applications
- Distributor
  - Helps you securely distribute and install software packages, such as software agents
- State Manager
  - Provides configuration management, which helps you maintain consistent configuration of your Amazon EC2 or on-premises instances
  - You can control configuration details such as server configurations, anti-virus definitions, firewall settings, and define configuration policies for your servers
- Parameter Store
  - A centralized store to manage your configuration data, whether plain-text data such as database strings or secrets such as passwords

Monitoring documentation

- Amazon CloudWatch
  - https://docs.aws.amazon.com/cloudwatch/
- Amazon CloudTrail
  - https://aws.amazon.com/cloudtrail
- AWS Systems Manager
  - https://aws.amazon.com/systems-manager/