MANAGEMENT AND GOVERNANCE IN AWS

CloudWatch and Metrics list

Amazon CloudWatch is a monitoring and observability service that provides insights into AWS resources and applications. It collects and tracks metrics, logs, and events, allowing you to monitor performance, detect anomalies, and set alarms for operational issues.

CloudWatch Metrics are numerical data points representing the performance of your systems. They help you track key performance indicators (KPIs) such as CPU usage, memory utilization, and request counts, enabling you to analyze and optimize the performance of your applications and infrastructure.

Default metrics setup in CloudWatch:

CPU Utilization of an EC2 instance,

Disk Reads activity of an EC2 instance, and

Network packets out of an EC2 instance are readily available in CloudWatch by default.

Custom metrics that are available for setup in CloudWatch:

- Memory utilization
- Disk swap utilization
- Disk space utilization
- Page file utilization
- Log collection

CloudWatch Logs Streams

Amazon CloudWatch Logs Streams are sequences of log events from the same source, such as an application or service instance. They organize log data within CloudWatch Logs, making it easy to monitor and analyze logs from different sources in near real-time.

Basically,

This is a feature which allows cloudwatch logs to be streamed **near real-time** into other services such as Elasticsearch (Amazon OpenSearch).

CloudTrail

Cloudtrail is **an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account**. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

Note:

CloudTrail ⇒ Tracking

CloudWatch ⇒ Monitoring

Cost and Usage Report vs Cost Explorer

Both services are for financial management in the cloud but are quite different in nature and functionality. Here is how:

Cost and Usage Report explorer is more detailed but more spreadsheet-like and harder to use over time but much more comprehensive.

Cost Explorer on the other hand, is more visual but cannot give in-depth hourly data beyond 14 days.

Quick Summary (Comparison Chart)

	AWS Cost and Usage Report	**AWS Cost Explorer**
Description	A comprehensive, spreadsheet-like report of your billing data for a Payer AWS account	Highly visual cost graphs and tables showing a relatively high-level view of your costs and usage data for a specific Payer account in AWS
Unique functionality	Details historical cost and usage data and sends it to an Amazon S3 bucket for further analysis and longer retention	Not only offers historical records but also creates forecasts and savings recommendations
Data fields	Multiple line items. Also supports Cost Categories and Cost Allocation Tags	Up to 18 filters and groupings
Format	CSV and Parquet	CSV
Cost data duration	Hourly, daily, and monthly	Hourly (up to 14 days), daily, and monthly

Pricing	Free, but standard Amazon S3 charges apply	Free, although querying cost and usage data via the Cost Explorer API costs $0.01 per paginated request

AWS Config

AWS Config is a service that allows you to assess, audit and evaluate the configurations *(and configuration changes)* of the AWS resources within your account.

Quick tip:

AWS Config rules can also be used to define and detect resources which are not properly tagged.

Keyword: Configuration

AWS Organizations and PrincipalOrg Id

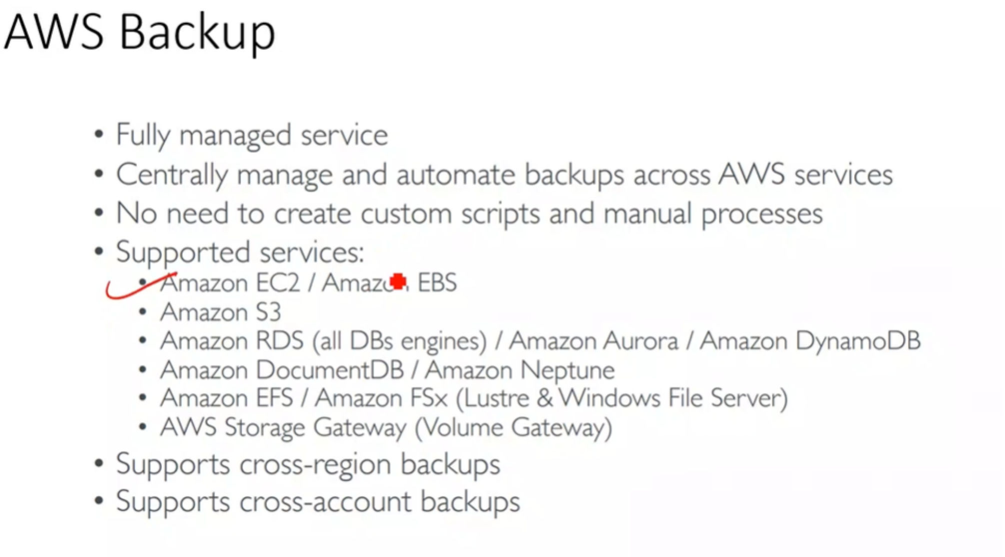
AWS Organizations facilitate resource sharing between accounts within the same organization. For example, you can share Amazon S3 buckets, Amazon RDS databases, or Amazon EC2 AMIs with other accounts within the organization.

In AWS, **the Principal Org ID is used to identify the organization when sharing resources.**

AWS Backup

AWS Backup is a fully managed backup service that centralizes and automates the backup of data across AWS services. It simplifies data protection by allowing you to define backup policies, automate backup scheduling, and manage backup retention periods.

It helps ensure data resilience and compliance with backup and recovery best practices without the need for custom scripting or manual intervention.



AWS Backup

- Fully managed service
- Centrally manage and automate backups across AWS services
- No need to create custom scripts and manual processes
- Supported services:
  - Amazon EC2 / Amazon EBS
  - Amazon S3
  - Amazon RDS (all DBs engines) / Amazon Aurora / Amazon DynamoDB
  - Amazon DocumentDB / Amazon Neptune
  - Amazon EFS / Amazon FSx (Lustre & Windows File Server)
  - AWS Storage Gateway (Volume Gateway)
- Supports cross-region backups
- Supports cross-account backups

Systems Manager Patch Manager vs Run Command

AWS Systems Manager Run Command allows you to remotely execute commands on multiple EC2 instances, on-premises servers, and virtual machines (VMs) at scale. It simplifies operational tasks by eliminating the need for manual SSH or RDP access, making it ideal for automating software installations, configuration changes, and administrative tasks across your infrastructure.

Patch Manager, also part of AWS Systems Manager, automates the process of patching operating systems and applications across your instances. It ensures that your systems remain up-to-date with the latest security patches and updates, thereby enhancing security and compliance while reducing manual effort in managing patch deployments. Together, these tools streamline management tasks and improve operational efficiency within your AWS environment.

Basically,

Systems Manager Patch Manager is used to perform OS level patches on the EC2 instances.

On the other hand, System manager run command is used to run third party commands and software updates and the like.

System Manager Session Manager

Systems Manager Session Manager is a secure and auditable tool for managing EC2 instances and on-premises servers. It allows us to create secure connections with EC2 Instances, with minimal overhead (no bastion host or SSH keys required).

CreationPolicy

Quick Tip:

When using CloudFormation, if the Architect needs to ensure that the required components are properly running before the stack creation proceeds, then the **CreationPolicy** attribute is to be used.

CloudFormation + CreationPolicy ⇒ Ensure components are running before stack creation proceeds.