**Content**

[1. Monitoring 2](#_Toc12633910)

[1. CloudWatch 2](#_Toc12633911)

[1.1.1. Events 2](#_Toc12633912)

[1.1.2. Logs 2](#_Toc12633913)

[2. CloudTrail 2](#_Toc12633914)

1. Monitoring
   1. CloudWatch
      1. Events

Are similar to alarms, instead of configuring thresholds and alarming on metrics, CloudWatch Events are matching event patterns and use targets to react.

Consists of

1. Event Source (operational change or schedule)
2. Rules (matches the events source and routes it to targets – if there is a match)
3. Targets (services that will react to the event)
   * 1. Logs

Requires the install of CloudWatch Unified Agent or Logs Agent (legacy)

Consists of

1. Log Events – Record of activity recorded by the monitored resource
2. Log Streams – Sequence of log events from the same source / application
3. Log Groups – a collection of log streams with same access control, monitoring and retention settings
4. Metric Filters – assigned to log groups, it extracts data from the groups‘ log streams and converts that data into a Metric data point. Enables to create alarms.
5. Retention Settings – period of time logs are kept. Assigned to log roups, but applies to all the streams in a group.
   1. CloudTrail

Recors API activity in your account

1. Organizations

AWS Organizations is an account mngmnt service that enables you to consolidate multiple AWS Accounts into an organization that you create and centrally manage.

* Centralized account management
* Consolidated billing
* Hierarchical grouping – budgetary, security, compliance
* Control over the AWS services and API actions

HTTPS Query API ???

AWS Tools for Windows PowerShell ???

1. Organization
2. Root
3. OU – Organization unit
4. Account
5. Invitation
6. Handshake
7. SCP – Service control policy
8. Whitelisting

You explicitly specify the access that is allowed. All other access is implicitly blocked. By default, AWS Organizations attaches an AWS managed policy called FullAWSAccess to all roots, OUs, and accounts. This ensures that, as you build your organization, nothing isblocked until you want it to be. In other words, by default all permissions are whitelisted

1. Blacklisting

You explicitly specify the access that is not allowed. Default behavior. Blacklists you typically leave the default FullAWSAccess policy in place (that allow "all") but then attach additional policies that explicitly deny access to the unwanted services and actions

**Service-Linked role -** When you enable an AWS service to perform tasks on your behalf in your organization's member accounts, AWS Organizations creates an IAM service-linked role for that service in each member account. The service-linked role has predefined IAM permissions that allow the other AWS service to perform specific tasks in your organization and its accounts. For this to work, all accounts in an organization automatically have a service-linked role that enables the AWS Organizations service to create the service-linked roles required by AWS services for which you enable trusted access. These additional service-linked roles come with policies that enable the specified service to perform only those tasks that are required by your configuration choices

Organizations also verifies that every account has a service-linked role named AWSServiceRoleForOrganizations. This role is mandatory in all accounts to enable all features. If you deleted the role in an invited account, accepting the invitation to enable all features recreates the role. If you deleted the role in an account that was created using AWS Organizations, that account receives an invitation specifically to recreate that role. All of these invitations must be accepted for the organization to complete the process of enabling all features