Tony Shen

AWS MALIR

Contents

Revision: v0.1
Created on November 22, 2019
Revised on February 26, 2020

Glossary

Item	Description
AWS	Amazon Web Services
MALIR	Monitoring, Alerting, Logging, and Incident Response
VPC	Virtual Private Cloud
Instance	Virtual Machine
S3	Simple Storage

Introduction

Cloud security includes monitoring, alerting, logging, and incident response, or MALIR for short. MALIR is eyes, ears, and responders for cloud. Without it, cloud security is left with no guards.

In this article we will discuss what AWS services are for MALIR, how they work, how to make most use of MALIR to secure and protect your cloud.

When you use cloud computing, you have an environment of your own separated from others in the cloud. As a totally virtual platform of yours out there in the cloud without any physical barriers, it is paramount to secure your cloud with online MALIR.

Figure 1 below depicts a typical cloud environment. Your security with MALIR defines your cloud's virtual boundary. Along your cloud boundary, your networking constitutes the infrastructure within which your virtual resources reside and run in three basic forms

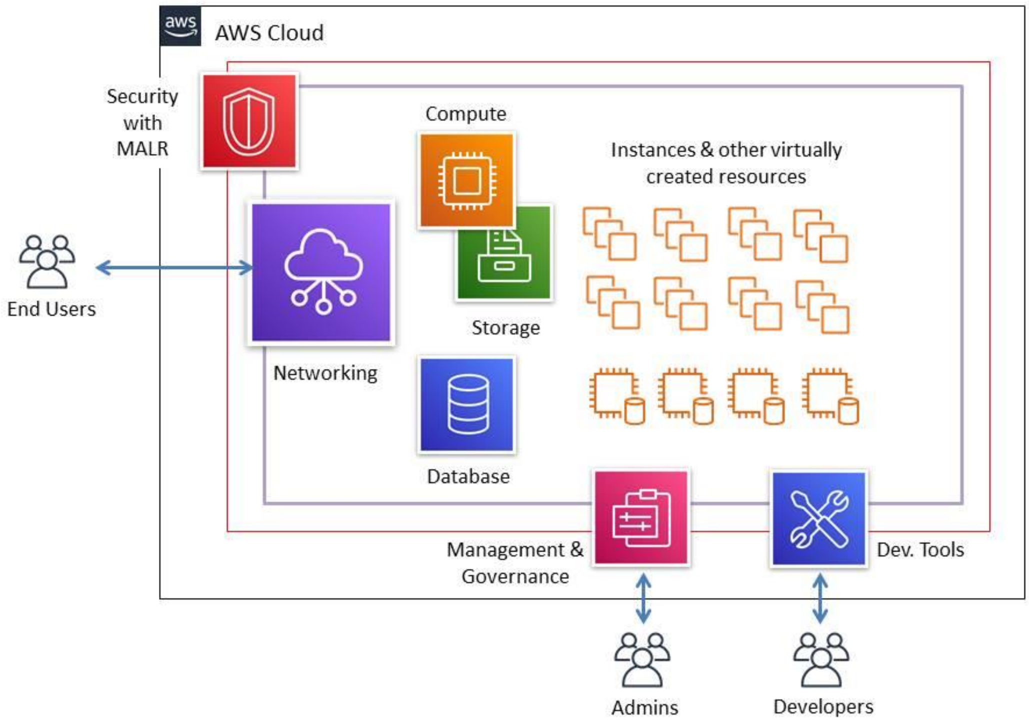
- Compute – Virtual Machines or Instances
- Storage – Data storage
- Database – Virtual database instances of various kinds

Your cloud applications run on your cloud resources

Your end users interact with your cloud when using your apps. Your support teams interact with your cloud when managing your cloud resources. Your cloud has multiple interfaces for users and support teams to interact with your cloud

User activities and services running with your resources in your cloud bring about constant changes. Your MALIR monitors all changes and responds to detected abnormalities timely.

Figure 1 – Security with MALIR defining and securing your cloud in AWS



Requirements for MALIR

1. Monitor continuously
2. Detect abnormalities quickly
3. React to incidents rapidly
4. Remediate issues timely
5. Improve security posture constantly

MALIR Domains

1. User activities
2. All changes, planned or unplanned, including unexpected, in your cloud
3. System performance
4. Resource utilization, including billing
5. Risks for service disruption
6. Vulnerabilities to intrusions, errors, failures, and possible loss of your data

Environment

MALIR Services

As of today, AWS offers 143 services in 25 categories. A good number of the services can be used for MALIR. None of those services, however, is intended to work alone. MALIR services work best when they work together.

Table 1 below lists fourteen AWS services as MALIR services. There are, of course, other services that can be used to assist MALIR, such as certain management tools and developer tools. The services identified in the table below constitute the main force for MALIR.

Table 1 – AWS MALIR Services

Item	Service	MALIR	Service Category
1	VPC (Flow Log)	Logging	Networking & Content Delivery
2	CloudTrail	Logging	Management & Governance
3	CloudWatch	Monitoring, Alerting, Logging	Management & Governance
4	Config	Monitoring	Management & Governance
5	Systems Manager	Monitoring, Response	Management & Governance
6	Trusted Advisor	Monitoring	Management & Governance
7	Security Hub	Monitoring, Response	Security, Identity & Compliance
8	GuardDuty	Monitoring	Security, Identity & Compliance
9	Inspector	Monitoring	Security, Identity & Compliance
10	Macie	Monitoring	Security, Identity & Compliance
11	SNS	Alerting	Application Integration
12	SQS	Alerting	Application Integration
13	Lambda	Alerting, Response	Compute
14	Step Function	Alerting, Response	Application Integration
15	CloudFormation	Response	Management & Governance

To meet the aforementioned requirements, MALIR services perform these tasks

1. Logging
2. Monitoring
3. Alerting
4. Responding

MALIR services and how they work are inspected in more details in the following sections

Logging

Three services listed below do logging

- VPC (Flow Log)
- CloudTrail
- CloudWatch

VPC Flow Log

VPC is the networking service that allows you to create virtual private clouds (VPCs), an important form of your networking infrastructure. After you created a VPC, VPC Flow Log is waiting for you to enable it. Once you enabled VPC Flow Log, it starts logging traffic data in and across the VPC. It keeps doing so until you disable it.

Flow Log uses S3 as its log data storage. You create a S3 bucket for Flow log to write its logs to. Alternatively, you can let Flow Log sends its log data to CloudWatch for storage and further handling. You can retrieve and inspect Flow Log data from CloudWatch or from S3. You can view it in Console or retrieve it by AWS CLI and/or API calls.

CloudTrail

AWS CloudTrail primarily logs events. Events are API calls. API calls are made by user activities or by services. When a user signs in the console, when an admin changes a user's permissions, and when a scheduled batch job is started to run, API calls are made, CloudTrail records them as events.

CloudTrail logs event data in trails that you created. Each trail writes and stores data in S3. In addition, CloudTrail can send event data to Lambda or to CloudWatch for further processing.

CloudWatch

CloudWatch was mentioned twice previously. CloudWatch monitors your virtual resources and running applications in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for the usage of your resources and applications, such as your instance CPU utilization and volumes (virtual disks) read or write performance. CloudWatch can also receive events sent over from other services, such as CloudTrail. CloudWatch, however, does not records API calls as events like CloudTrail does.

CloudWatch logs data in CloudWatch log groups (LGs). LG storage is managed by AWS internally but it lets you do what you need to do. For instance, you can create multiple log groups to log monitoring data separately according to different monitoring targets, i.e., you can log production instances data in one LG, and development instances data in another LG. You can view log data from Console. You can retrieve log data from LGs by AWS CLI or by AWS SDK API calls, too.

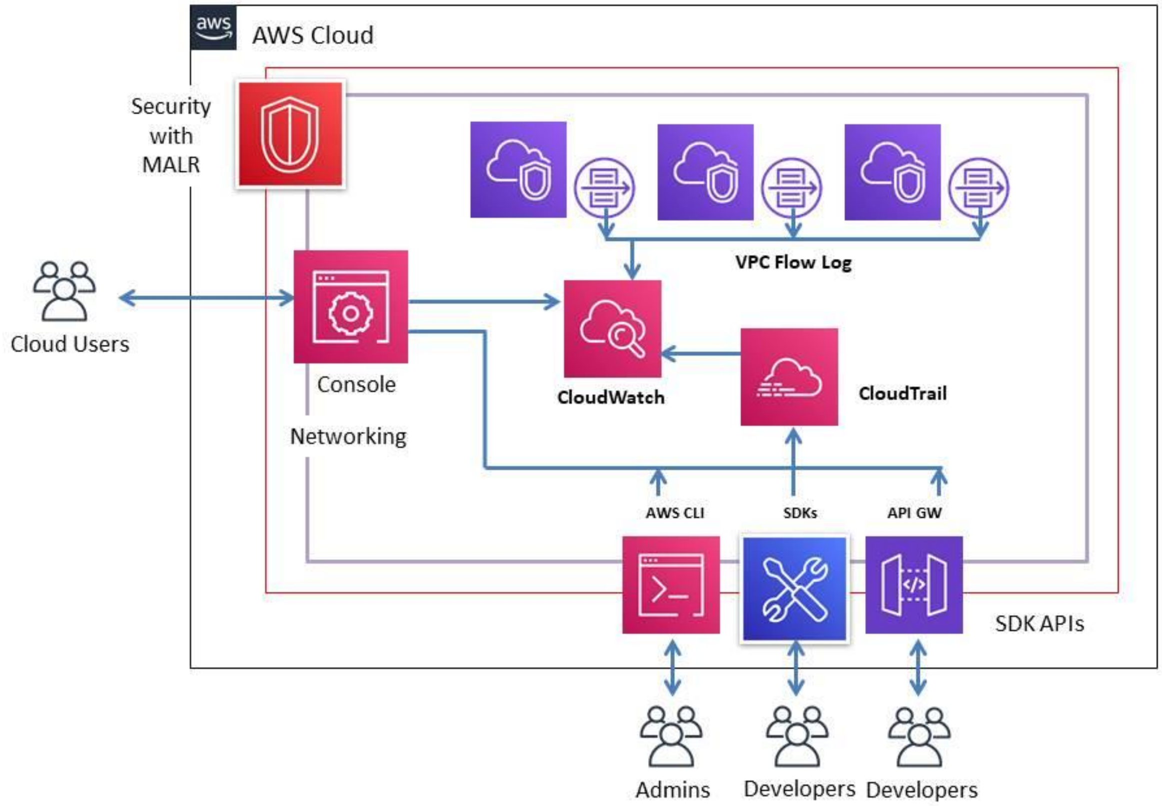
Collective Logging

Figure 2 below shows how VPC Flow Log, CloudTrail, and CloudWatch services work together for logging.

VPC Flow Log captures network traffic data. Flow Log sends the data to CloudWatch. CloudTrail captures and logs event data. CloudTrail sends event data to CloudWatch. Events are actions taken by users and/or by services. Users take actions when interacting with cloud in one of the four interfaces, namely, Console, AWS CLI, SDK API calls, or API Gateway.

Being the front-end interface, Console access ought to be restricted, tightly controlled, and closely monitored. AWS CLI, SDKs, and API Gateway are backend interfaces for management, security, operations, and development.

Figure 2 – VPC Flow Log, CloudTrail, and CloudWatch working together



In Figure 2, Cloud Users include the following

- Cloud admins
- Cloud operators
- Cloud developers
- Cloud engineers
- Cloud auditors

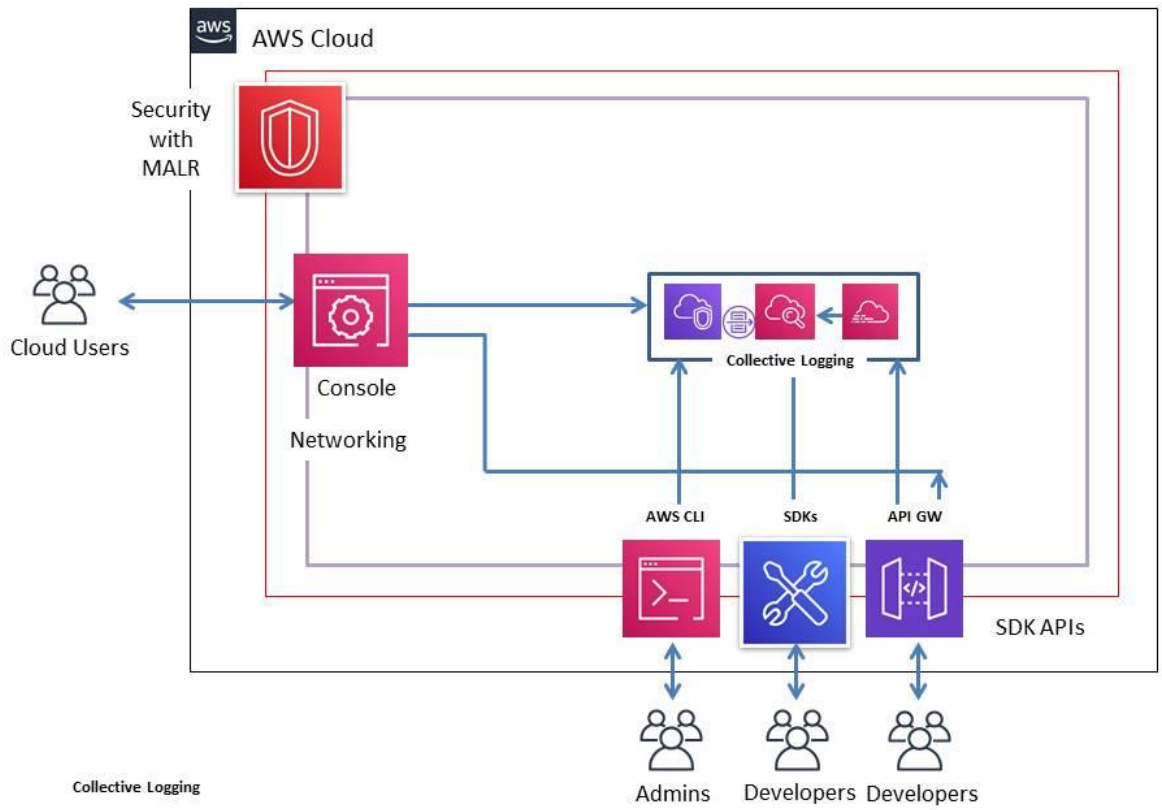
In Figure 2, Cloud Users do not include the following

- WF end users of cloud applications
- WF customer end users of cloud applications
- WF partners and other approved parties who use cloud applications

The excluded end users listed above do not have a need to access WF cloud environment directly because they are not allowed to create their own apps or provision any resources for their apps in the cloud but simply using cloud apps that they are given. Cloud app users identification and authorization are handled differently from cloud users.

The trio of VPC Flow Log, CloudTrail, and CloudWatch services can be viewed collectively as Collective Logging

Figure 3 – Collective Logging



Monitoring

- Config
- Systems Manager
- Trusted Advisor
- Security Hub
- Guard Duty

- Inspector
- Macie

Config

AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows customers to automate the evaluation of recorded configurations against desired configurations.
[AWS Documentation, EY 2018]

Systems Manager

AWS Systems Manager, formerly known as “Amazon EC2 Systems Manager” and "Amazon Simple Systems Manager", gives customers the visibility and control to their infrastructure on AWS. AWS Systems Manager provides customers a unified user interface so customers can view their operational data from multiple AWS services, and allows customers to automate operational tasks across the AWS resources.
[EY 2018]

Trusted Advisor

Trusted Advisor (TA) is part of AWS Case Management System. TA allows customer to open a case with AWS support quickly and provides AWS support with sufficient background information to facilitate incident investigation, troubleshooting and timely resolution of reported issues. TA API allows automation of case management that adds value to security monitoring and incident status tracking from the very beginning through the end of its full remediation
[AWS Support Case Management User Guide]

Security Hub

AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your compliance with the security industry standards and best practices. Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.
[AWS Documentation]

GuardDuty

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following data sources: VPC Flow Logs, AWS CloudTrail event logs, and DNS logs. It uses threat intelligence feeds, such as lists of malicious IPs and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IPs, URLs, or domains. For example, GuardDuty can detect compromised EC2 instances serving malware or mining bitcoin. It also monitors AWS account access behavior for signs of compromise, such as unauthorized infrastructure deployments, like instances deployed in a region that has never been used, or unusual API calls, like a password policy change to reduce password strength. GuardDuty informs you of the status of your AWS environment by producing security findings that you can view in the GuardDuty console or through CloudWatch events.
[AWS Documentation]

Inspector

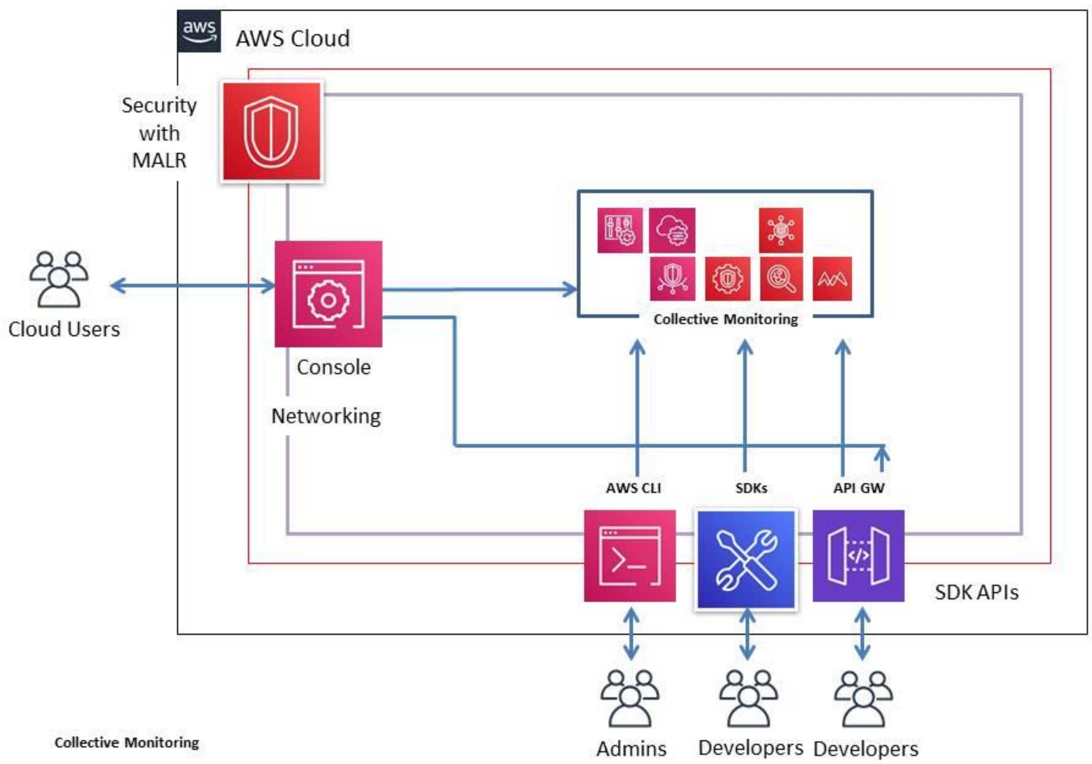
Amazon Inspector is an automated security assessment service for customers seeking to improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.
[EY 2018]

Macie

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property. It provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.
[AWS Documentation]

Collective Monitoring

Figure 5 – Collective Monitoring



Alerting

- SNS
- SQS

SNS

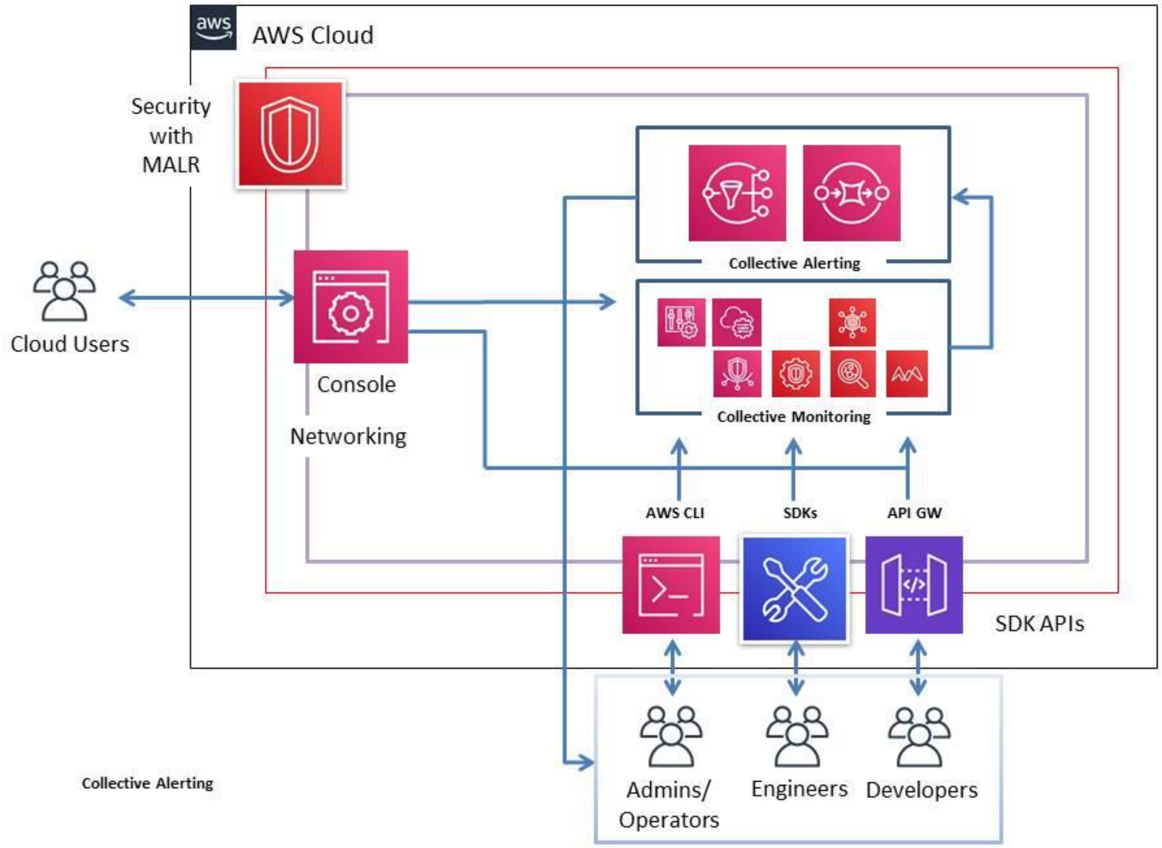
Amazon Simple Notification Service is a web service to set up, operate, and send notifications. It provides developers the capability to publish messages from an application and deliver them to subscribers or other applications. Amazon SNS follows the “publish-subscribe” (pub-sub) messaging paradigm, with notifications being delivered to clients using a “push” mechanism.
[AWS Documentation, EY 2018]

SQS

Amazon Simple Queue Service offers a distributed hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can move data between distributed components of their applications that perform different tasks, without losing messages or requiring each component to be always available. Amazon SQS allows customers to build an automated workflow, working in close conjunction with Amazon EC2 and the other AWS infrastructure web services.
[AWS Documentation, EY 2018]

Collective Alerting

Figure 6 – Collective Alerting



Responding

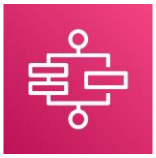
- Lambda
- Step Functions
- CloudFormation
- Event Bridge

Lambda

AWS Lambda lets customers run code without provisioning or managing servers on their own. AWS Lambda uses a compute fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones in a region, which provides the high availability, security, performance, and scalability of the AWS infrastructure

[AWS Documentation, EY 2018}

Step Function



AWS Step Functions is a web service that enables customers to coordinate the components of distributed applications and microservices using visual workflows. Customers can build applications from individual components that each perform a discrete function, or task, allowing them to scale and change applications quickly.
[AWS Documentation, EY 2018]

CloudFormation

AWS CloudFormation enables customers to create and manage a collection of related AWS resources by providing templates to use in the provisioning and updating of AWS services.
[AWS Documentation, EY 2018]

EventBridge

Amazon EventBridge is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as AWS Lambda. You can set up routing rules to determine where to send your data to build application architectures that react in real time to all of your data sources. EventBridge allows you to build event driven architectures, which are loosely coupled and distributed.

EventBridge was formerly called Amazon CloudWatch Events. It includes new features that enable you to receive events from SaaS partners and your own applications. Existing CloudWatch Events users can access their existing default bus, rules, and events in the new EventBridge console and in the CloudWatch Events console. EventBridge uses the same CloudWatch Events API, so all of your existing CloudWatch Events API usage remains the same.

You can configure the following AWS resources as targets for EventBridge:

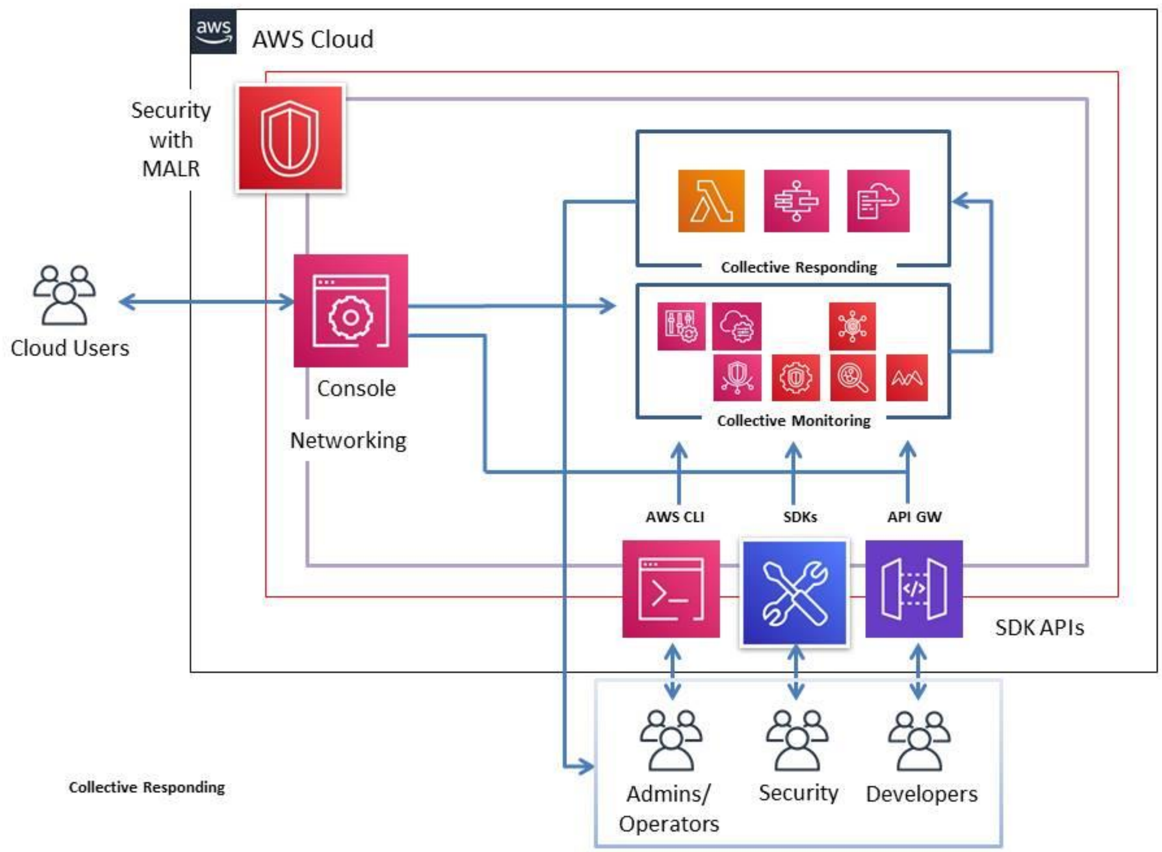
- Lambda functions
- Amazon EC2 instances
- Streams in Amazon Kinesis Data Streams
- Delivery streams in Amazon Kinesis Data Firehose
- Log groups in Amazon CloudWatch Logs
- Amazon ECS tasks
- Systems Manager Run Command
- Systems Manager Automation
- AWS Batch jobs
- AWS Step Functions state machines
- Pipelines in AWS CodePipeline
- AWS CodeBuild projects
- Amazon Inspector assessment templates
- Amazon SNS topics
- Amazon SQS queues
- Built-in targets: EC2 CreateSnapshot API call, EC2 RebootInstances API call, EC2 StopInstances API call, and EC2 TerminateInstances API call
- The default event bus of another AWS account

[AWS Documentation]

Collective Responding

Part of SIEM (Security Information and Event Management) and IR (Incident Response), Collective Responding (CR) is at the core of MALIR. It automates detecting security vulnerabilities and timely remediation to address security issues based on constant logging, monitoring, and alerting functions of MALIR. As Figure 7 shows below, Collective Monitoring (CM) collects events raised by user and service activities. CR screens events with defined compliance rules and usage matrices to detect abnormal changes, which, once found, immediately notify cloud support teams for them to take actions and, more importantly, triggers remediation measures by code to correct issues without waiting, thereby minimizing delays, if any, in response time.

Figure 7 – Collective Responding

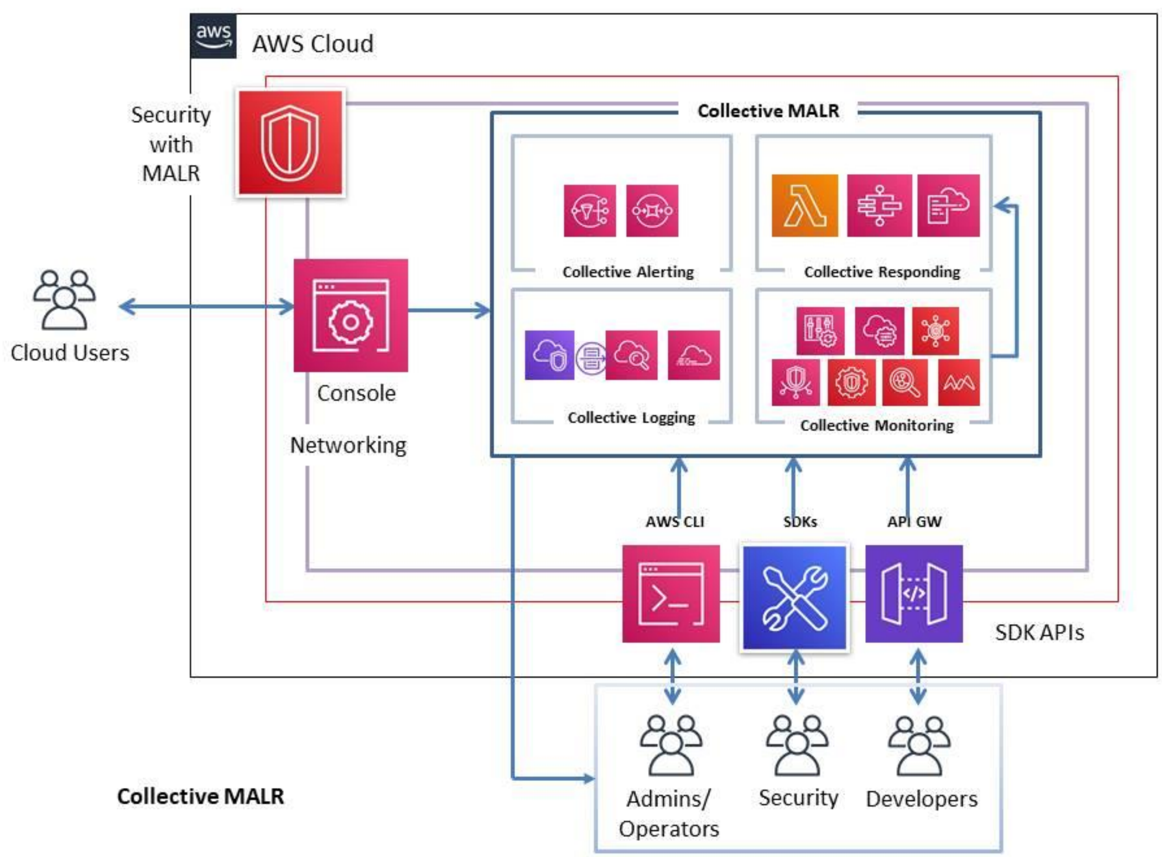


MALIR Services Recap

Collective MALIR encapsulates MALIR services that include CL (Collective Logging, CM (Collective Monitoring), CL (Collective Alerting), and CR (Collective Responding). See Figure 8 below.

Collective MALIR captures all events and changes in the cloud and timely reacts to detected abnormalities by both engaging support teams with notifications and resolving issues automatically following predefined security compliance rules and measuring matrices by code. Logs accumulated by CL facilitates in-depth security investigations and auditing for CSPM (Cloud Security Posture Management), the outcomes of which feed back into MALIR to refine compliance rules and matrices so as for MARL to improve proactively and stay ever green in pace with ever evolving business changes.

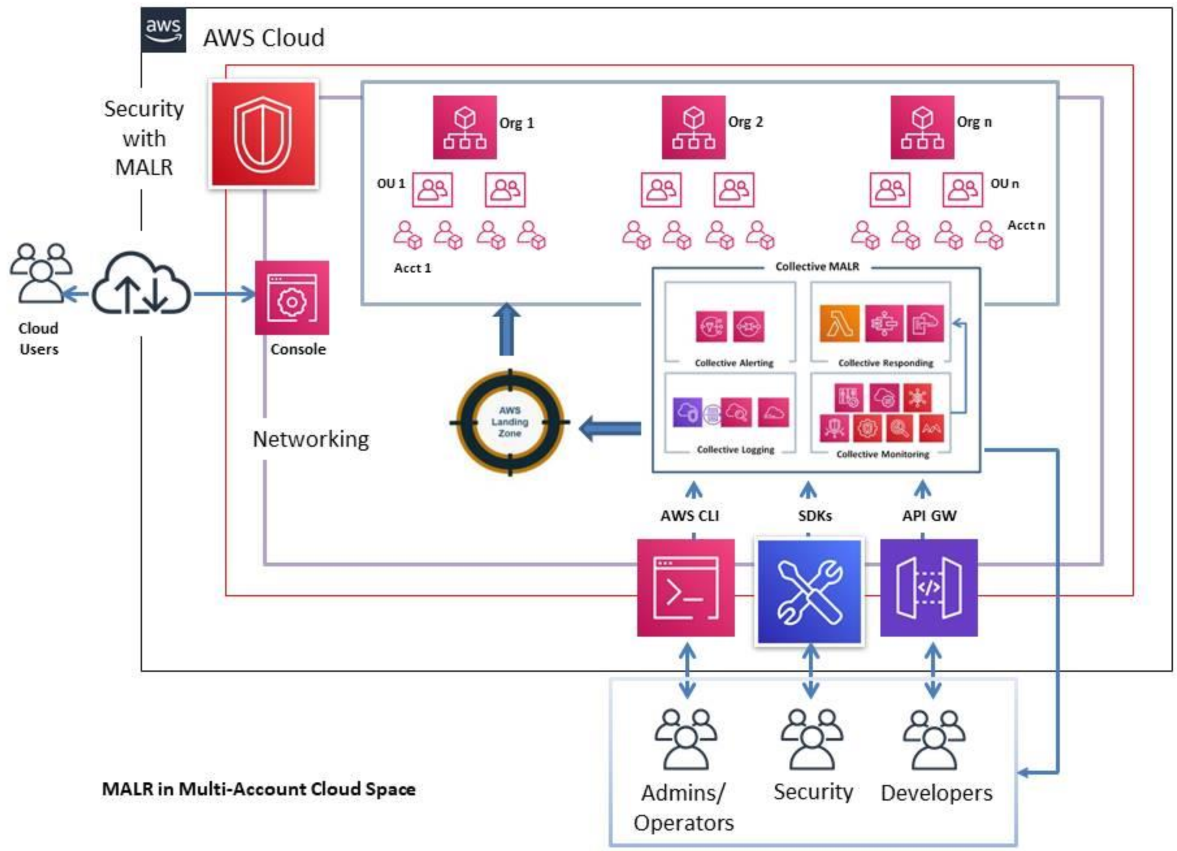
Figure 8 – Collective MALIR



MALIR Architecture

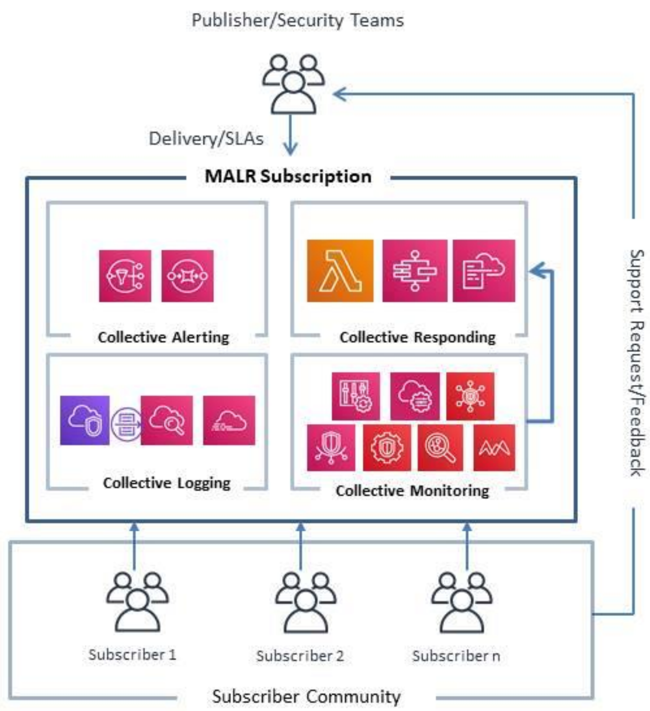
Multi-Account Cloud Space

Figure 11 – MALIR in Multi-Account Cloud Space



Subscription Model

Figure 12 – MALIR Subscription Model



MALR Subscription Model

How to Subscribe to MALIR

Request Process

MALIR Subscription Request Process is designed for subscriber to obtain right MALIR services that fit their business needs.

The process requires subscriber to specify

1. MARL domain(s)
2. MALIR notification preferences
3. MALIR remediation preferences
4. MALIR billing code to accept billing responsibility
5. MALIR package(s) to subscribe to
6. MALIR support tier(s) to have, which affects subscriber's billing cost

MALIR Domains

- User Activities
- IAM Changes
- Networking Changes
- Compute Changes
- Storage Changes
- Database Changes
- Analytics Changes
- Web Services Changes

[Content to be added]

MALIR Notification Preferences

- By email
- By SMS
- By phone

MALIR Remediation Preferences

1. Human intervention
2. Machine intervention
3. Both Human intervention and machine intervention
    - Machine intervention requires human approval
    - Machine intervention does not require human approval

Preference 2 and 3 requires subscriber to work with CPSSE to define desired security compliance rules and measuring matrices

Billing Responsibilities

Subscriber is assigned with a billing code. Subscriber is obligated to follow a naming convention in naming and tagging all their MALIR targeted resources. Their billing code is embedded in the naming convention.

Support

Support Tiers

1. WF MALIR Support
2. AWS MALIR Support
3. WF and AWS MALIR Support

[Content to be added]

MARL Subscription Packages

1. Bronze
2. Silver
3. Gold
4. Platinum

MALIR Subscription Request Form

Scope	Domain	Target	Description	Trigger alert by	Action	Frequency	Remark

MALIR Scope Options

1. Organizations
2. Organizational Unit (OU)
3. Account
4. Region (applies to regionally scoped services such as VPC, EC2, and RDS)

MALIR Domain Options

1. User Activities
2. IAM Changes
3. Networking Changes
4. Compute Changes
5. Storage Changes
6. Database Changes
7. Analytics Changes
8. Web Services Changes

MALIR Targets (Service Resources)

For example, VPC has the following resources as MALIR targets. Most, if not all, those targets need to be monitored so changes can be detected, and response measures can be taken timely to ensure security

Networking

1. ENIs (Elastic Network Interface)
2. Route Tables
3. Internet Gateways
4. Egress-Only Internet Gateways
5. DHCP Options Sets
6. Elastic IPs
7. Endpoints
8. Endpoint Services (for cross-account sharing)
9. NAT Gateways
10. NAT Instances

11. Peering Connections

Security
1. Network ACLs (NACLs)
2. Security Groups (SGs)

VPN
1. Customer Gateways
2. Virtual Private Gateways
3. Site-to-Site VPN Connections
4. Client VPN Endpoints

Cross-Boundary Sharing
1. Transit Gateways
2. Transit Gateway Attachments
3. Transit Gateway Route Tables

Cross-Boundary Traffic Monitoring
1. Mirror Sessions
2. Mirror Targets
3. Mirror Filters

MALIR Security Frameworks

- CIS Controls
- CSA Control Domains
- NIST 800-53 R4 Control Families
- MALIR Security Framework Support Matrix

CIS Controls

Table 3 – CIS Controls (20)

Control ID	Control Name
1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management
4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops,

	Workstations and Servers
6	Maintenance, Monitoring and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Implement a Security Awareness and Training Program
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

CSA Control Domains

Table 4 – CSA Control Domains (17)

Domain ID	Control Domain
AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Management & Operational Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Management
DCS	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance and Risk Management
HRS	Human Resources
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization Security
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Security Incident Management, E-Discovery & Cloud Forensics
STA	Supply Chain Management, Transparency and Accountability
TVM	Threat and Vulnerability Management

NIST 800-53 R4 Control Families

Table 5 – NIST 800-53 R8 Security Control Families

Code	Control Family
AC	ACCESS CONTROL
AT	AWARENESS AND TRAINING
AU	AUDIT AND ACCOUNTABILITY
CA	SECURITY ASSESSMENT AND AUTHORIZATION
CM	CONFIGURATION MANAGEMENT
CP	CONTINGENCY PLANNING
IA	IDENTIFICATION AND AUTHENTICATION
IR	INCIDENT RESPONSE
MA	MAINTENANCE
MP	MEDIA PROTECTION
PE	PHYSICAL AND ENVIRONMENTAL PROTECTION
PL	PLANNING
PS	PERSONNEL SECURITY
RA	RISK ASSESSMENT
SA	SYSTEM AND SERVICES ACQUISITION
SC	SYSTEM AND COMMUNICATIONS PROTECTION
SI	SYSTEM AND INFORMATION INTEGRITY
PM	PROGRAM MANAGEMENT

MALIR Security Framework Support Matrix

Table 6 - Mapping Between MALIR and Security Frameworks

Item	Service	NIST 800-53-R4	CIS	CSA
1	VPC Flow Log	MA	AWS Logging, Monitoring	IVS
2	CloudTrail	MA	AWS Logging, Monitoring	IVS
3	CloudWatch	MA	AWS Logging, Monitoring	IVS
4	Config	CM	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	IVS, CCC
5	Trusted Advisor	MA, IR	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	IVS
6	GuardDuty	MA	Limitation and Control of Network Ports,	IVS

			Protocols, and Services	
7	Inspector	MA	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	IVS
8	Macie	MA	Data Protection	IVS, AIS
9	Security Hub	MA, AU	Maintenance, Monitoring and Analysis of Audit Logs	IVS, TVM
10	Systems Manager	MA	Inventory and Control of Software Assets	IVS, TVM
11	Lambda	MA, IR	Continuous Vulnerability Management	IVS, SEF
12	Step Function	MA, IR	Continuous Vulnerability Management	IVS, SEF
13	SNS	MA, IR	Continuous Vulnerability Management	IVS, SEF
14	SQS	MA, IR	Continuous Vulnerability Management	IVS, SEF

References

AWS Documentation