VPC NETWORK MANAGEMENT AND MONITORING *“What network management and monitoring features are available for Amazon VPC?”*

Overview

Amazon Web Services (AWS) and AWS Partner Network (APN) members offer a comprehensive set of capabilities for managing and monitoring Amazon Virtual Private Cloud (Amazon VPC) networks. This document provides an overview of the network management and monitoring features available for the AWS platform. It provides guidance on how to effectively utilize these tools to control, manage, and track network changes and gain visibility into your VPC network traffic. For more information about controlling network traffic, please see the *VPC Security Capabilities* Solution Brief.

The following sections assume basic knowledge of AWS Identity and Access Management (IAM), AWS Service Catalog, AWS Config, AWS CloudTrail, Amazon CloudWatch, and network logging and monitoring.

General Best Practices

Efficient management and monitoring is essential to the security of any computer network and should incorporate the following principles:

- Understand the available network management and monitoring capabilities and how they relate to your applications.
- Control changes to the network infrastructure through a combination of access control, access monitoring, and configuration tracking.
- Monitor network traffic for expected and unexpected traffic to identify irregularities and gain key insight into the security of the system. For example, a poorly performing network can indicate that the network is under attack, and irregular attempts to contact unexpected external systems can indicate that an internal host has been compromised.

Application on the AWS Platform

The following sections describe AWS and APN member-provided capabilities for network-resource access control and change tracking, and network traffic monitoring.

Access Control to Network Resources

AWS Identity and Access Management (IAM)

IAM enables you to securely control how users create, configure, change, and delete AWS network resources. For example, an IAM Network Administrator group or role can be granted permission to administer VPCs, subnets, route tables, gateways, and peering connections while a Developer group can be granted more restrictive, view-only access to these resources, or permission to launch Amazon Elastic Compute Cloud (Amazon EC2) instances into only specific VPCs or subnets. Granular permissions can be used to restrict other network-related tasks, such as API calls that modify a security group or VPC route table changes.

When planning IAM controls, identify users who need permission to perform network operations and the scope of their permitted actions. For example, some AWS customers identify a group of network administrators for their organization while others have specific network administrators for each AWS account or even for specific VPCs within an account. Please see the *IAM in Practice* Solution Brief for additional guidance for creating IAM policies and permissions.

Service Catalog

AWS Service Catalog enables organizations to centrally manage and control changes to their network resources. Use AWS Service Catalog to create and manage portfolios of IT services, products, and configuration information, including approved network templates, and then grant access to these portfolios along with carefully constrained permissions that allow users to instantiate only preapproved network configurations. AWS Service Catalog provides safe and powerful self-service options for an organization while ensuring network changes are coordinated through predefined network templates.

When planning to use AWS Service Catalog to control changes to network resources, determine if predefined network templates are appropriate for your use case. Network portfolio and product development requires additional overhead for creating, testing, approving, and publishing predefined network templates. Next create a strategy for organizing and distributing network templates, such as using network-specific portfolios versus user-specific product portfolios. Typically, organizations create network-specific portfolios when network changes are restricted to specific network administration groups, and incorporate network templates as products in user-specific portfolios when creating self-service network provisioning capabilities for non-network administrators.

Network Configuration Change Monitoring

AWS CloudTrail and CloudWatch

AWS CloudTrail provides a history of AWS API calls for an account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). This AWS API call history enables security analysis, resource change tracking, and compliance auditing. Customers can also deliver CloudTrail data to CloudWatch Logs to store, monitor, and process API calls for network-specific changes and to send appropriate notifications. CloudTrail provides an AWS CloudFormation template to automatically create CloudWatch alarms for security- and network-related API activity.[1]

The integration between CloudTrail and CloudWatch Logs, and AWS CloudFormation template for automatically creating CloudWatch Alerts, is currently the most convenient way to get started with AWS network monitoring and alerting. CloudWatch Alerts provide notification of the specific security or network API activity that occurred, but it does not provide details about which specific resource or values were changed. Therefore, this approach is recommended for customers who want to get started quickly and easily and will use the AWS Config console to research and review CloudTrail generated change notifications.

AWS Config and Config Rules

AWS Config creates an AWS network resource inventory, including configuration history and configuration change notification. AWS Config discovers existing AWS resources, provides configuration details, shows relationships between resources, and determines how a resource was configured at a specific point in time. Customers can leverage AWS Config to examine relationships between network resources and understand the possible impact of changes before they make them. AWS Config can also be used reactively to retrieve configuration data, such as route table settings or security group rules, from a certain point in time.

When a resource configuration is modified, AWS Config can proactively send a change notification to Amazon Simple Notification Service (Amazon SNS) containing the updated configuration along with the old and new values for each modified attribute. Amazon SNS can, in turn, send an email or SMS notification, trigger an Amazon Lambda function, or put the message in an Amazon Simple Queue Service (Amazon SQS) queue for further processing.

AWS Config Rules evaluates newly discovered resources or configuration changes to existing resources against the desired configuration and displays the results in a consolidated compliance dashboard. AWS Config and AWS Config Rules allow customers to assess the overall compliance and risk status of a network configuration, view compliance trends over time, and pinpoint which configuration change caused a resource to drift out of compliance with a rule.

AWS Config provides comprehensive change notifications that allow network changes to be assessed without searching for the change in the AWS Config console or examining CloudTrail logs. However this approach requires custom development of AWS Lambda functions or EC2 instances with SQS message processors to incorporate the appropriate formatting and business logic so changes can be sent to the appropriate notification system. Therefore, this approach is recommended for more mature customers who are looking for more notification versatility and want to develop more sophisticated change notification systems.

Implementation Guidance

When planning to use AWS Config and AWS Config Rules, first determine whether to use the service reactively or proactively. Some AWS customers use CloudTrail for proactive notification of network configuration changes, and then use AWS Config reactively to further investigate these changes. Other customers process AWS Config change messages for both proactive change notification as well as to further research the history of a change.

To use AWS Config reactively, simply enable the service and it will start creating an inventory of AWS resources and a history of changes. To use AWS Config for proactive change notification, do the following tasks:

- Create an Amazon SNS topic to receive configuration change notifications.
- Develop AWS Lambda function(s) or EC2-based SQS message processors[2] to identify network-specific changes and to send appropriate notifications.

[1] https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/new?stackName=CloudWatchAlarmsForCloudTrail&templateURL=https://s3-us-west-2.amazonaws.com/awscloudtrail/cloudwatch-alarms-for-cloudtrail-api-activity/CloudWatch_Alarms_for_CloudTrail_API_Activity.json

[2] http://docs.aws.amazon.com/config/latest/developerguide/monitor-resource-changes.html

- Consider at least two different recipients for change notifications:
  - A network security email or paging distribution list to receive notifications that require immediate human intervention (e.g., modifying a security group to allow all access globally or attaching an Internet gateway to an internal-only VPC).
  - A central logging or change management system that can be used to reconcile approved change requests with actual configuration changes.
- Subscribe your AWS Lambda function(s) or SQS queues to the change notification SNS topic.
- Configure AWS Config to publish change notifications to the change notification SNS topic.

Network Traffic Monitoring

CloudWatch and CloudWatch Logs

Amazon EC2 instances automatically track aggregate network inbound and outbound traffic with Amazon CloudWatch. Additionally, custom metrics and log files can also be pushed to CloudWatch for metric and log storage, aggregation, reporting and alert notification. These features can be used to profile the expected network behavior for each EC2 instance and trigger alarms when deviations are detected. For example, system or web logs sent to CloudWatch Logs could trigger alarms based on the number of login failures or web request latencies. In another example, TCP connection or outstanding connection request counts could be stored in CloudWatch and used to detect security threats like SYN flood attacks.

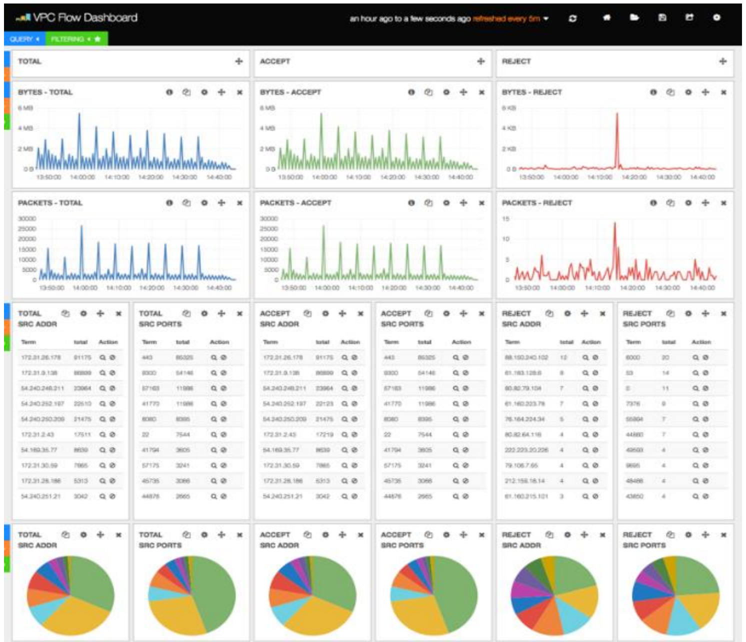
VPC Flow Logs

VPC Flow Logs capture network flow information for a VPC, subnet, or network interface in Amazon CloudWatch Logs. Flow logs can help you with a number of tasks, such as troubleshooting why specific traffic is not reaching an instance, which in turn can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance, to profile your network traffic, and to look for abnormal traffic behaviors. A common use of VPC flow logs is to watch for abnormal and unexpected denied outbound connection requests, which could be an indication of a misconfigured or compromised EC2 instance. CloudWatch Alerts can provide rudimentary network alerting on VPC Flow Logs, however AWS APN members provide third-party log management systems that provide extensive reporting, visualization, and alerting capabilities based on VPC Flow Log data.

Third-Party Solutions

APN members and Marketplace solutions provide excellent network monitoring capabilities that complement AWS native network monitoring features. Third-party network solutions include in-line gateways and host-based monitoring solutions. In-line network gateway solutions are described in more detail in the [Controlling VPC Egress Traffic] Solution Brief. Host-based monitoring solutions range from traditional OS management tools such as SNMP agents, to deep application network usage analysis from APN members like Boundary, to integrated security suites with robust deep packet inspection capabilities and network security as a service offerings from APN members like Alert Logic, Trend Micro, or Threat Stack.

These APN partner offerings also integrate with the AWS monitoring and management data sources described previously to provide unified dashboards. In addition to APN partner products, AWS provides templates for a one-click solution[3] to aggregate and visualize AWS generated network log data with Elasticsearch and Kibana (an example dashboard is depicted in the image to the right). Expect to incorporate both AWS and third-party tools into a holistic network management and monitoring solution.



TOTAL SRC ADDR

Term	total	Action
172.31.26.178	91175	🔍 ⊘
172.31.9.138	86809	🔍 ⊘
54.240.248.211	23964	🔍 ⊘
54.240.252.197	22510	🔍 ⊘
54.240.250.209	21475	🔍 ⊘
172.31.2.43	17511	🔍 ⊘
54.169.35.77	8639	🔍 ⊘
172.31.30.59	7865	🔍 ⊘
172.31.28.186	5313	🔍 ⊘
54.240.251.21	3042	🔍 ⊘

TOTAL SRC PORTS

Term	total	Action
443	86325	🔍 ⊘
9300	54146	🔍 ⊘
57183	11986	🔍 ⊘
41770	11986	🔍 ⊘
8080	8395	🔍 ⊘
22	7544	🔍 ⊘
41794	3805	🔍 ⊘
57175	3241	🔍 ⊘
45736	3066	🔍 ⊘
44876	2665	🔍 ⊘

ACCEPT SRC ADDR

Term	total	Action
172.31.26.178	91175	🔍 ⊘
172.31.9.138	86809	🔍 ⊘
54.240.248.211	23964	🔍 ⊘
54.240.252.197	22123	🔍 ⊘
54.240.250.209	21475	🔍 ⊘
172.31.2.43	17219	🔍 ⊘
54.169.35.77	8639	🔍 ⊘
172.31.30.59	7865	🔍 ⊘
172.31.28.186	5313	🔍 ⊘
54.240.251.21	3042	🔍 ⊘

ACCEPT SRC PORTS

Term	total	Action
443	86325	🔍 ⊘
9300	54146	🔍 ⊘
57183	11986	🔍 ⊘
41770	11986	🔍 ⊘
8080	8395	🔍 ⊘
22	7544	🔍 ⊘
41794	3805	🔍 ⊘
57175	3241	🔍 ⊘
45736	3066	🔍 ⊘
44876	2665	🔍 ⊘

REJECT SRC ADDR

Term	total	Action
88.150.240.102	12	🔍 ⊘
61.183.128.6	8	🔍 ⊘
80.80.79.104	7	🔍 ⊘
61.160.223.78	7	🔍 ⊘
76.164.224.34	5	🔍 ⊘
80.82.64.116	4	🔍 ⊘
222.223.20.226	4	🔍 ⊘
79.106.7.65	4	🔍 ⊘
212.158.18.14	4	🔍 ⊘
61.160.215.101	3	🔍 ⊘

REJECT SRC PORTS

Term	total	Action
6000	20	🔍 ⊘
53	14	🔍 ⊘
0	11	🔍 ⊘
7376	9	🔍 ⊘
55904	7	🔍 ⊘
44860	7	🔍 ⊘
49593	4	🔍 ⊘
9695	4	🔍 ⊘
48486	4	🔍 ⊘
43650	4	🔍 ⊘

[3] https://github.com/awslabs/cloudwatch-logs-subscription-consumer

Resources

Controlling VPC Egress Traffic	https://d0.awsstatic.com/aws-answers/Controlling_VPC_Egress_Traffic.pdf AWS Solution Brief on approaches to control network traffic out of a VPC
IAM in Practice	https://d0.awsstatic.com/aws-answers/AWS_IAM_in_Practice.pdf AWS Solution Brief on IAM best practices and implementation strategies
VPC Security Capabilities	https://d0.awsstatic.com/aws-answers/VPC_Security_Capabilities.pdf AWS Solution Brief on features and considerations for secure VPC design
AWS Service Catalog Product Website	http://aws.amazon.com/servicecatalog/
AWS Marketplace Offerings	Alert Logic https://aws.amazon.com/marketplace/pp/B00DZYG3D6/ Boundary https://aws.amazon.com/marketplace/pp/B0082FE9O8/ Threat Stack https://aws.amazon.com/marketplace/pp/B00ZDTH8EO/ Trend Micro https://aws.amazon.com/marketplace/search/results/ref=dtl_navgno_search_box?page=1&searchTerms=trend+micro
Elasticsearch and Kibana Solution	https://github.com/awslabs/cloudwatch-logs-subscription-consumer