Management and Governance Services

David Tucker

TECHNICAL ARCHITECT & CTO CONSULTANT

@_davidtucker_ davidtucker.net

AWS Management & Governance Services

AWS CloudTrail

AWS CloudFormation

Amazon CloudWatch

AWS Config

AWS Systems Manager

AWS Control Tower

Overview

Reviewing the ecosystem of services that are provided for management

Examining how to create an audit trail with AWS CloudTrail

Exploring how you track infrastructure with CloudWatch and Config

Introducing infrastructure automation with CloudFormation

Looking at operational insights with Systems Manager

Reviewing AWS Organizations leveraging Control Tower

AWS CloudTrail

> “With **CloudTrail**, 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.”

Amazon Web Services

AWS CloudTrail

Inserts audit trail in an S3 bucket or into CloudWatch Logs

Logs events in the regions in which they occur

Meets many compliance requirements for infrastructure auditing

As a best practice, it should be enabled on every AWS account

Can be consolidated into an Organizational trail using AWS Organizations

Compliance requirement

Forensic analysis

Operational analysis

Troubleshooting

AWS CloudTrail Use Cases

Amazon CloudWatch and AWS Config

Managing Infrastructure

Amazon CloudWatch

Provides metrics, logs, and alarms for infrastructure

AWS Config

Continually evaluates infrastructure against a set of rules

AWS Systems Manager

Provides operational data and automation across infrastructure

Amazon CloudWatch

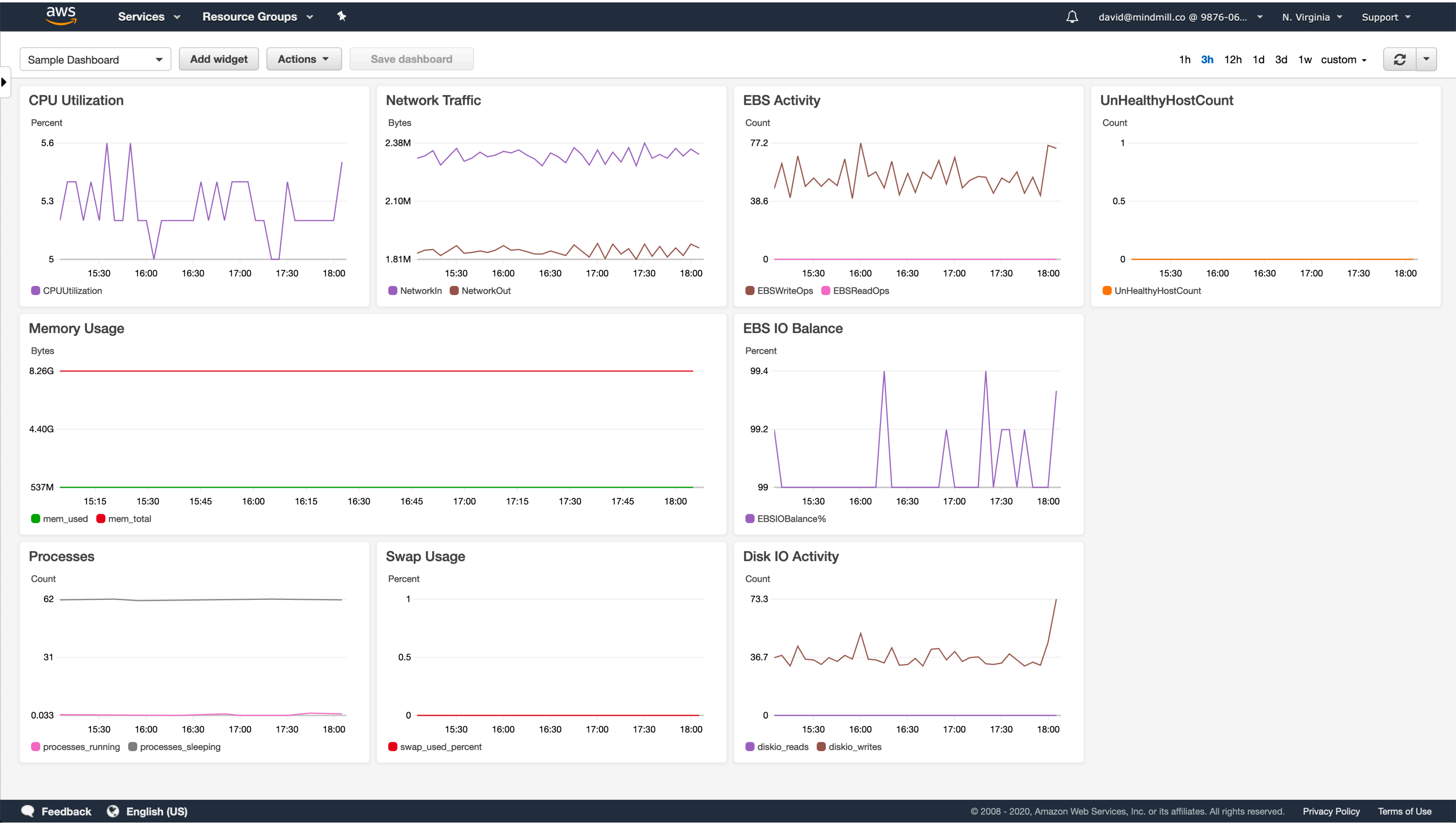
Monitoring and management service

Collects logs, metrics, and events from most AWS services

Enables alarms based on metrics

Provides visualization capabilities for metrics

Allows for custom dashboards based on collected metrics


aws
Services
Resource Groups
david@mindmill.co @ 9876-06...
N. Virginia
Support
Sample Dashboard
Add widget
Actions
Save dashboard
1h
3h
12h
1d
3d
1w
custom
CPU Utilization
Percent
5.6
5.3
5
15:30
16:00
16:30
17:00
17:30
18:00
CPUUtilization
Network Traffic
Bytes
2.38M
2.10M
1.81M
15:30
16:00
16:30
17:00
17:30
18:00
NetworkIn
NetworkOut
EBS Activity
Count
77.2
38.6
0
15:30
16:00
16:30
17:00
17:30
18:00
EBSWriteOps
EBSReadOps
UnHealthyHostCount
Count
1
0.5
0
15:30
16:00
16:30
17:00
17:30
18:00
UnHealthyHostCount
Memory Usage
Bytes
8.26G
4.40G
537M
15:15
15:30
15:45
16:00
16:15
16:30
16:45
17:00
17:15
17:30
17:45
18:00
mem_used
mem_total
EBS IO Balance
Percent
99.4
99.2
99
15:30
16:00
16:30
17:00
17:30
18:00
EBSIOBalance%
Processes
Count
62
31
0.033
15:30
16:00
16:30
17:00
17:30
18:00
processes_running
processes_sleeping
Swap Usage
Percent
1
0.5
0
15:30
16:00
16:30
17:00
17:30
18:00
swap_used_percent
Disk IO Activity
Count
73.3
36.7
0
15:30
16:00
16:30
17:00
17:30
18:00
diskio_reads
diskio_writes
Feedback
English (US)
© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

“**AWS Config** continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.”

Amazon Web Services

AWS Config

Provides configuration history for infrastructure

Works against rules that you can customize or even create custom validations

Includes conformance packs for compliance standards including PCI-DSS

Can work with AWS Organizations for both cross-region and cross-account setup

Provides remediation steps for infrastructure not meeting criteria

AWS Systems Manager

> “**AWS Systems Manager** provides 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.”

Amazon Web Services

AWS Systems Manager

Provides multiple tools that make it easier to manage your AWS infrastructure

Enables automation tasks for common maintenance actions

Gives a secure way to access servers using only AWS credentials

Stores commonly used parameters securely for operational use

AWS CloudFormation

AWS CloudFormation

Managed service for provisioning infrastructure based on templates

No additional charge

Templates can be YAML or JSON

Enables infrastructure as code

Manages dependencies between resources

Provides drift detection to find changes in your infrastructure

```yaml
Description: Creates an S3 bucket

Resources:
  SampleS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: sample-s3-bucket
```

Example CloudFormation YAML

The code above if placed within a full CloudFormation template would create a single S3 bucket

AWS Organizations and Control Tower

AWS Organizations

Allows organizations to manage multiple accounts under a single master account

Provides organizations with the ability to leverage Consolidated Billing for all accounts

Enables organizations to centralize logging and security standards across accounts

AWS Control Tower

A service to create a multi-account environment on AWS that follows the recommended best practices in operational efficiency, security, and governance.

AWS Control Tower

Centralizes users across all AWS accounts

Provides a way to create new AWS accounts based on templates

Integrates Guardrails for accounts

Includes a dashboard to gain operational insights from a single view

Scenario Based Review

Scenario 1

Elliott is an operations engineer at a financial services company

He recently discovered that someone had disabled a security setting on a server

He is concerned that events like this might go unnoticed until a breach

Which service would allow the organization to continually track configuration of infrastructure?

Scenario 2

James is the lead architect at a SaaS company

They will be launching a new application that includes several components

He is looking to minimize manual work required when creating infrastructure

What service would enable James to automate much of this effort?

Scenario 3

Candace is the CTO at a manufacturing company

A cloud server needed to support their manufacturing process was deleted

They want to make sure the follow up with the person who deleted this instance

Which service could show the individual that deleted this specific server?

Summary

Summary

Reviewed the ecosystem of services that are provided for management

Examined how to create an audit trail with AWS CloudTrail

Explored how you track infrastructure with CloudWatch and Config

Introduced infrastructure automation with CloudFormation

Looked at operational insights with Systems Manager

Reviewed AWS Organizations leveraging Control Tower

Scenario 1

Elliott is an operations engineer at a financial services company

He recently discovered that someone had disabled a security setting on a server

He is concerned that events like this might go unnoticed until a breach

Which service would allow the organization to continually track configuration of infrastructure?

Solution: AWS Config

Scenario 2

James is the lead architect at a SaaS company

They will be launching a new application that includes several components

He is looking to minimize manual work required when creating infrastructure

What service would enable James to automate much of this effort?

Solution: AWS CloudFormation

Scenario 3

Candace is the CTO at a manufacturing company

A cloud server needed to support their manufacturing process was deleted

They want to make sure the follow up with the person who deleted this instance

Which service could show the individual that deleted this specific server?

Solution: AWS CloudTrail

Preparing for the Exam