Compliance Benchmarks using Cloud Custodian

Vishnu Varma

Compliance Benchmarks using Cloud Custodian

GIAC GCSA Gold Certification

Author: Vishnu Varma, nvvarma19@hotmail.com
Advisor: Mohammed Haron
Accepted: August 22nd, 2020

Abstract

With the increased cloud adaption rate, many companies are looking for ready to use product available to define the security benchmarks at the beginning of their cloud transition. Companies involved in highly regulated industries such as banking, insurance, finance, and healthcare would also require complying with compliance frameworks. Even though many amazing open-source tools utilized for compliance benchmarks and enforcement, still many organizations chose the commercial tools to fulfill the requirements. The paper will examine multiple compliance benchmarks and frameworks that could enforce policies primarily using Cloud Custodian along with highlighting the ease of use and deployment strategies, mainly covering Amazon Web Services. Cloud Custodian is an open-source tool that provides the ability to set up rules for security, cost optimization, governance, and take action on resources.

1. Introduction

Any organization involved in highly regulated industries such as financial services, insurance, defense, government, and healthcare would need to follow specific compliance frameworks to provide services to their customer. The Organization attaining compliance framework would establish ISMS (Information Security Management System), baseline security checks on the infrastructure, and regularly monitor the baselines (Dutton, 2019). In the process of following specific compliance framework which includes ISO 27001, SOC 1, SOC 2, PCI DSS; Each company would follow the defined controls, which include establishing security policies, asset management, human resources security, communication, and operations management, access controls (Baker, 2019). ISMS (information security management system) is a systematic approach consisting of processes, technology and people that help Organization secure its information, increase the flexibility of the cyber-attacks and defense along with establishing an effective risk management and mitigation strategies. ISO 27001 is one of the most popular, which could is considered a good starting point for the Organization and technology-neutral compliance framework to establish an ISMS (information security management system) (Baker, 2019). According to the Logic Monitor Cloud Vision 2020: The future of the cloud study ("Cloud Vision 2020: The Future of the Cloud Study", 2020), predicts the following:

- 66% of the organizations engaged with the public cloud have identified Security as a Challenge

Vishnu Varma, nvvarma19@hotmail.com

- 60% of the Organization involved with the public cloud have identified Governance and Compliance as a challenge
- In 2020 the survey predicted 41% of the workload would run Public Cloud vs. 31% today, 20% of the workload will run private cloud vs. 19% today, and 22% of the workload will run in the hybrid cloud vs. 18% today.
- Compliance is a significant barrier to business opportunities ("2020 Cyber Report: Compliance Burdens Unsustainable", 2020).

2. Compliance Framework Overview

ISO (the International Organization for Standardization) and IEC (the international electrotechnical commission) formed the specialized system for worldwide standardization. ISO/IEC 27001 is prepared by Join technical committee ISO/IEC JTC 1, Information technology subcommittee SC 27, IT Techniques ("ISO/IEC 27001 Security Standard"). ISO 27001 standard is prepared to provide requirements for establishing, implementing, maintaining, and continually improving an information security management system. According to the IT governance website, All the fortune 500 companies are ISO 27001 certified and have become the de facto standard for Information security management system (ISMS) certification (Baker, 2019). While partnering with companies that are already ISO 27001 certified, a company aligned with the ISO 27001 framework would be beneficial during the business partner due diligence process. ISO 27001 framework has more than 110+ controls, and the requirements fall into 14 categories (Gouveia, 2020):

- Information Security Policies
- Organization of information security

Vishnu Varma, nvvarma19@hotmail.com

- Human resource security
- Asset management
- Access Control
- Cryptography
- Physical and environmental security
- Operations Security
- Communications Security
- Systems Acquisitions, development, and maintenance
- Supplier Relationships
- Information Security incident management
- Information security aspects of business continuity management
- Compliance

To maintain the ISO 27001 compliance, an organization would need to perform four kinds of audits: Certification audit, Internal Audit, Surveillance audit, and recertification audit. The certification audit is the initial audit conducted for the Organization to get an ISO 27001 certificate, which is administered by Certificate body approved auditor. ISO 27001 certificate is issued for three years, and the organization needs to make sure the management systems will be in place as long as the certificate is valid. It requires a surveillance audit to occur at least once a year by an external auditor who is approved by the certification body. Apart from the Surveillance audit, it is required by the Organization to conduct an internal audit to examine the Organization's ISMS to ensure it meets the requirements. Unlike the

surveillance and recertification audit, the internal audit is performed by internal staff with adequate knowledge of the framework.

Organizations with only on-premise infrastructure will need to plan accordingly with frameworks requirements along and make changes to existing policies. Whereas when an organization transitions from on-premise infrastructure to Public cloud providers such as AWS (Amazon Web services), Azure and GCP (Google Cloud provider) can reduce the workload for audit and evidence as cloud provides their compliance certificates.

3. Cloud Custodian

3.1. Overview of Cloud Custodian

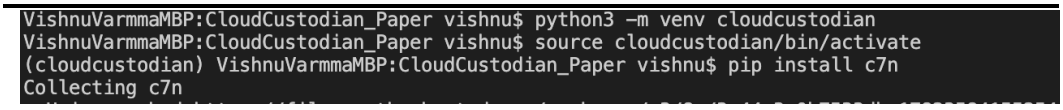
According to the recent Cobalt Compliance survey, it identified that for the majority of the organizations growing compliance obligations are now consuming 40% or more of the IT security budgets and threaten to become an unsustainable cost ("2020 Cyber Report: Compliance Burdens Unsustainable", 2020). Amongst the surveyed organizations, nearly half of the companies end almost 20,000 hours a year to maintain compliance ("2020 Cyber Report: Compliance Burdens Unsustainable", 2020). Automating compliance monitoring of individual sections of the framework will not only reduce the burden but also increase the visibility across cloud environments. With the increasing cost and human effort to keep up with the compliance, deploying an open-source tool for compliance monitoring would help any organization.

Cloud Custodian is an open-source tool which could implement real-time compliance across multi-cloud environment which include Azure, Amazon web services, and Google Cloud provider using simple easy to read DSL (Domain-Specific language). The cloud custodian project was initially developed at CapitalOne and later became one of the most frequently maintained open-source projects. The tool offers multiple ways of deployment and reporting capabilities. The tool will be able to drive real-time enforcement or run the policies on frequent intervals.

3.2. Cloud Custodian Basic Usage

Cloud Custodian rules are straightforward to write because it's in human-readable format and written in YAML. Cloud Custodian have well-maintained documentation, and anyone with the ability to understanding to write a YAML should be able to write any rule. To go over the process of writing a rule, we would be using preferred IDE (visual studio code in my situation) and follow along with documentation to review how easy it is to write a rule. For demonstration purposes, we would be writing a rule to stop RDS public instance. Process of writing a rule from the beginning would be the following:

- Create a virtual environment and install cloud Custodian using the commands:



- I have configured my AWS CLI with credentials associated with sufficient permissions to perform remediations.
- I have created a test database that is publicly accessible for testing purposes.

a.
```
(cloudcustodian) VishnuVarmmaMBP:CloudCustodian_Paper vishnu$ sudo aws rds describe-db-instances --pr
ofile sans --query 'DBInstances[*].[DBInstanceIdentifier,PubliclyAccessible]'
[
    [
        "database-1",
        true
    ]
]
```

- Based on the cloud custodian documentation (Link), created the following code to remediate the RDS instance:

a.
```
policies:
  - name: stop-public-rds-instance
    resource: rds
    filters:
      - PubliclyAccessible: true
    actions:
      - type: modify-db
        update:
          - property: 'PubliclyAccessible'
            value: false
        immediate: true
```

- It is always preferred to run a dry run command before executing the command on infrastructure. The dry run command runs the policy sections before the actions. Each execution of Cloud custodian would generate a folder containing three files: custodian-run.log (see Appendix B), metadata.json (see Appendix C) resources.json (see Appendix A).
- To execute the remediation, all user needs to do is to remove the dry-run command and cloud custodian performs the actions

```
(cloudcustodian) VishnuVarmmaMBP:CloudCustodian_Paper vishnu$ sudo custodian run --profile sans -s . Initial_Rule/Stop-Public-RdsInstance.yml
2020-05-16 20:05:51,966: custodian.policy:INFO policy:stop-public-rds-instance resource:rds region:us-west-2 count:1 time:0.00
2020-05-16 20:05:52,413: custodian.policy:INFO policy:stop-public-rds-instance action:modifydb resources:1 execution_time:0.45
```

- You could notice the change of status of PubliclyAccessible from True to False (refer step 3).

```
(cloudcustodian) VishnuVarmmaMBP:CloudCustodian_Paper vishnu$ sudo aws rds describe-db-instances --profile sans --query 'DBInstances[*].[DBInstanceIdentifier,Public
lyAccessible]'
[
    [
        "database-1",
        false
    ]
]
```

With simple 11 lines of code, any organization would be able to remediate the public RDS issue. Anyone with basic understanding would be able to write and run the cloud custodian policy with less effort vs. having a developer with python programming experience in AWS SDK (Standard Development Kit). Cloud Custodian offers multiple ways for deploying the policies: using a single node (either running on an EC2 instance or ECS), Lambda functions deployed executed based on cron expression ex: every 15 minutes and Lambda function execution based on CloudTrail event configured as the trigger in CloudWatch. Cloud Custodian implements custom lambda function and automatically sets the CloudWatch triggers based on the deployment definition. Deployment of policies is as easy as adding 3-5 lines of code to the existing policy file vs. configuring it manually via aws console or access keys to each policy.

4. Compliance Benchmarks

ISO 27001 compliance framework primarily focuses on organization ISMS (information security management systems), which focuses on policies enforces in ISMS and security/benchmarks applied on infrastructure in scope. Being a vendor-neutral Audit framework, it makes it easy for an organization to define the required security enforcements where applicable. A significant part of the ISO 27001 standards can be enforced through checks or guard rails in place. The compliance

framework mapping section covers the mapping of ISO 27001 objectives to each cloud custodian compliance rule for the AWS environment. Our scope for our paper will be limited to popular services used in AWS which includes IAM (Identity and Access Management), KMS(Key Management System), SNS(Simple Notification Service), S3(Simple Storage Service), SES(Simple Email Service), CloudTrail, CloudWatch, EC2(Elastic Compute Cloud), RDS (Relational Database Service).

4.1. Compliance Framework Mapping

Following are the mapping of ISO standards, let us go over each section and review the objectives to define benchmarks required for the AWS services.

ISO 27001 Section 6: Organization of information security

Description: The primary objective is to enforce general information security implementation, which includes roles, responsibilities, segregations of duties, information security in project management, and mobile device management. Even though the mobile device management section primarily focuses on remote mobile devices and teleworking, but it does require to enforce restrictions on access to information ("ISO/IEC 27001:2013", 2019). The scope could include best practices for VPC and IAM.

AWS Service	Rule Name	Description
VPC	VPC without Flow Logs enabled	Checks for VPCs without Flow logs enabled and automatically configured with the S3 bucket

IAM	Disable IAM keys older than 90 days	Checks for Users with access keys older than 90 days and disable them
IAM	Policy with full IAM permissions	Checks for IAM policies used assigned with full wild card permissions used
EC2	Terminate public instance when launched	Checks for EC2 instances attached with Public IP address via CLoudwatch events
RDS	Terminate Public and Encrypted RDS instance	Terminate RDS instances with Public IP addresses and Unecrypted via the CloudWatch Events.

ISO 27001 Section 8: Asset Management

Description: The primary objective is to require the Organization to setup tagging on each asset in scope covers owners, usage, Data classification, client, or project reference. Along with tagging the assets based on the classification of assets, the Organization can enforce benchmarks for assets.

AWS Services	Rule Name	Description
RDS	Mandatory RDS Tags	Checks for necessary tags, i.e., classification, cost center, project
EC2	Mandatory EC2 Tags	Checks for essential tags, i.e., classification, cost center, project
RDS	Benchmark checks for confidential RDS instance	Checks for Confidential classified RDS instances not implementing the required practices

EC2	Benchmark checks for Confidential EC2 instance	Checks for Confidential, classified EC2 instance with best practices
EC2	Benchmark checks for Public EC2 instance	Checks for public EC2 instances
S3	Benchmarks for Log S3 Buckets	Checks for logs buckets with best practices
S3	Benchmarks for Confidential S3 Buckets	Checks for confidential buckets with best practices
S3	Benchmarks for General S3 Buckets	Checks for general S3 buckets with best practices

ISO 27001 Section 9: Access Control

Description: The primary objective is to restrict limited access to assets and the processing resources in the cloud, which include IAM (Identity Access Management), Security Groups (Access to internal Ports), KMS (Key management service), and other processing services used in the environment.

AWS Service	Rule Name	Description
IAM	Disable IAM keys older than 90 days	Checks for Users with access keys older than 90 days and disable them
IAM	A policy with full IAM permissions	Checks for IAM policies used assigned with full wild card permissions used
IAM	Checks for IAM users with privileged access to permissions management	Identifies Users with access to make changes to permissions
SG	Checks for security port allowing SSH, RDP ports	Identifies security groups which will enable 0.0.0.0 access to SSH and RDP

S3	Checks for S3 buckets against our best practices	Identifies the S3 buckets violating our best practices
KMS	Checks for KMS with the cross-region and high Grant Count	Determines KMS keys violating best practice and Sets Key rotation is disabled
IAM	Checks for Users with Privileged EC2 Access	Identifies Users with access to EC2 privileges
IAM	Checks for Users with Privileged RDS Access	Identifies Users with access to RDS privileges

ISO 27001 Section 10: Cryptography

Description: The primary objective is to make sure the Organization is properly using cryptography. Rules for this section will primarily focus on usage on KMS and its best practices deployed on the cloud.

AWS Service	Rule Name	Description
KMS	Check for non-CMK keys	Rule checks for CMK keys not used
KMS	Check for ViaService Statement not used	Rule checks for KMS Keys not using the ViaService condition
KMS	Check for KMS best practices	Rule checks for KMS general practices
ELB	Classic Load Balancer does not use SSL	Rule checks for non-SSL configured ELB used
ALB	Application Load Balancer configured with HTTP]	Rule checks for ALB configured with HTTP
RDS	Non-encrypted RDS instance used	Rule checks for RDS without encryption
EC2	EC2 instances with non-encrypted EBS Volumes	Rule checks for EC2 instances without un-encrypted EBS volume

ISO 27001 Section 12: Operational Security:

Description: The primary objective is to enforce change management, capacity management, protection from malware, backup, logging, and monitoring. Rules for this section primarily focus on best practices need to by services along with customized rules to cover the topics.

AWS Service	Rule Name	Description
RDS	RDS instance with snapshot retention less than seven days	Rule checks for RDS instances with less than seven days of snapshot retention
RDS	RDS instance without logging setup	Rule checks for RDS instances with no logging setup
EC2	EC2 instances without monitoring used	Rule checks for all the EC2 instances with monitoring state disabled
EBS	EBS volumes which are not fault-tolerant	Rule checks for EBS volumes which do not have snapshots taken for last seven days
S3	S3 Buckets configured without logging	Rule checks for S3 buckets without logging setup
ALB	ALB without logging	Rule checks for ALBs without logging
ELB	ELB without logging	Rule checks for Classic ELB configured without logging
Cloudtrail	Cloud Trails violating best practice	Rules checks for CloudTrail against best practices

ISO 27001 Section 13: Communications security

Description: The primary objective is to make sure the external communication and internal communication is secure between the assets and information processing assets in scope ("ISO/IEC 27001:2013",

2019). Rules for this section primarily focus on network services of AWS, such as VPC, ELB, and Security Groups.

AWS Services	Rule Name	Rule
ELB	Classic Load Balancer does not use SSL	Rule checks for non-SSL configured ELB used
ALB	Application Load Balancer configured with HTTP	Rule checks for ALB configured for HTTP
EC2	Benchmark checks for Public EC2 instance	Rule checks for public EC2 instances
SG	Security Groups allow HTTP	Rule checks for Security group allowing public HTTP

ISO 27001 Section 14: System acquisition, development, and maintenance

Description: The primary objective is to make sure information security is an integral part of the application lifecycle while also includes resources that provide functionality over the public network ("ISO/IEC 27001:2013", 2019). Rules for this section primarily focus on Public instance and general networking-based benchmarks.

AWS Services	Rule Name	Rule
EC2	Benchmark checks for Public EC2 instance	Rule checks for public EC2 instances against best practices
S3	Benchmarks for General S3 Buckets	Rule checks for general S3 buckets with best practices
RDS	Terminate Public and unencrypted RDS instance	Rule terminates RDS instances with Public IP

		addresses and unencrypted via the CloudWatch Events
RDS	Benchmarks for confidential RDS instance	Rule checks for Confidential classified RDS instances not implementing the required practices
SG	Security Groups allow HTTP	Rule Checks for Security group enabling public HTTP
SG	Security Groups allow Public SSH and RDP	Rule checks for Security group allowing public SSH and RDP
RDS	RDS snapshot shared cross-Account	Rule checks for RDS snapshots shared cross accounts
EBS	EBS snapshots shared cross Account	Rule checks for Cross account shared EBS snapshots

ISO 27001 Section 17: Information security aspects of business continuity management

Description: The primary objective of the section is to make sure information security continuity is to plan with the Organization's business continuity during a crisis or natural disaster, which includes the high availability of processing instances ("ISO/IEC 27001:2013", 2019). Rules for this section primarily focus on RDS, EC2 instances configured for Multi-AZ, and backup retention policies.

AWS Service	Rule Name	Description
EC2	Benchmarks for Confidential EC2 instance	Rule checks for Confidential, classified EC2 instance with best practices

EC2	Benchmarks for Public EC2 instance	Rule checks for public EC2 instances against best practices
RDS	RDS with snapshot retention less than seven days	Rule checks for RDS instances with less than seven days of snapshot retention
EBS	EBS volumes which are not fault-tolerant	Rule checks for EBS volumes which do not have snapshots taken for last seven days
RDS	Benchmark checks for confidential RDS instance	Rule checks for Confidential classified RDS instances not implementing the required practices

.

As discussed, the various sections where automated compliance benchmarks implemented, a significant number of rules might be repetitive. For each rule mentioned in the above sections, we have created cloud custodian rules anyone can deploy in their environment and ready to use. Please note the rules may not include all the services used in AWS but would cover essential services, which include S3, IAM (identity access management), EC2 (Elastic Compute Cloud), RDS (Relational Database Service) and KMS (Key Management Service). The link for the GitHub repository is this. The GitHub repository will include details on how to configure Cloud Custodian rules and configure them.

4.2. Benefits of Cloud Custodian

Cloud Custodian offers different ways to deploy rules which include the following:

- Run Cloud Custodian on EC2 instances configured attached with required instances role to run the rules

- Run Cloud Custodian on Docker via supported tool Cask (link)
- Deploy Cloud Custodian on Amazon Web services using Lambda and trigger lambda based on our interval required.

Cloud Custodian also offers different ways to report findings of instances violating rules, which includes producing metrics and results. Each execution of cloud custodian generates three files:

- Custodian-run.log: Contains the output of the cloud custodian (See Appendix B)
- Metadata.json: Contains Metadata generated by the rule and includes metrics as well (See Appendix A)
- Resources.json: Contains all the required information of the resource violating the rule (See Appendix C)

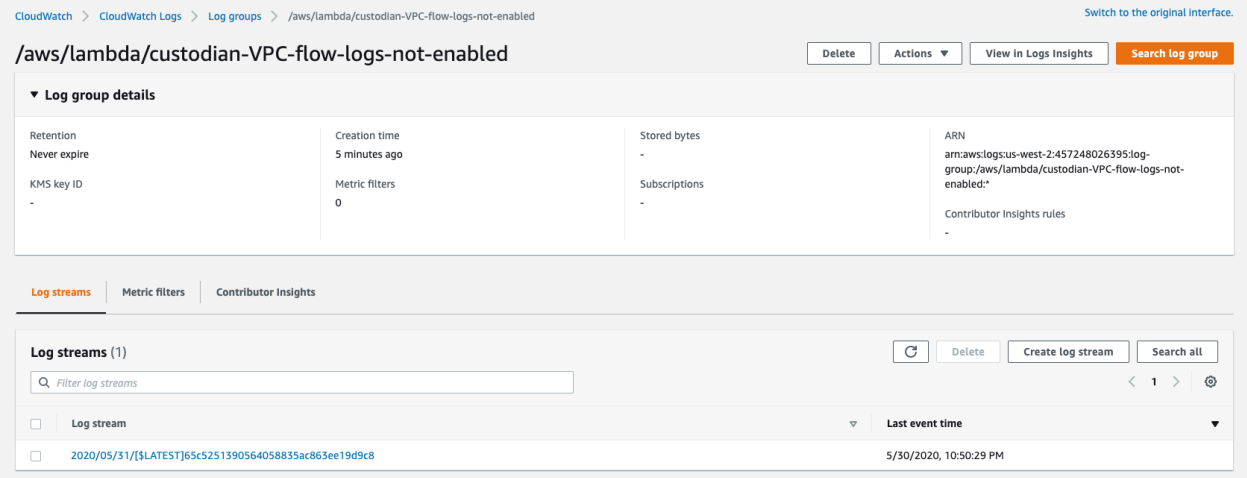
Each execution generates three types of metrics: ResourceCount, ResourceTime, and ActionTime(If Applicable).

Lambda based deployment is the preferred method primarily due to pricing and less overhead. When a policy is configured on lambda deployment, all the user need is to configure the required permission role, and the cloud custodian will deploy the lambda function along with setting the intervals as needed. Cloud custodian configured lambda functions can be customized to output the files to an S3 bucket for analysis or output the metrics to CloudWatch to create dashboards. To demonstrate the lambda-based deployment, we have created a test script that would check for VPC configured without flow logs.

Vishnu Varma, nvvarma19@hotmail.com

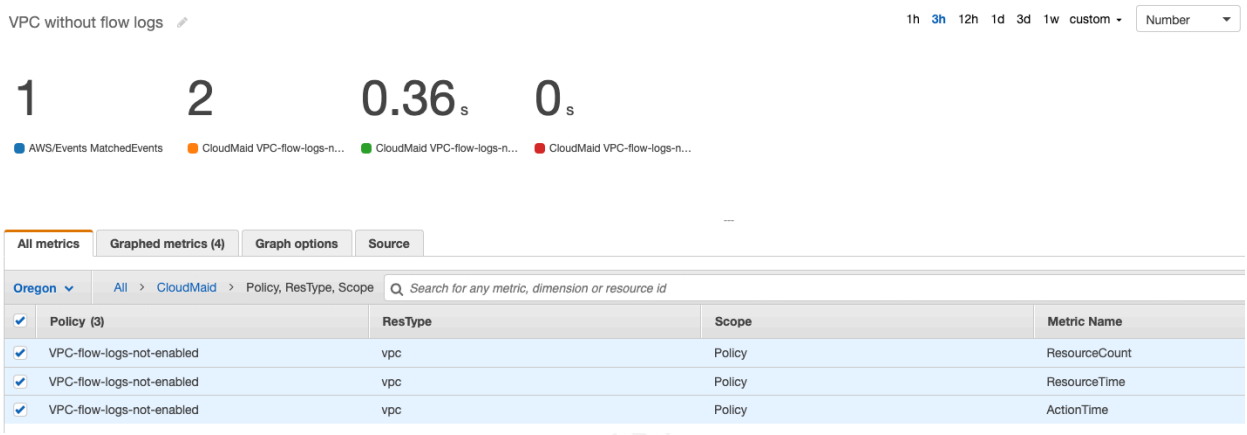
```
policies:
  - name: VPC-flow-logs-not-enabled
    description: |
      Policy which check for VPCs without flow logs enabled
    mode:
        type: periodic
        schedule: "rate(2 minutes)"
        role: custodian
        execution-options:
          metrics: aws
    resource: vpc
    filters:
      - type : flow-logs
        enabled : false
```

Each lambda function deployed through cloud custodian creates a cloud watch log group and creates one log group named after the rule.



Each rule will provide metrics for Resource Count, Resource Time, and Action Time.

Vishnu Varma, nvvarma19@hotmail.com



Cloud custodian rules can be configured output the results to Guard Duty, SSM Ops dashboard, and DataDog. It also notifications through Webhook and email through SES (Simple Email Service).

4.3. Tool Usage

Cloud Custodian lambda function is configured with 512 MB of memory by default. Using Lambda is one of the cheapest ways to run compliance monitoring because it would only run on the required intervals and will not run resources when not required. As per cost analysis, if we configure a rule to run every 15 minutes for 1000 milliseconds execution time, it would only cost 0.02$ per rule even though the duration of each request depends upon the number of resources needed to be scanned by the custodian. User needs to be careful while scanning snapshots, security groups, S3 buckets as these rules would consume more duration of the request. Best recommend practice is to follow the following reduce the interval, Increase the memory, or C7n-salactus (https://cloudcustodian.io/docs/tools/c7n-salactus.html) tool. Custodian Rules are generally very minimal in code with options to run dry-run, CI integration, and validation of the policies before AWS.

Vishnu Varma, nvvarma19@hotmail.com

Each Custodian rule should be considered similar to infrastructure as code, which would include peer review, continuous integration, and continuous delivery pipeline setup. For continuous integration, organizations should enable webhook to the Continuous Integration system when pull requests are open or updated, which continuously tests and validate the policies. The following code configures the pull requests for Azure DevOps which would validate the policies:

```
trigger:
- master

jobs:
  - job: 'Validate'
    pool:
      vmImage: 'Ubuntu-16.04'
    steps:
      - checkout: self
      - task: UsePythonVersion@0
        displayName: "Set Python Version"
        inputs:
          versionSpec: '3.7'
          architecture: 'x64'
      - script: pip install --upgrade pip
        displayName: Upgrade pip
      - script: pip install c7n c7n_azure c7n_gcp
        displayName: Install custodian
      - script: custodian validate policy.yml
        displayName: Validate policy file
```

4.4. General Security Strategy:

At several Cloud conferences, Kapil Thangavelu has talked about Cloud custodian and Cloud Security strategies. While we discussed different cloud custodian deployments and rules, it is also essential to describe security strategy recommended by the tool creators themselves. The following are the few recommended strategies from a Talk at AWS Transformation Day (link):

- Focus on Least Privileges

- Think like Red team around each API
- Implement Preventive cloud controls on AWS IAM
- Implement Detective cloud controls on Discovery and remediation post creation

Highly recommended for any organization interested in deploying cloud custodian to view all the talks at various conferences (see Appendix D),

4.5. Cloud Custodian vs. Commercial Tool

To write the rules set required for ISO 27001 stack, it would take around 30-40 hours because of the ease of writing cloud custodian policies and widely supported AWS services. Regarding the cost analysis of running 100 rules for one month, it would cost only, 2$ including considering the rules run for an average of 1000ms. Even though the execution duration might increase or decrease based on the number of resources identified, it will have an exponential change in the cost. For a team having to implement compliance monitoring using a commercial tool could not be a viable solution as prices might vary from as low as $10,000 to $50,000 for small to medium-sized AWS accounts. For companies with limited budget and resources, implementing compliance monitoring using cloud custodian would be one the most comfortable option and the ability to fully customized the rules. Even though cloud custodian requires an analyst to write the rules for the Organization, the ease of writing the rules and well-maintained documentation will help the analyst while achieving a higher return on investment of time over the next months with

serverless based deployment. There are many tools similar to cloud custodian, which would also enforce compliance monitoring and other benchmarks for the cloud environments.

Each Organization's architecture and usage of cloud resources are different from one another. Even though premium tools cover all the requirements or security measures, not all of them provide the ability to customize according to the Organization's architecture. Instead of learning how to use the premium tool, anyone with an understanding of AWS and Origination's architecture would be able to write cloud custodian rules with a small learning curve. Cloud Custodian covers the majority of the AWS services and runs much faster configured with CloudWatch events. AWS provides a similar config monitoring tool called AWS Config using which anyone can write their own config rules. Organizations utilizing AWS Config can also provision custodian policies as config rules. Cloud Custodian has the ability to email users based on his/her activity violating the Organization's policies.

5. Conclusion

With the increasing cloud adaption rate and requirements for cloud custodian, not all the enterprises would be able to purchase commercial compliance monitoring tool. If you would be able to conduct the sample type of monitoring of the Cloud environments with negligible infrastructure cost will help organizations save time during their due diligence and evidence collection. The rules will be updated to support more AWS services as needed, along with compliance monitoring for GCP, Azure. There is no GitHub repository for Cloud custodian rules,

which provide ready to deploy and maintained rules set for AWS, Azure, and GCP to date. Once achieving ISO 27001 for all three cloud providers will continue to expand the compliance frameworks as needed. It would not only help the Organization deploying open source tools for their compliance monitoring but could also be a starter kit for companies newly transitioning to cloud something they could use since the early stage.

References

Vishnu Varma, nvvarma19@hotmail.com

Dutton, J. (2019, December 18). What is an ISMS? 9 reasons why you should implement one. Retrieved from https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one

Baker, A. (2019, December 19). Why are so many organisations getting certified to ISO 27001? Retrieved from https://www.itgovernance.eu/blog/en/why-are-so-many-organisations-getting-certified-to-iso-27001

Cloud Vision 2020: The Future of the Cloud Study. (2020, January 23). Retrieved from https://www.logicmonitor.com/resource/the-future-of-the-cloud-a-cloud-influencers-survey

2020 Cyber Report: Compliance Burdens Unsustainable. (2020, May 13). Retrieved from https://www.coalfire.com/News-and-Events/Press-Releases/2020-Cyber-Report-Compliance-Burdens-Unsustainabl

ISO/IEC 27001 Security Standard. (n.d.). Retrieved from https://www.ssh.com/compliance/iso-27001/

Gouveia, A. (2020, May 11). Preparing for an ISO 27001 and 27002 Audit. Retrieved from https://reciprocitylabs.com/preparing-for-an-iso-27001-and-27002-audit/

ISO/IEC 27001:2013. (2019, June 3). Retrieved from https://www.iso.org/standard/54534.html

Vishnu Varma, nvvarma19@hotmail.com

Appendix A

Contents of Resources.json file for RDS instance


```
[
 {
   "DBInstanceIdentifier": "database-1",
   "DBInstanceClass": "db.t2.micro",
   "Engine": "mysql",
   "DBInstanceStatus": "available",
   "MasterUsername": "admin",
   "Endpoint": {
     "Address": "database-1.cj7qgzr6gvsh.us-west-
2.rds.amazonaws.com",
     "Port": 3306,
     "HostedZoneId": "Z1PVIF0B656C1W"
   },
   "AllocatedStorage": 20,
   "InstanceCreateTime": "2020-05-17T01:44:52.777000+00:00",
   "PreferredBackupWindow": "07:05-07:35",
   "BackupRetentionPeriod": 7,
   "DBSecurityGroups": [],
   "VpcSecurityGroups": [
     {
       "VpcSecurityGroupId": "sg-9dd32ad8",
       "Status": "active"
     }
   ],
   "DBParameterGroups": [
     {
       "DBParameterGroupName": "default.mysql5.7",
       "ParameterApplyStatus": "in-sync"
     }
   ],
```


Vishnu Varma, nvvarma19@hotmail.com

```
    "AvailabilityZone": "us-west-2c",
    "DBSubnetGroup": {
      "DBSubnetGroupName": "default-vpc-f2ac248a",
      "DBSubnetGroupDescription": "Created from the RDS Management
Console",
      "VpcId": "vpc-f2ac248a",
      "SubnetGroupStatus": "Complete",
      "Subnets": [
        {
          "SubnetIdentifier": "subnet-9dc430c0",
          "SubnetAvailabilityZone": {
            "Name": "us-west-2c"
          },
          "SubnetStatus": "Active"
        },
        {
          "SubnetIdentifier": "subnet-928ee2b9",
          "SubnetAvailabilityZone": {
            "Name": "us-west-2d"
          },
          "SubnetStatus": "Active"
        },
        {
          "SubnetIdentifier": "subnet-08b0aa71",
          "SubnetAvailabilityZone": {
            "Name": "us-west-2b"
          },
          "SubnetStatus": "Active"
        },
        {
          "SubnetIdentifier": "subnet-5afff811",
          "SubnetAvailabilityZone": {
            "Name": "us-west-2a"
          },
          "SubnetStatus": "Active"
        }
      ]
    },
    "PreferredMaintenanceWindow": "sun:12:48-sun:13:18",
    "PendingModifiedValues": {},
    "LatestRestorableTime": "2020-05-17T02:05:00+00:00",
    "MultiAZ": false,
    "EngineVersion": "5.7.22",
    "AutoMinorVersionUpgrade": true,
    "ReadReplicaDBInstanceIdentifiers": [],
    "LicenseModel": "general-public-license",
    "OptionGroupMemberships": [
      {
```

```
        "OptionGroupName": "default:mysql-5-7",
        "Status": "in-sync"
      }
    ],
    "PubliclyAccessible": true,
    "StorageType": "gp2",
    "DbInstancePort": 0,
    "StorageEncrypted": false,
    "DbiResourceId": "db-CTV7HGP2EFHVHOENNYNA7375PM",
    "CACertificateIdentifier": "rds-ca-2019",
    "DomainMemberships": [],
    "CopyTagsToSnapshot": true,
    "MonitoringInterval": 0,
    "DBInstanceArn": "arn:aws:rds:us-west-2:457248026395:db:database-
1",
    "IAMDatabaseAuthenticationEnabled": false,
    "PerformanceInsightsEnabled": false,
    "DeletionProtection": false,
    "AssociatedRoles": [],
    "MaxAllocatedStorage": 24,
    "Tags": [],
    "c7n:MatchedFilters": [
      "PubliclyAccessible"
    ]
  }
]
```


Appendix B

Contents of Custodian-run.log

```
2020-05-16 19:09:46,307 - custodian.policy - INFO - policy:stop-public-
rds-instance resource:rds region:us-west-2 count:1 time:0.57
```

Appendix C

Contents of Metadata.json

```
{
```

Vishnu Varma, nvvarma19@hotmail.com

```
"policy": {
  "name": "stop-public-rds-instance",
  "resource": "rds",
  "filters": [
    {
      "PubliclyAccessible": true
    }
  ],
  "actions": [
    {
      "type": "modify-db",
      "update": [
        {
          "property": "PubliclyAccessible",
          "value": false
        }
      ],
      "immediate": true
    }
  ]
},
"version": "0.9.1",
"execution": {
  "id": "34836294-786e-48f7-a0ee-64af2c654735",
  "start": 1589681385.723959,
  "end_time": 1589681386.308218,
  "duration": 0.584259033203125
},
"config": {
  "region": "us-west-2",
  "regions": [
    "us-west-2"
  ],
  "cache": "~/.cache/cloud-custodian.cache",
  "profile": "sans",
  "account_id": "457248026395",
  "assume_role": null,
  "external_id": null,
  "log_group": null,
  "tracer": null,
  "metrics_enabled": null,
  "metrics": null,
  "output_dir": ".",
  "cache_period": 15,
  "dryrun": true,
  "authorization_file": null,
  "subparser": "run",
  "config": null,
```

```
    "configs": [
      "Initial_Rule/Stop-Public-RdsInstance.yml"
    ],
    "policy_filters": [],
    "resource_types": [],
    "verbose": null,
    "quiet": null,
    "debug": false,
    "skip_validation": false,
    "command": "c7n.commands.run",
    "vars": null
  },
  "sys-stats": {},
  "api-stats": {
    "rds.DescribeDBInstances": 1,
    "tagging.GetResources": 1
  },
  "metrics": [
    {
      "MetricName": "ResourceCount",
      "Timestamp": "2020-05-16T19:09:46.307670",
      "Value": 1,
      "Unit": "Count"
    },
    {
      "MetricName": "ResourceTime",
      "Timestamp": "2020-05-16T19:09:46.307680",
      "Value": 0.5683269500732422,
      "Unit": "Seconds"
    }
  ]
}
```


Appendix D

Cloud Custodian Youtube Talks

- https://www.youtube.com/watch?v=oY8Nmh6B7P8
- https://www.youtube.com/watch?v=7psvM3r_wCg
- https://www.youtube.com/watch?v=7psvM3r_wCg
- https://www.youtube.com/watch?v=hm9Bx2MHyNw
- https://www.youtube.com/watch?v=gBIrMIixMUE&t

Vishnu Varma, nvvarma19@hotmail.com

- https://www.youtube.com/watch?v=e2lT2i7zqOM
-

Last Updated: October 25th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**