



PacBot – Open Source Compliance Automation Tool

Published by **Setu** on February 24, 2019

What is PacBot?

f PacBot is Policy as Code Bot which does continuous compliance monitoring, compliance reporting and security automation for AWS(as of the date I am writing this post) from T-Mobile. In PacBot, security and compliance policies are implemented as a code. All resources discovered by PacBot are evaluated against a set of policies to gauge policy conformance.

How to Install PacBot?

Installation instructions for PacBot are located [here](#) on their official GitHub repo. However, there are some prerequisites that needs to be installed and you can use this EC2 User Data script to automate the prerequisites installation process as well. **Kathy** deploying PacBot and finally was able to deploy with a t2.medium instance.

```
1. #!/bin/bash
2. #EC2 user script to install Pacbot p
3.
4. #Setting up Prereqs
5.
6. cd /opt
7. yum update -y
8. yum install git -y
9. yum install wget -y
10.
```

Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift

```

11. #Install and setup Python3.6
12.
13. yum install epel-release -y
14. yum install python36-pip -y
15. echo alias python3=python3.6 >> ~/.bashrc
16. echo alias pip3=pip3.6 >> ~/.bashrc
17. source ~/.bashrc
18.
19. #Clone Repo
20.
21. git clone https://github.com/tmobile/pacbot.git
22.
23. #Other Prereqs
24. yum -y install java-1.8.0-openjdk docker maven unzip mysql
25. systemctl start docker
26. wget https://releases.hashicorp.com/terraform/0.11.8/terraform_0.11.8_linux_amd64.zip
27. unzip terraform_0.11.8_linux_amd64.zip
28. mv terraform /usr/bin/
29. pip3.6 install -r /opt/pacbot/installer/requirements.txt
30.
31. #Setup UI components
32. sudo yum install nodejs npm -y
33. cd /opt/pacbot/webapp
34. npm install -g @angular/cli@1.6.8
35. sudo npm install -g bower
36. sudo npm install
37. bower install --allow-root
38.
39. #Copy the default Settings file and create a local.py
40. cp /opt/pacbot/installer/settings/default.local.py
   /opt/pacbot/installer/settings/local.py

```

f

Once the EC2 server is ready to use, you need to update the local.py settings file with the Access Keys, VPC ID, Subnets(different regions), etc and other requested information. The final steps are to launch the UI and kick off the terraform build script.

```

1. vim /opt/pacbot/installer/settings/local.py
2.
3. AWS_ACCESS_KEY = "<>"
4. AWS_SECRET_KEY = "<>"
5. AWS_REGION = "<>"
6. VPC ID: "<>",
7. CIDR_BLOCKS: ["<>"],
8. SUBNETS: ["<>", "<>"]
9. }
10. # Launch UI
11. ng serve &>/dev/null
12. python3.6 /opt/pacbot/installer/manager.py install

```

Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift

It will take up to 20mins to complete the terraform build. Once the build is completed you should be able to access the Internal ELB URL using a windows server launched within the same VPC or using a

VPN tunnel between the VPC and your on-prem network. Don't forget to update the security group rules to use the Pacbot Internal ELB from you on-prem network. Note the summary of the build success message to access Kibana and Elasticsearch cluster URLs that were generated as a part of the build process.

What are the services that the PacBot Installer script deployed?

IAM Roles, IAM Policies, S3 Bucket, RDS, MySQL 5.6.X, Elasticsearch Service, Elasticsearch version 5.5, Redshift, Single Node, Batch, Compute environments, Job Definitions and Job Queues, Elastic Container Registry, Repositories – for batch job, API and UI, Elastic Container Service – AWS Fargate, Clusters – for APIs, UI and Batch, Task Definitions – for APIs and UI, Lambda Functions, SubmitBatchJob and SubmitRuleJob, CloudWatch Rules

How does PacBot does Compliance Automation?

Pacbot discovers resources using AWS Batch Jobs and these assets are evaluated against [predefined policies](#)(~60) to gauge policy conformance. We can also create and write custom policies as per our organizational compliance needs. There are two main batch jobs that are responsible to achieve compliance monitoring

1. PacBot Rule Engine – Runs a predefined set of rules against the assets discovered by PacBot data collector
2. PacBot Data Collector – Set of batch jobs that run and discover resources in an AWS Account and stores the information

Screenshots from my PacBot Deployment in a sandbox environment:

Job queues
You submit AWS Batch jobs to a job queue. Job queues are given a priority value and job queues with a higher integer value for priority are given preference for compute resources.

Create queue Edit Enable Delete

Queue name	Priority
pacbot-rule-engine	6
pacbot-data	6

Compute environments
Compute environments contain EC2 instances that are used to run containerized batch jobs. In a managed compute environment AWS handles the instances.

Create environment Edit Enable Delete

Name	Type	Provisioning model	Instance types	Status
pacbot	MANAGED	EC2	m4.xlarge	VALID

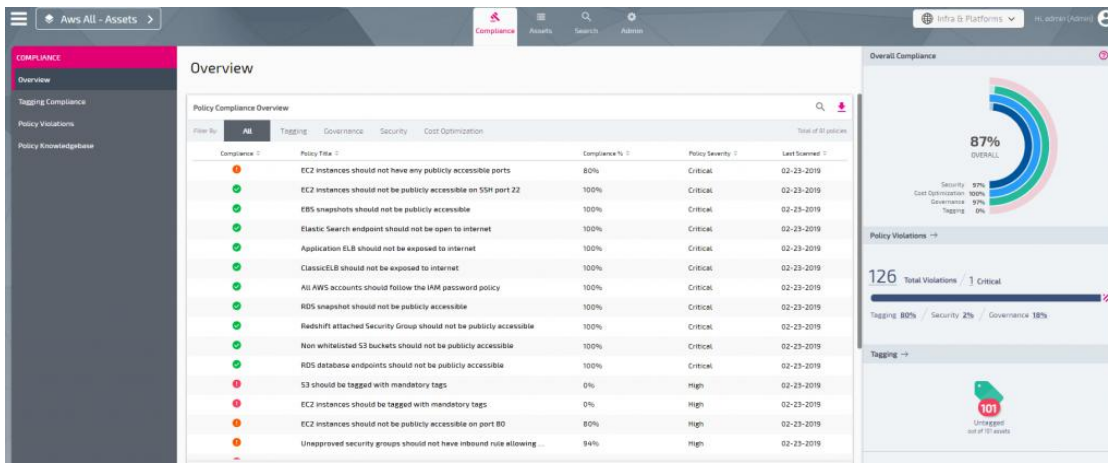
PacBot Compute Environment for running the Batch Jobs

Chat overlay:
Kathy
Welcome to CloudSecOps! What brought you here to check us out?
Type your message...
Chat ⚡ by Drift

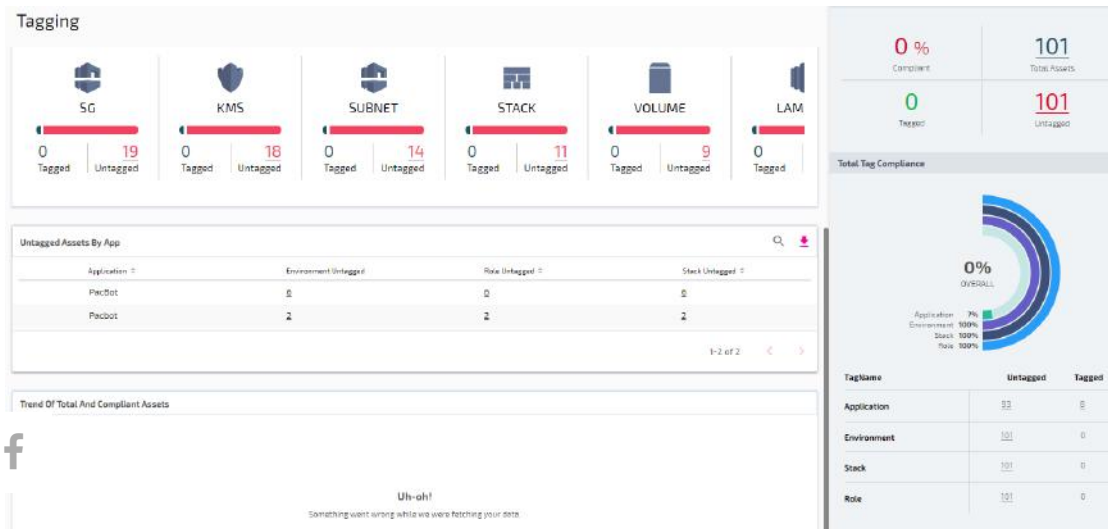
batch Jobs Dashboard

Snippet of a few PacBot CloudWatch Rules

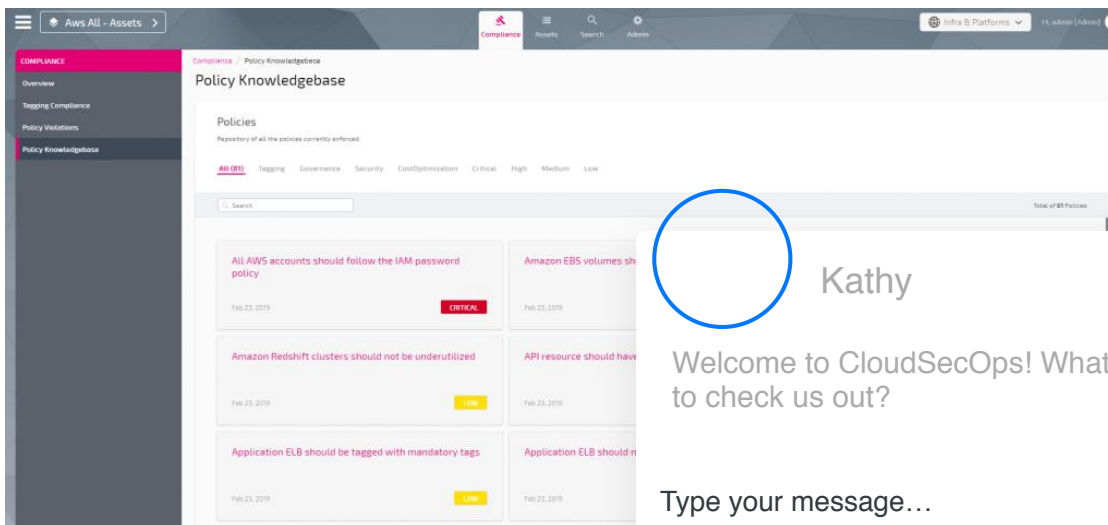
4/15



Asset Overview Board

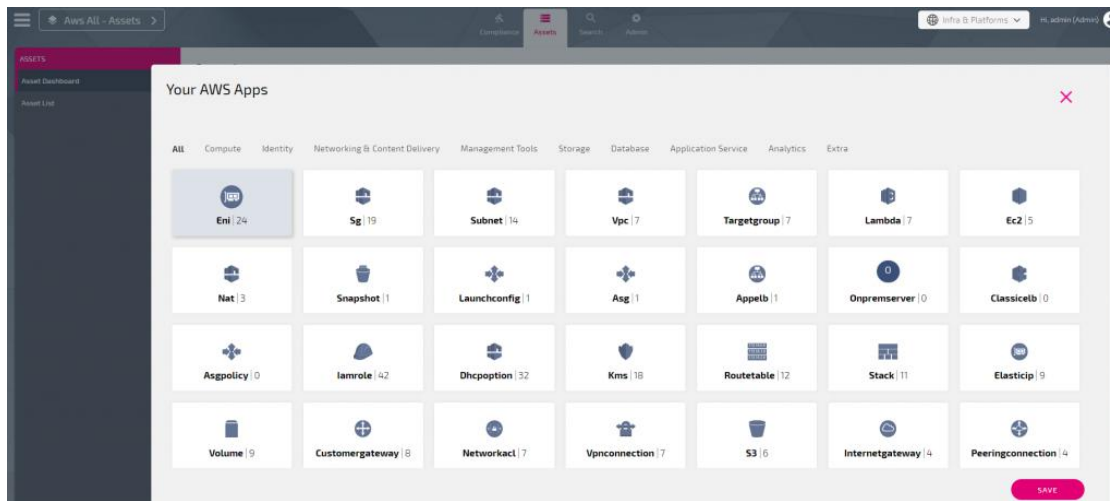


Tagging Compliance Dashboard(Facing Issues here, working on troubleshooting)

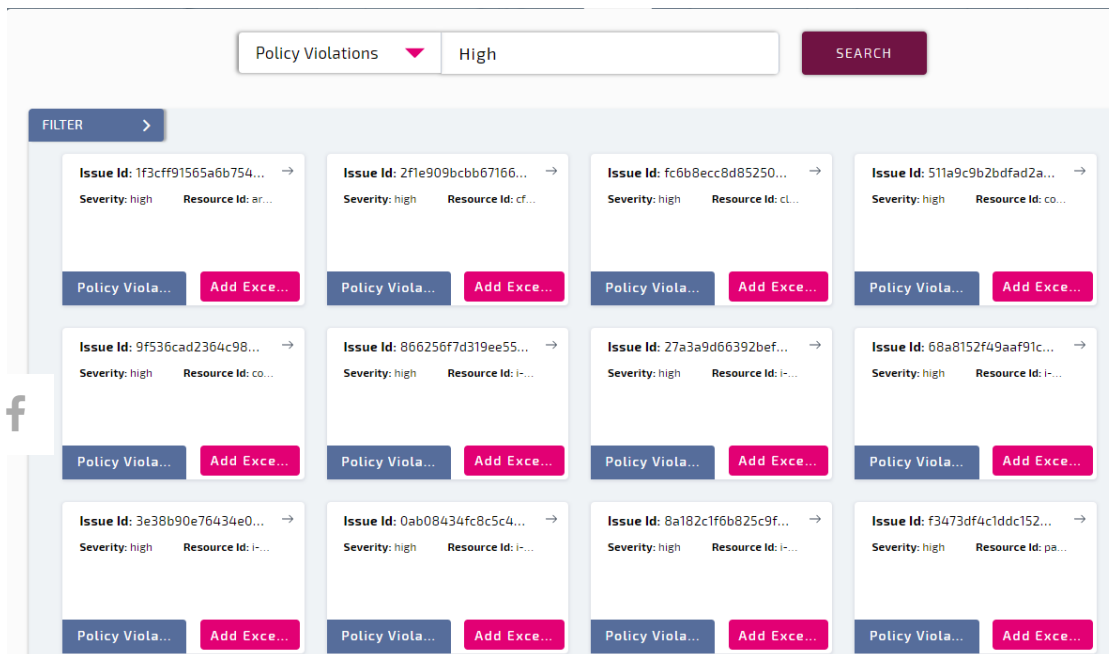


Policy

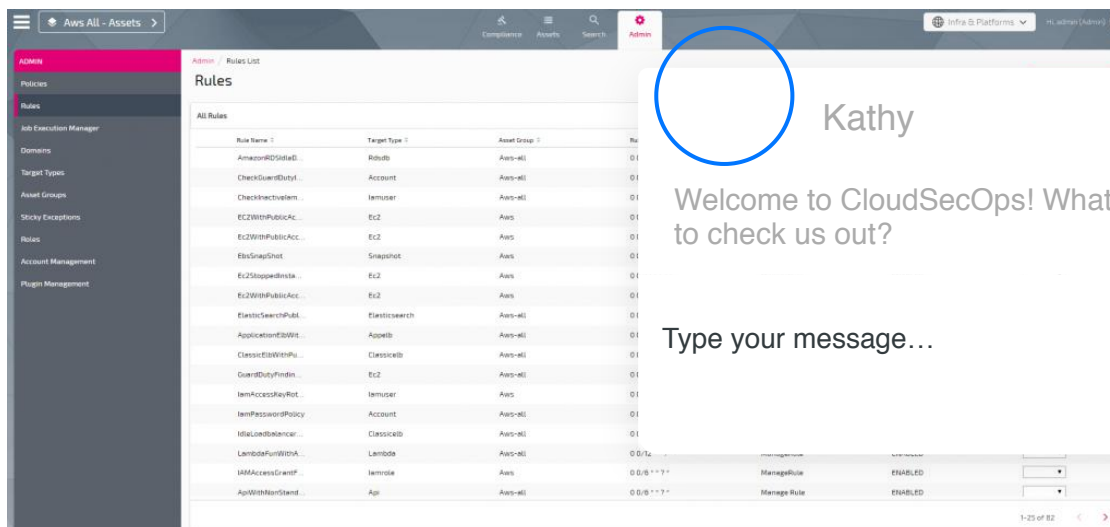
Chat ⚡ by Drift



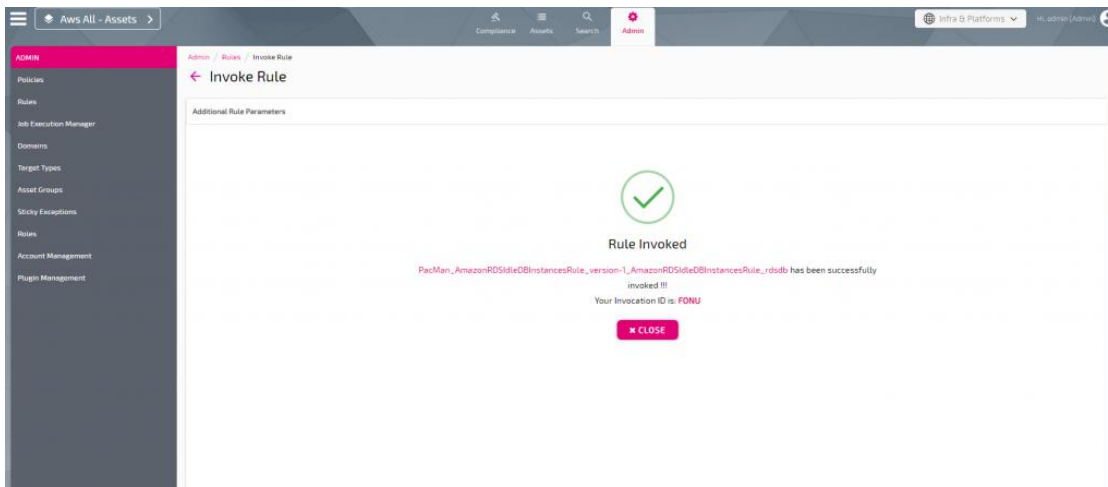
Assets Dashboard



Policy Violation Search Wizard



Admin – Panel – Compliance Rules



Invoking Ad-Hoc Rules

What are the currently available admin features?

- Create Asset Group
- Update Asset Group
- Delete Asset Group
- Rule/Policy Configuration
- Rule Troubleshooting

How to add multiple AWS Accounts to be monitored PacBot?

1. **IAM Role Changes** The account where PacBot is installed is called base account. The accounts that are monitored by PacBot is called client account.
 - Client Account Change: Create an IAM role named pacbot_ro and attach ReadOnlyAccess, AmazonGuardDutyReadOnlyAccess & AWSSupportAccess policies. Allow pacbot_ro from the base account to assume this role. Sample trust configuration for pacbot_ro role is here

1.

```
{  "Version": "2012-10-17",  "Statement": [    {      "Effect": "Allow",      "Principal": {        "AWS": [          "arn:aws:iam::Base_Account_ID:role/pacbot_ro"        ]      },      "Action": "sts:AssumeRole"    }  ]}
```

1. Base Account Change: Fetch client account ID and policy which is associated with pacbot_ro role.

1.

```
{  "Version": "2012-10-17",  "Statement": [    {      "Effect": "Allow",      "Principal": {        "AWS": [          "arn:aws:iam::Client_Account_ID_1:role/pacbot_ro",          "arn:aws:iam::Client_Account_ID_2:role/pacbot_ro"        ]      },      "Action": "sts:AssumeRole"    }  ]}
```

Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift

1. Cloudwatch Rule Changes

- Update “**accountinfo**” value (in *Constant (JSON text)* of cloudwatch rule) with new client account ids in cloudwatch rule named “**AWS-Data-Collector**”. Sample configuration is `{"encrypt":false,"value":"Base_Account_ID,Client_Account_ID_1,Client_Account_ID_2","key":"accountinfo"}`

References:

<https://github.com/tmobile/pacbot/wiki>

My Personal Experiences:

- Batch Jobs fail several times while running policy engine rule, and asset collection. The fix would be going ahead and manually invoking the PacBot asset collector lambda function with the using the cloudwatch rule JSON payload
- Create a private hosted zone in AWS and map the internal ELB URL as a CNAME
- Add SSL certificate to Internal ELB and Map the targets with appropriate PacBot Services using Target Rules in ELB
- There will be a need for reverse DNS resolver that needs to be added to AWS Route 53 to access PacBot private hosted zone CNAME from you internal on-prem network.
- Change the default password of PacBot admin by performing a simple CRUD to PacBot RDS database, instructions are available in PacBot Wiki
- The instance which was used to build PacBot setup can be converted to a t2.micro for cost optimization. Rules can be configured based to run as per your organization time requirements to save the cost related to AWS Fargate/ECS/Batch Jobs.
- Several issues can occur during the deployment and during the build destroy process, you can reach PacBot team and they are “VERY” good at providing some valuable suggestions to resolve the issues. Their Gitter chat URL: <https://gitter.im/TMO-OSS/PacBot>

Thank you for reading! – [Setu Parimi](#) & Steve

Sign up for the blog directly [here](#).

Check out our professional services [here](#).

Feedback is welcome! For professional service contact setu@cloudsecops.com

Share this:



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by [Drift](#)



Like this:

Loading...

Related[Security audit using Cloud Custodian for compliance in AWS](#)

June 15, 2018

In "Amazon Web Services"

[Post Exploitation in AWS using Nimbostratus](#)

June 23, 2018

In "Cloud Penetration Testing"

[Auditing AWS Environments for HIPAA Compliance](#)

July 16, 2018

In "Cloud Security"

Categories: **CLOUD SECURITY TOOLS**Tags: [#compliance](#) [awssecurity](#) [monitoring](#)

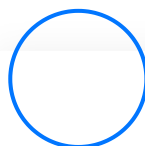
Leave a Reply

Name *

Email *

Website

What's on your mind?



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by [Drift](#)☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.☐ I'm not a spammer.

POST COMMENT

Search ...



Subscribe

Always be the first to know news related to Cloud Security. We will never spam you.

Email Address

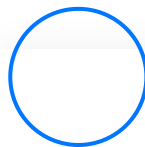
SUBSCRIBE



Categories

[Amazon Web Services](#)[Cloud Penetration Testing](#)[Cloud Security](#)[Cloud Security Tools](#)[Cloud Security Tutorial](#)[Uncategorized](#)

Recent Posts

[PacBot – Open Source Compliance Automation Tool](#)[Automated Remediation for CloudTrail Disruption](#)

Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

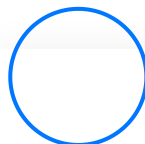
Chat ⚡ by [Drift](#)

[Shifting strategy from DevOps to DevSecOps](#)

[Auditing AWS Environments for HIPAA Compliance](#)

[AWS Post Exploitation – Part 1](#)

Related Posts



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by [Drift](#)



The screenshot shows the CloudSploit web interface. On the left is a dark sidebar with navigation links. The main content area displays a table of scan results for AWS IAM policies. Below the table, there are sections for 'Next Steps', 'Additional Info', and 'Recommended Action'.

Category	Item	Region	Result	Item ID	Resource	More Info
iam	Amazon S3 Access	global	fail	arn:aws:iam::123456789012:policy/AmazonS3Access	arn:aws:iam::123456789012:policy/AmazonS3Access	Check if using both access keys
iam	Amazon S3 Access	global	pass	arn:aws:iam::123456789012:policy/AmazonS3Access	arn:aws:iam::123456789012:policy/AmazonS3Access	Check if not using both access keys
iam	Amazon S3 Access	global	pass	arn:aws:iam::123456789012:policy/AmazonS3Access	arn:aws:iam::123456789012:policy/AmazonS3Access	Check if not using both access keys
iam	Amazon S3 Access	global	pass	arn:aws:iam::123456789012:policy/AmazonS3Access	arn:aws:iam::123456789012:policy/AmazonS3Access	Check if not using both access keys
iam	The latest IAM Policies	global	pass	arn:aws:iam::123456789012:policy/AmazonS3Access	arn:aws:iam::123456789012:policy/AmazonS3Access	Check if using attached or inline policies

Next Steps
Review IAM policies and permissions closely to IAM users.

Additional Info
The IAM policy management console, IAM permissions should only be assigned to roles and groups. Roles can then be added to those groups. Policies should not be applied directly to IAM users.

Recommended Action
Review groups with the required policies, move the IAM users to the existing groups and then remove the roles and directly attached policies from the IAM user.

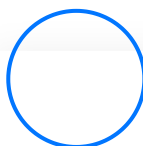
Link
[https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices-for-groups-for-permissions.html](#)



CLOUD SECURITY

Auditing AWS Environments for HIPAA Compliance

Introduction CloudSploit is an AWS compliance, security and configuration monitoring scanner which is the first of its kind. It is an open source project designed to detect security risks in AWS. The CloudSploit Scans is built [Read more...](#)



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift

- **Nimbostratus:** Tool for fingerprinting and exploiting Amazon cloud infrastructures.

- Using Nimbostratus for dumping permissions

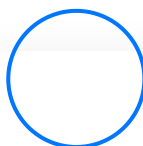
```
./nimbostratus dump-permissions --access-key .....  
--secret-key ..... --token .....
```

```
root@kali:~/nimblestratus# ./nimblestratus dump-permissions --access-k
ken PQ00Yd20S4a000Fk/GapK/R67rpk34wZr100Mv81Ps+sc1ixw8c/3KsoyCh4F
320R13oxup0oyYr0k53vY2p08M478yVt0r0w00F0/747pm1Ym00x0ejw111Le
yP000ge1E{8aw}c}12C8A8yA0K{4dYt0r00y78Pk+/1q7h03E25P0azv+Tryn3
F/8j750+Ep91k1L8P00c1HvCqC4C9y3C00W18qC1r2w44g5cc+Rj8dv00T8p00y+P
3p1t0fy1AN004500X00T8P00w15K2AM=
{"statement": [{"action": ["DescribeImages",
                           "DescribeInstances",
                           "DescribeInstanceStatus",
                           "ListImages",
                           "DescribeOptimizedImages",
                           "DescribeOSSecurityGroups",
                           "DescribeOSSnapshots"],
                  "effect": "Allow",
                  "resource": "*"}]}
```



CLOUD PENETRATION TESTING

Introduction Nimbostratus is a tool developed by Andres Riancho for fingerprinting and exploiting Amazon cloud infrastructures. Nimbostratus uses any application level HTTP proxy vulnerability to enumerate the instance and credentials from the metadata service which [Read more...](#)



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift



Cloud Custodian

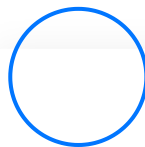


AMAZON WEB SERVICES

Security audit using Cloud Custodian for compliance in AWS

Introduction In this article, we will be talking about Cloud Custodian, an open source rules engine for fleet management in AWS. The simple YAML DSL allows you to easily define rules to enable a well-managed

[Read more...](#)



Kathy

Welcome to CloudSecOps! What brought you here to check us out?

Type your message...

Chat ⚡ by Drift

