

Module 2: Security Management in AWS

Demo Document 6

edureka!

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

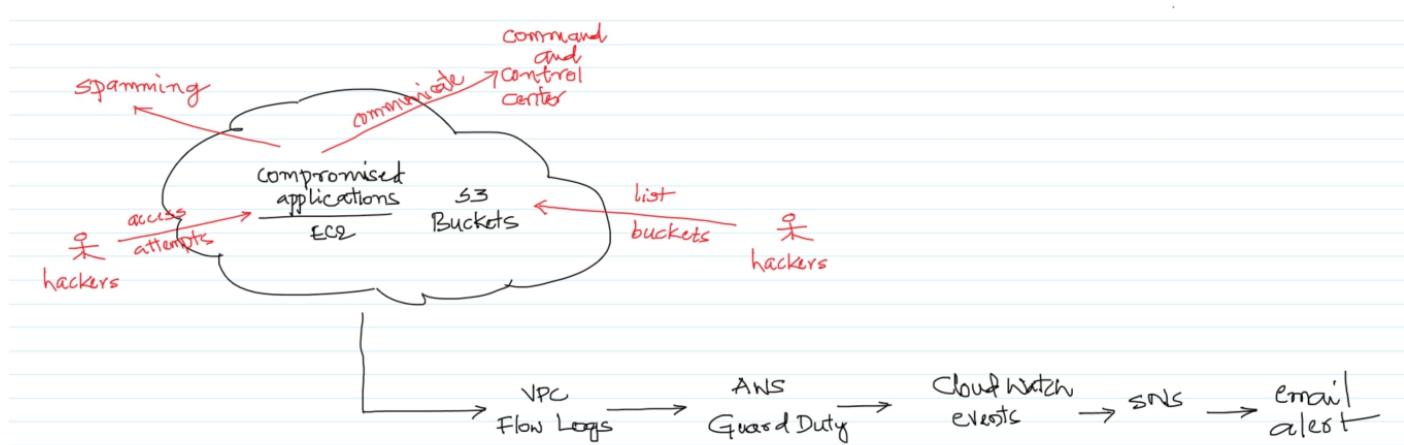
Title: Monitoring Malicious Activity or Unauthorized Behaviour via GuardDuty

Use Case

When we deploy any resources in AWS — whether it's public-facing or private — the hackers always attempt to break into the resources and steal the confidential data to exploit them to their advantages. These resources can be an EC2 instance, an S3 Bucket, an RDS instance, or anything else. While the hackers always look for loopholes to break into the systems, the onus is on the company to protect themselves before hackers can exploit the vulnerabilities to compromise your systems.

To address this challenge, AWS provides Amazon GuardDuty: A managed service that continuously monitors your resources for any malicious activity or unauthorized behavior, thus helping you protect your AWS accounts and workloads. Once Amazon GuardDuty is enabled, it automatically monitors for

- Anomalous API activity
- Potentially unauthorized deployments and compromised instances
- Reconnaissance by attackers



In this use case, we will perform the below activities and check if GuardDuty is able to identify them and alert us. These are the scenarios of a hacker attempting to break into a system or a compromised system.

- Create a Windows EC2 instance and make a connection to a TorGuard or an Authority node.
- Hacker performing some reconnaissance from Kali Linux on the S3 buckets.
- Invoking AWS API using root credentials.

All of the above involve network traffic, which can be captured by the VPC Flows and which GuardDuty automatically analyzes and checks for any anomaly. In the event of an anomaly detected, it sends an event to CloudWatch, which in turn triggers an email via SNS service.

Note that in this use case, we will create an EC2 instance and an S3 bucket to perform some of the steps typically performed by hackers. We will also check if GuardDuty is able to identify them and notify us.

AWS Services: GuardDuty, EC2, S3, VPC, CloudWatch, SNS, SES

Step 1: Navigate to the SNS Management Console and enter the **Topic name** and click on **Next step**.

The screenshot shows the AWS SNS Management Console. On the left, there's a sidebar with 'Amazon SNS' selected. The main content area has a dark header 'Amazon Simple Notification Service' with the subtitle 'Pub/sub messaging for microservices and serverless applications.' Below this, there's a section titled 'Benefits and features' with several cards: 'Reliably deliver messages with durability', 'Automatically scale your workload', 'Simplify your architecture with Message Filtering', and 'Keep messages private and secure'. To the right, there are three boxes: 'Create topic' (with 'Topic name' set to 'GuardDutyTopic'), 'Pricing' (mentioning no upfront costs), and 'Documentation' (links to Developer Guide, API Reference, FAQs, and Support forums). At the bottom, there's a footer with links for Feedback, English (US), and various AWS services.

Step 2: Go with all the default options and click on **Create topic**.

The screenshot shows the 'Create topic' wizard in the AWS SNS Management Console. The 'Name' field is set to 'GuardDutyTopic'. The 'Encryption - optional' section is expanded, stating 'Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.' Other sections like 'Access policy - optional', 'Delivery retry policy (HTTP/S) - optional', 'Delivery status logging - optional', and 'Tags - optional' are also present but collapsed. The 'Create topic' button is located at the bottom right of the form.

Step 3: Click on Create subscription.

The screenshot shows the 'Amazon SNS' service in the AWS console. The left sidebar has 'Topics' selected under 'Amazon SNS'. The main content area shows the 'GuardyDutyTopic' configuration. The 'Subscriptions' tab is active, displaying a table with no rows. At the top of the table, there is an orange 'Create subscription' button. Other tabs include 'Access policy', 'Delivery retry policy (HTTP/S)', 'Delivery status logging', 'Encryption', and 'Tags'.

Step 4: Select Email for the Protocol and the email address for the Endpoint. Click on Create subscription.

The screenshot shows the 'Create subscription' wizard. Step 1: Details. Topic ARN: arn:aws:sns:us-east-1:304000509264:GuardyDutyTopic. Protocol: Email. Endpoint: ugetaws@gmail.com. Note: After your subscription is created, you must confirm it. Step 2: Subscription filter policy - optional. Step 3: Redrive policy (dead-letter queue) - optional.

Step 5: When SNS sends an email, open it and click on the link to change the status of the subscription: From **pending** to **confirmed** status. Once in a while, the email is marked as spam. So, ensure to check the spam folder every now and then.

The screenshot shows the AWS SNS Subscriptions page. On the left, there's a sidebar with options like Dashboard, Topics, Subscriptions (which is selected), and Mobile (Push notifications, Text messaging (SMS)). The main content area shows a subscription details card for a topic named 'GuardyDutyTopic'. The ARN is listed as 'arn:aws:sns:us-east-1:304000509264:GuardyDutyTopic:5f20e345-8576-44ec-b848-4cdffa124f263'. The status is 'Confirmed' with a green circular icon. The endpoint is 'ugetaws@gmail.com'. The protocol is 'EMAIL'. Below this, there are tabs for 'Subscription filter policy' (selected) and 'Redrive policy (dead-letter queue)'. The 'Subscription filter policy' section contains a note: 'No filter policy configured for this subscription. To apply a filter policy, edit this subscription.' An 'Edit' button is present. At the bottom of the page, there are links for Feedback, English (US), and a copyright notice: '© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.

Security Management in AWS

Step 6: Go to the CloudWatch Management Console and then to the **Rules** tab. Click on **Create rule**.

The screenshot shows the AWS CloudWatch Events console. On the left, there's a navigation sidebar with various monitoring services like CloudWatch Metrics, CloudWatch Logs, CloudWatch Alarms, and CloudWatch Events. The 'Events' section is expanded, and 'Rules' is selected. The main content area is titled 'Rules' and contains a message: 'CloudWatch Events is now Amazon EventBridge'. It provides a brief description of EventBridge and a link to its documentation. Below this, there are buttons for 'Create rule' and 'Actions'. A table lists rules, with a single entry: 'You have no rules.' At the bottom, there are links for 'Feedback', 'English (US)', and copyright information.

Step 7: Enter the attached event-pattern.json in the **Event Source**. Click on **Add target**.

The screenshot shows the 'Step 1: Create rule' dialog. The left sidebar is identical to the previous screenshot. The main area has a title 'Step 1: Create rule' and a sub-instruction 'Create rules to invoke Targets based on Events happening in your AWS environment.' Under 'Event Source', there are two options: 'Event Pattern' (selected) and 'Schedule'. A dropdown menu 'Build custom event pattern' contains the JSON code shown below. Below the dropdown, there are buttons for 'Show sample event(s)' and 'Required'. On the right, under 'Targets', there is a button 'Add target*' and a note: 'Select Target to invoke when an event matches your Event Pattern or when schedule is triggered'. At the bottom right are 'Cancel' and 'Configure details' buttons.

```
{ "source": [ "aws.guardduty" ], "detail-type": [ "GuardDuty Finding" ], "detail": { "severity": [ 4, 4.0, 4.1, 4.2, 4.3 ] } }
```

Step 8: Select the **SNS Topic** and the Topic created in the previous steps. Select **Input Transformer** and enter the below JSON.

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

And for the **Input Template**, enter the below text and click on **Configure details**.

"You have a severity <severity> GuardDuty finding type <Finding_Type> in the <region> region."

"**Finding Description:**"

"<Finding_description>."

"For more details open the GuardDuty console at

https://console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"

The screenshot shows the AWS CloudWatch Events console. On the left, there's a sidebar with various monitoring services. The main area is titled 'Step 1: Create rule' and shows an 'Event Source' section where 'Event Pattern' is selected. A dropdown menu 'Build custom event pattern' contains the provided JSON. Below it is a 'Show sample event(s)' button. To the right, there's a 'Targets' section where 'SNS topic' is selected and 'GuardDutyTopic' is specified. Under 'Configure input', 'Input Transformer' is chosen, and a JSON template is displayed. This template includes the original JSON and the additional descriptive text and URL. A note at the bottom of the target panel provides instructions for finding the finding ID.

Security Management in AWS

Step 9: Give the rule a name and enter some description. Click on **Create rule** to create the rule.

The screenshot shows the 'Step 2: Configure rule details' page. On the left, there's a sidebar with navigation links for CloudWatch, Dashboards, Alarms, Logs, Metrics, Events, and Rules. The 'Rules' link is highlighted. The main area has fields for 'Name' (GuardDutyRule), 'Description' (Rule to capture the GuardDuty events and send an email via SNS), and 'State' (Enabled). A note below says 'CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.' At the bottom right are 'Cancel', 'Back', and 'Create rule' buttons.

The screenshot shows the 'Rules' list page. The sidebar remains the same. The main area displays a success message: 'Success Rule GuardDutyRule was created.' Below it is an info message about Amazon EventBridge. The 'Create rule' button is visible at the top left of the list table. The table lists one rule: 'GuardDutyRule' (Status: Enabled, Description: Rule to capture the GuardDuty events and send an email via SNS). At the bottom right, it says 'Viewing 1 to 1 of 1 Rules'.

Security Management in AWS

Step 10: Navigate to the GuardDuty Management Console and click on **Get started**.

The screenshot shows the Amazon GuardDuty Management Console. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, user 'praveen sripati', region 'N. Virginia', and 'Support'. The main header features a shield icon and the text 'Amazon GuardDuty' with a subtitle 'Intelligent threat detection to protect your AWS accounts and workloads'. Below this are three cards: 'Continuous' (monitoring AWS environment), 'Comprehensive' (analyzing multiple data sources like CloudTrail and VPC Flow Logs), and 'Customizable' (adding threat lists). A large button labeled 'Get started' is prominent, along with a 'Getting started guide' link. At the bottom, there's a section for documentation and support, followed by footer links for 'Feedback', 'English (US)', 'Privacy Policy', and 'Terms of Use'.

Step 11: Click on **Enable GuardDuty**.

The screenshot shows the 'Welcome to GuardDuty' page. On the left, a sidebar has 'GuardDuty' selected and 'Enable GuardDuty' highlighted. The main content area has a 'Service permissions' section with a note about granting GuardDuty permission to analyze AWS CloudTrail logs, VPC Flow Logs, and DNS query logs. It includes a 'View service role permissions' button and a note about GuardDuty's free trial. A large 'Enable GuardDuty' button is at the bottom right. The footer includes 'Feedback', 'English (US)', 'Privacy Policy', and 'Terms of Use'.

Security Management in AWS

Step 12: GuardDuty is free for 30 days once we enable it. Go to the **Usage** tab to figure out how many days are left for free.

The screenshot shows the AWS GuardDuty Usage page. On the left, there's a sidebar with options like Findings, Usage (which is selected), Settings, Lists, S3 Protection, Accounts, What's New, and Partners. The main content area has a title 'Usage' and a sub-section 'Estimated total daily cost \$0.00'. It includes a link 'About GuardDuty pricing' and a note: 'Some features are still in free trial. You pay nothing for these features while free trials are in effect. These estimates reflect what you can expect to pay after your free trial ends.' Below this is a table titled 'Breakdown by data source' with four rows: CloudTrail, VPC Flow Logs, DNS Logs, and S3 Data Events. Each row shows a pending status and a note: 'Daily cost will be available 7 days after enabling data source.' and 'Free trial ends November 27 (30 days remaining)'. At the bottom of the page, there are links for Feedback, English (US), and a footer with copyright information and links to Privacy Policy and Terms of Use.

Step 13: Under the **Settings** tab, change the **Frequency for updated findings** to 15 minutes and click on **Save**.

The screenshot shows the AWS GuardDuty Settings page. The sidebar is identical to the previous page. The main content area has a success message 'Successfully updated CloudWatch Events frequency' in a green box. Below it is a 'Settings' section with tabs for 'About GuardDuty' (Detector ID: e8bab6aa96c8d299dd4a0539252e4dd) and 'Permissions' (View service role permissions). The 'Findings export options' section contains a note about CloudWatch Events and S3 buckets, a dropdown for 'Frequency for updated findings' set to 'Update CWE and S3 every 15 minutes', and a 'Save' button. The 'S3 bucket' section shows a note: 'You have not configured findings export to S3' and a 'Configure now' button. At the bottom, there's a 'Sample findings' section and a footer with copyright information and links to Privacy Policy and Terms of Use.

Step 14: For some reason, if we want to disable GuardDuty, you can use the option **Disable GuardDuty** in the same Settings tab. For now, keep it enabled, so there is no need to make any changes.

Findings are automatically sent to CloudWatch Events. You can also export findings to an S3 bucket. New findings are exported within 5 minutes. You can modify the frequency for updated findings below. [Learn more](#)

Frequency for updated findings
Update CWE and S3 every 15 minutes

S3 bucket [Configure now](#)

You have not configured findings export to S3

Sample findings
Generate sample findings

Suspend GuardDuty

When you disable GuardDuty, you not only stop GuardDuty from monitoring your AWS environment and generating new findings, you also lose your existing findings and your GuardDuty configuration. You can't recover that data later. To save a copy of existing findings, export them before you disable GuardDuty. [Learn more](#)

Step 15: In the EC2 Management Console, create a Security Group with all the traffic allowed inbound, as shown below.

Note: We do not recommend this approach. This is only for demonstration.

Name	Group ID	Group Name	VPC ID	Owner	Description
sg-0088e1af32b6b3b5d	vpc-3bc6e341	AllowRedis	vpc-3bc6e341	304000509264	AllowRedis
sg-016a65f059031ff1	vpc-3bc6e341	AllowNFS	vpc-3bc6e341	304000509264	AllowNFS
sg-0194f43816d90161b	vpc-3bc6e341	AllowAll	vpc-3bc6e341	304000509264	AllowAll
sg-0273390aba287bc7e	vpc-3bc6e341	AllowMQ	vpc-3bc6e341	304000509264	AllowMQ
sg-028ce84f5107866	vpc-3bc6e341	AllowSSHnEFS	vpc-3bc6e341	304000509264	AllowSSHnEFS
sg-03836433adc5a2499	vpc-3bc6e341	AllowMySQL	vpc-3bc6e341	304000509264	AllowMySQL
sg-040f6c6f9932bb5	vpc-3bc6e341	AllowHTTP	vpc-3bc6e341	304000509264	AllowHTTP

Security Group: sg-0194f43816d90161b

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Step 16: Launch an EC2 instance and select **Kali Linux** under the AWS Marketplace. Kali Linux is mainly used for penetration testing and any action we take against AWS resources will be captured by GuardDuty as an anomaly.

The screenshot shows the AWS Marketplace search results for the term "kali". The left sidebar contains navigation links for Quick Start, My AMIs, AWS Marketplace (with a "Free tier eligible" badge), Categories (All Categories, Infrastructure Software, DevOps), Architecture (64-bit (x86)), Operating System (All Linux/Unix, Ubuntu, Other), and Software Pricing Plans (Bring Your Own License, Free, Hourly). The search bar at the top has "kali" typed into it. The main results section displays three items:

- Kali Linux**: A Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It has a 4-star rating from 27 reviews. The listing includes details like "Starting from \$0.13 to \$0.13hr for software + AWS usage fees" and "Linux/Unix, Other 2020.3 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 10/7/20". A "Select" button is available.
- Desktop Linux by Techlatest.net**: An Ubuntu-based Linux GUI environment loaded with open source productivity tools and applications. It has a 4-star rating from 1 review. The listing includes details like "Starting from \$0.13 to \$0.13hr for software + AWS usage fees" and "Linux/Unix, Ubuntu 18.04 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 2/7/20". A "Select" button is available.
- Evolve Security Automation**: The world's first Security Automation Cloud. It has a 4-star rating from 0 reviews. The listing includes details like "Linux/Unix, Ubuntu 2019.11.13 | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 4/8/20". A "Select" button is available.

Below the results, a note states: "The following results for "kali" were found in other catalogs: • 5 results in Community AMIs".

Step 17: Click on **Continue**.

The screenshot shows the product details page for the Kali Linux AMI. The left sidebar is identical to the previous screenshot. The main content area is titled "Kali Linux" and contains the following information:

- Product Details**:
 - By: Kali Linux
 - Customer Rating: ★★★★☆ (27)
 - Latest Version: Kali Linux 2020.3
 - Base Operating System: Linux/Unix, Other 2020.3
 - Delivery Method: 64-bit (x86) Amazon Machine Image (AMI)
 - License Agreement: End User License Agreement
 - On Marketplace Since: 10/19/16
 - AWS Services Required: Amazon EBS, Amazon EC2
- Highlights**:
 - Advanced penetration testing platform
 - Hundreds of security tools included
- Pricing Details**:

Instance Type	Software	EC2	Total
t2.nano	\$0.00	\$0.006	\$0.006/hr
t2.micro	\$0.00	\$0.012	\$0.012/hr
t2.small	\$0.00	\$0.023	\$0.023/hr
t2.medium	\$0.00	\$0.046	\$0.046/hr
t2.large	\$0.00	\$0.093	\$0.093/hr
t2.xlarge	\$0.00	\$0.186	\$0.186/hr
t2.2xlarge	\$0.00	\$0.371	\$0.371/hr
m4.large	\$0.00	\$0.10	\$0.10/hr
m4.xlarge	\$0.00	\$0.20	\$0.20/hr
m4.2xlarge	\$0.00	\$0.40	\$0.40/hr
m4.4xlarge	\$0.00	\$0.80	\$0.80/hr
m4.10xlarge	\$0.00	\$2.00	\$2.00/hr
m4.16xlarge	\$0.00	\$3.20	\$3.20/hr
m3.medium	\$0.00	\$0.067	\$0.067/hr
m3.large	\$0.00	\$0.133	\$0.133/hr
m3.xlarge	\$0.00	\$0.266	\$0.266/hr
m3.2xlarge	\$0.00	\$0.532	\$0.532/hr

At the bottom right of the modal window, there are "Cancel" and "Continue" buttons.

Step 18: Make sure to select **t2.micro** as it falls under the AWS free trial. Click on **Next**.

The screenshot shows the AWS EC2 instance selection interface. At the top, there are tabs for 'Choose AMI', 'Choose Instance Type' (which is selected), 'Configure Instance', 'Add Storage', 'Add Tags', 'Configure Security Group', and 'Review'. Below the tabs, a note says 'Step 2: Choose an Instance Type' and describes the selection process. A table lists various instance types with their details like Family, Type, vCPUs, Memory, Instance Storage, EBS-Optimized Availability, Network Performance, and IPv6 Support. The **t2.micro** instance is selected, indicated by a blue border and a green 'Free tier eligible' badge. Other instances listed include t2.nano, t2.small, t2.medium, t2.large, t2.xlarge, t3.nano, t3.micro, t3.small, t3.medium, t3.large, and t3.xlarge. At the bottom right, there are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Configure Instance Details'.

Step 19: Go with the default options under the **Configure Instance Details** and click on **Next**.

The screenshot shows the 'Configure Instance Details' step of the AWS EC2 wizard. At the top, there are tabs for 'Choose AMI', 'Choose Instance Type', 'Configure Instance' (selected), 'Add Storage', 'Add Tags', 'Configure Security Group', and 'Review'. Below the tabs, a note says 'Step 3: Configure Instance Details' and describes the configuration options. The configuration section includes fields for 'Number of instances' (set to 1), 'Purchasing option' (checkbox for Request Spot Instances), 'Network' (set to 'vpc-3bc6e341 | Default (default)'), 'Subnet' (set to 'No preference (default subnet in any Availability Zone)'), 'Auto-assign Public IP' (checkbox for 'Use subnet setting (Enable)'), 'Placement group' (checkbox for 'Add instance to placement group'), 'Capacity Reservation' (dropdown set to 'Open'), 'Domain join directory' (dropdown set to 'No directory'), 'IAM role' (dropdown set to 'None'), 'CPU options' (checkbox for 'Specify CPU options'), 'Shutdown behavior' (dropdown set to 'Stop'), 'Stop - Hibernate behavior' (checkbox for 'Enable hibernation as an additional stop behavior'), 'Enable termination protection' (checkbox for 'Protect against accidental termination'), 'Monitoring' (checkbox for 'Enable CloudWatch detailed monitoring Additional charges apply.'), 'Tenancy' (dropdown set to 'Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.'), 'Elastic Inference' (checkbox for 'Add an Elastic Inference accelerator Additional charges apply.'), and 'Credit specification' (checkbox for 'Unlimited'). At the bottom right, there are buttons for 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Add Storage'.

Security Management in AWS

Step 20: On this EC2 instance, we will install a bunch of software applications to change the storage from the default 8GB to 15GB. Click on **Next**.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-02f3ebe89274a4bd	15	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Step 21: Tags are optional. Click on **Next**.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes
Name	Webserver			<input type="checkbox"/>	<input type="checkbox"/>

This resource currently has no tags

Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Security Management in AWS

Step 22: Under the **Select an existing security group**, select the Security Group created in the previous step. Click on **Next**.

The screenshot shows the 'Configure Security Group' step of the EC2 instance creation wizard. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group (which is selected), and 7. Review.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group:

- Create a new security group
- Select an existing security group

Existing Security Groups:

Security Group ID	Name	Description	Actions
<input checked="" type="checkbox"/> sg-0194f43816d90161b	AllowAll	AllowAll	Copy to new
<input type="checkbox"/> sg-040fc6ef9932dbb5	AllowHTTP	AllowHTTP	Copy to new
<input type="checkbox"/> sg-027643ad9ca700a3	AllowICMP	AllowICMP	Copy to new
<input type="checkbox"/> sg-0273390aa287bc7e	AllowMQ	AllowMQ	Copy to new
<input type="checkbox"/> sg-0383643adc5a2499	AllowMySQL	AllowMySQL	Copy to new
<input type="checkbox"/> sg-016af65185b8f31f1	AllowNFS	AllowNFS	Copy to new
<input type="checkbox"/> sg-07bb6fd3d39329a93	AllowRDP	AllowRDP	Copy to new
<input type="checkbox"/> sg-07f84e4d18ea283d	AllowRDnSSH	AllowRDnSSH	Copy to new
<input type="checkbox"/> sg-00808e1af2b6b85d	AllowRedis	AllowRedis	Copy to new
<input type="checkbox"/> sg-07a7df1da4d7e0cb	AllowSSH	AllowSSH	Copy to new
<input type="checkbox"/> sg-028c8e84f5107860c	AllowSSHnEFS	AllowSSHnEFS	Copy to new
<input type="checkbox"/> sg-0a787ae2ed4454fe	AllowSSHnHTTP	AllowSSHnHTTP	Copy to new

Inbound rules for sg-0194f43816d90161b (Selected security groups: sg-0194f43816d90161b)

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Buttons: Cancel, Previous, **Review and Launch**

Step 23: Review all the details and click on **Launch**.

The screenshot shows the 'Review Instance Launch' step of the EC2 instance creation wizard. At the top, there are tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review (which is selected).

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details:

Kali Linux
kali-linux-2020.3-cloud-ec2-amd64-disk.raw
Free tier eligible
Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t2.micro instance. Additional taxes or fees may apply.
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the sellers' End User License Agreement.

Instance Type:

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups:

Security Group ID	Name	Description
sg-0194f43816d90161b	AllowAll	AllowAll

All selected security groups inbound rules:

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Buttons: Cancel, Previous, **Launch**

Security Management in AWS

Step 24: Make sure to select the KeyPair, select I acknowledge and click on Launch Instances.

The screenshot shows the AWS Step 7: Review Instance Launch page. A modal window titled "Select an existing key pair or create a new key pair" is open. It contains instructions about key pairs and a dropdown menu where "my-keypair" is selected. Below the dropdown is a checkbox labeled "I acknowledge that I have access to the selected private key file (my-keypair.pem), and that without this file, I won't be able to log into my instance." At the bottom of the modal are "Cancel" and "Launch Instances" buttons. The background of the main page shows the AMI Details section with "Kali Linux" selected, the Instance Type section with "t2.micro" chosen, and the Security Groups section with "AllowAll" selected. The top navigation bar includes tabs for "1. Choose AMI", "2. Choose Instance Type", "3. Configure Instance", "4. Add Storage", "5. Add Tags", "6. Configure Security Group", and "7. Review". The status bar at the bottom indicates "praveen srivati N. Virginia Support".

Step 25: The EC2 instances would in a running state in a few minutes.

The screenshot shows the AWS Instances page. On the left, there's a sidebar with various service links like New EC2 Experience, Limits, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main area displays a table of instances. One instance is highlighted: "i-0eeb1672798aab48" with a Public DNS of "ec2-100-26-178-109.compute-1.amazonaws.com". The instance status is listed as "running". The table includes columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, Key Name, Monitoring, and Launch time. The "Key Name" column shows "my-keypair". The "Launch time" column shows "October 28, 2020 at 11:46:47 AM UTC+5:30 (less than one hour)". The bottom of the page includes a feedback link and a status bar with "praveen srivati N. Virginia Support".

Step 26: Go to the IAM Management Console and then to the **Roles** tab. Click on **Create role**.

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation links like Dashboard, Access management, Policies, and Roles. The Roles link is highlighted. The main area has a search bar and a table with columns: Role name, Trusted entities, and Last activity. The table lists various AWS service roles, such as aws-ec2-spot-fleet-tagging-role, aws-elasticbeanstalk-ec2-role, and aws-quicksight-service-role-v0. Each row shows the service that the role trusts and the last time it was used.

Step 27: Select EC2 under **Common use cases** and click on **Next**.

The screenshot shows the 'Create role' wizard, Step 1: Select type of trusted entity. It has four tabs: AWS service (selected), Another AWS account, Web identity, and SAML 2.0 federation. Below the tabs, there's a note about allowing AWS services to perform actions on behalf of the role. Under 'Choose a use case', the 'Common use cases' section is expanded, showing 'EC2' selected. A tooltip for 'EC2' says 'Allows EC2 instances to call AWS services on your behalf.' Other options like Lambda are also listed. At the bottom, there's a table of services and their associated use cases, and a note that some fields are required.

Step 28: Select **AdministratorAccess** Policy and click on **Next**.

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies Showing 728 results

	Policy name	Used as
<input type="checkbox"/>	AccessAnalyzerServiceRolePolicy	None
<input checked="" type="checkbox"/>	AdministratorAccess	None
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	None
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	None
<input type="checkbox"/>	AlexaForBusinessNetworkProfileServicePolicy	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	None

Set permissions boundary

* Required

Cancel Previous **Next: Tags**

Feedback English (US) ▾ © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 29: Tags are optional. Click on **Next**.

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Cancel Previous **Next: Review**

Feedback English (US) ▾ © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 30: Give the Role a name and click on **Create role**.

Create role

Review

Provide the required information below and review this role before you create it.

Role name* Role4EC2-FA
Use alphanumeric and '+', '.', '@', '-' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+', '.', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AdministratorAccess

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

Cancel Previous Create role

Feedback English (US) ▾ © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 31: Attach the IAM Role to the earlier created EC2 instance.

New EC2 Experience

Instances

Images

Elastic Block Store

Network & Security

Load Balancing

Auto Scaling

Feedback English (US) ▾

Launch Instance Connect Actions

Connect Get Windows Password

Create Template From Instance

Launch More Like This

Instance State

Instance Settings

Add/Edit Tags

Attach to Auto Scaling Group

Attach/Replace IAM Role

Change Instance Type

Change Termination Protection

View/Change User Data

Change Shutdown Behavior

Change T2/T3 Unlimited

Get System Log

Get Instance Screenshot

Modify Instance Placement

Modify Capacity Reservation Settings

Description Status Checks

Instance ID i-0eeb16727982aab48

Instance state running

Instance type t2.micro

Finding Opt-in to AWS Compute Optimizer for this instance

Private DNS ip-172-31-50-241.ec2.internal

Private IPs 172.31.50.241

VPC ID vpc-3bc5e341 (Default)

Platform Other Linux

Platform details Linux/UNIX

Usage operation RunInstances

Source/dest. check True

T2/T3 Unlimited Disabled

EBS-optimized False

Root device type ebs

Root device /dev/sda1

Block devices /dev/sda1

Elastic Graphics ID -

Elastic Inference accelerator ID -

Capacity Reservation -

Capacity Reservation Settings Open

Outpost Arm -

Public DNS (IPv4) ec2-100-26-178-109.compute-1.amazonaws.com

IPv4 Public IP 100.26.178.109

IPv6 IPs -

Elastic IPs

Availability zone us-east-1e

Security groups AllowAll, view inbound rules, view outbound rules

Scheduled events No scheduled events

AMI ID ami-01f9e4b8b12276174b

Subnet ID subnet-70560a4e

Network interfaces eth0

IAM role -

Key pair name my-keypair

Owner 304000509264

Launch time October 28, 2020 at 11:46:47 AM UTC+5:30 (less than one hour)

Termination protection False

Lifecycle normal

Monitoring basic

Alarm status None

Kernel ID -

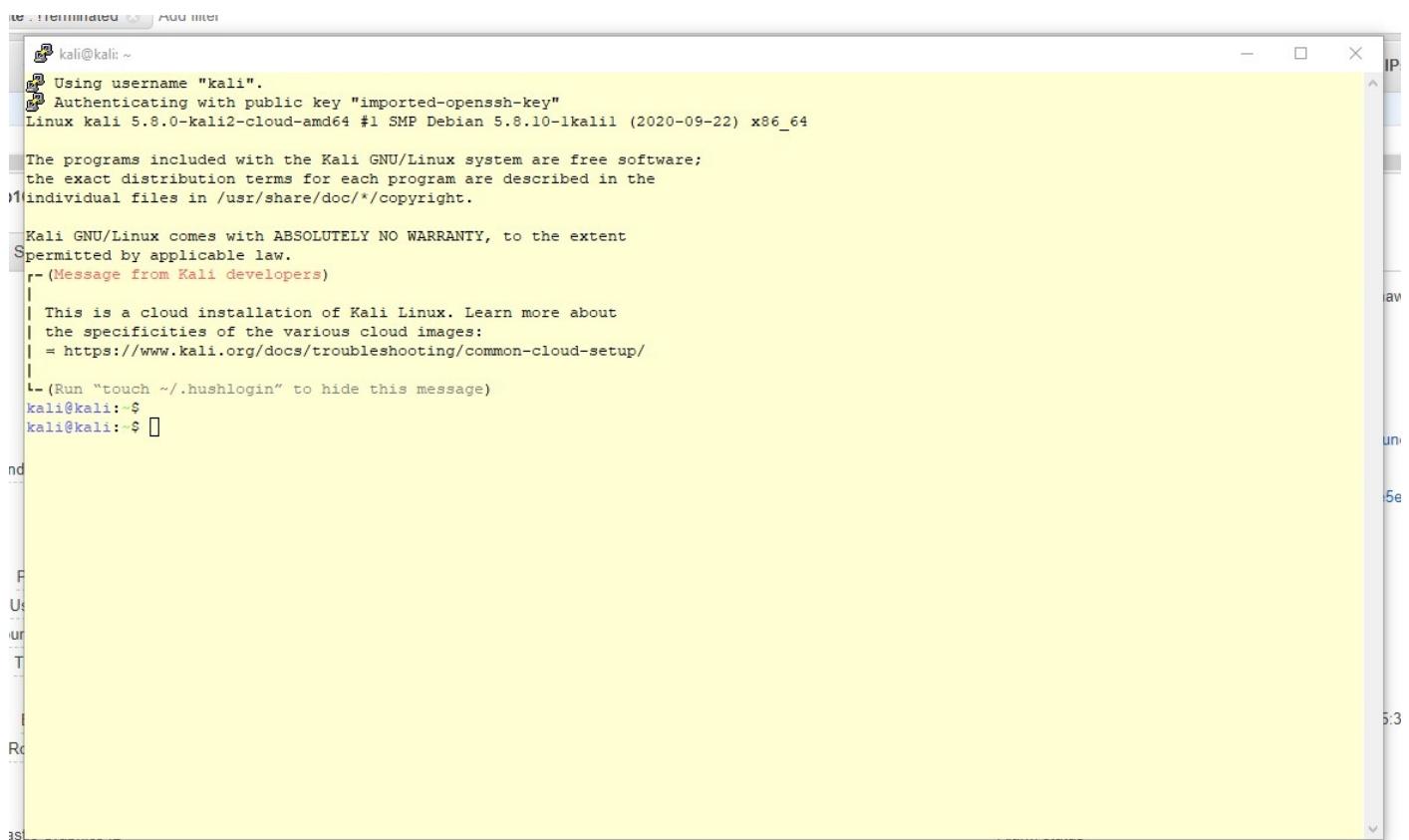
RAM disk ID -

Placement group -

Partition number -

Feedback English (US) ▾ © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Step 32: Connect to the EC2 instance via PuTTY or some other SSH client. Note that the user name to connect to the EC2 instance is **kali**.



The screenshot shows a terminal window titled "Terminal" with the following text output:

```
kali@kali: ~
Using username "kali".
Authenticating with public key "imported-openssh-key"
Linux kali 5.8.0-kali2-cloud-amd64 #1 SMP Debian 5.8.10-1kali1 (2020-09-22) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
-- (Message from Kali developers)

This is a cloud installation of Kali Linux. Learn more about
the specificities of the various cloud images:
= https://www.kali.org/docs/troubleshooting/common-cloud-setup/
--(Run "touch ~/.hushlogin" to hide this message)
kali@kali: ~
kali@kali: ~
```

Step 33: The below actions have to be performed on the Kali Linux:

a) Execute the below commands.

```
sudo apt update
sudo apt install -y xfce4 xfce4-goodies tightvncserver midori python3 python3-pip
pip install awscli --upgrade
export PATH="$PATH:/home/ubuntu/.local/bin/"
```

b) Execute the **aws configure** command and enter **us-east-1** for the default Region and leave the rest of the fields without anything.

c) Execute the **vncpasswd** command and enter the **kali123** password thrice, as shown below at the end.

The above code will alert for any Medium to High finding

```
kali@kali: ~
Setting up gstreamer1.0-x:amd64 (1.18.0-2) ...
Setting up gnome-keyring (3.36.0-1) ...
Setting up xfce4-goodies (4.14.0) ...
Setting up gstreamer1.0-plugins-good:amd64 (1.18.0-1) ...
Setting up gstreamer1.0-pulseaudio:amd64 (1.18.0-1) ...
Processing triggers for initramfs-tools (0.137) ...
update-initramfs: Generating /boot/initrd.img-5.8.0-kali2-cloud-amd64
Processing triggers for dictionaries-common (1.28.3) ...
aspell-autobuildhash: processing: en [en-common].
aspell-autobuildhash: processing: en [en-variant_0].
aspell-autobuildhash: processing: en [en-variant_1].
aspell-autobuildhash: processing: en [en-variant_2].
aspell-autobuildhash: processing: en [en-w_accents-only].
aspell-autobuildhash: processing: en [en-wo_accents-only].
aspell-autobuildhash: processing: en [en_AU-variant_0].
aspell-autobuildhash: processing: en [en_AU-variant_1].
aspell-autobuildhash: processing: en [en_AU-w_accents-only].
aspell-autobuildhash: processing: en [en_AU-wo_accents-only].
aspell-autobuildhash: processing: en [en_CA-variant_0].
aspell-autobuildhash: processing: en [en_CA-variant_1].
aspell-autobuildhash: processing: en [en_CA-w_accents-only].
aspell-autobuildhash: processing: en [en_CA-wo_accents-only].
aspell-autobuildhash: processing: en [en_GB-ise-w_accents-only].
aspell-autobuildhash: processing: en [en_GB-ise-wo_accents-only].
aspell-autobuildhash: processing: en [en_GB-ize-w_accents-only].
aspell-autobuildhash: processing: en [en_GB-ize-wo_accents-only].
aspell-autobuildhash: processing: en [en_GB-variant_0].
aspell-autobuildhash: processing: en [en_GB-variant_1].
aspell-autobuildhash: processing: en [en_US-w_accents-only].
aspell-autobuildhash: processing: en [en_US-wo_accents-only].
Processing triggers for libc-bin (2.31-3) ...
kali@kali: $ vncpasswd
Using password file /home/kali/.vnc/passwd
VNC directory /home/kali/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
kali@kali: $
kali@kali: $
kali@kali: $
```

d) Create a file in the **~/.vnc/xstartup** path with the below content

```
#!/bin/bash
xrdb $HOME/.Xresources
startxfce4 &
```

e) Change the permissions on the above file and execute the **vncserver** command.

```
chmod +x ~/.vnc/xstartup
vncserver
```

Step 34: Create a file named **threat-list.txt** with the IP address of Google and the Public IP of the EC2. One IP address per line, as shown below. The IP address of the Google can be obtained by executing **ping google.com** command from the Windows Command Prompt.

a.b.c.d

m.n.o.p

Now, create an S3 bucket and upload the file, as shown below.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, user name 'praveen sripati', and dropdown menus for 'Global' and 'Support'. Below the navigation bar, the URL 'Amazon S3 > guard-duty-123' is visible. The main area shows a bucket named 'guard-duty-123'. Below the bucket name, there are tabs: 'Overview' (selected), 'Properties', 'Permissions', 'Management', and 'Access points'. A search bar with the placeholder 'Type a prefix and press Enter to search. Press ESC to clear.' is present. Below the search bar are buttons for 'Upload', '+ Create folder', 'Download', and 'Actions'. On the right side, it shows the location 'US East (N. Virginia)' and a link to 'Viewing 1 to 1'. The list of objects in the bucket includes a single file named 'threat-list.txt'. The details for this file are: Name (checkbox), Last modified (Oct 28, 2020 12:12:49 PM GMT+0530), Size (31.0 B), and Storage class (Standard). At the bottom of the page, there are links for 'Operations', 'Feedback', 'English (US)', and legal notices like '© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Step 35: Go back to the GuardDuty Management Console and click on **Lists** under **Settings**. Click on **Add a threat list**.

Security Management in AWS

The screenshot shows the AWS GuardDuty List management interface. On the left, a sidebar menu includes Findings, Usage, Settings (with Lists selected), S3 Protection, Accounts, What's New, and Partners. The main content area has two sections: "Trusted IP lists" and "Threat lists". Each section contains a brief description, a "Add a [list type]" button, a table header row with columns for List name, List file URL, Format, and Active, and a detailed information box with an info icon and a link to learn more.

Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

+ Add a trusted IP list

List name	List file URL	Format	Active
-----------	---------------	--------	--------

Info Trusted IP lists

Trusted IP lists consist of IP addresses that are trusted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

Threat lists

Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. [Learn more](#)

+ Add a threat list

List name	List file URL	Format	Active
-----------	---------------	--------	--------

Info Threat lists

Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. [Learn more](#)

Feedback English (US) ▾

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Step 36: Give the list a name and enter the proper location of the file in S3 from the previous step. For the format, select **Plaintext**. And, finally, click on **I agree** and **Add list**.

The screenshot shows the AWS GuardDuty service console. In the left sidebar, under the 'Lists' section, the 'Threat lists' tab is selected. A modal window titled 'Add a threat list' is open. Inside the modal, there are fields for 'List name' (set to 'CustomThreatList'), 'Location' (set to 's3://guard-duty-123/threat-list.txt'), and 'Format' (set to 'Plaintext'). Below these fields is a note about using TXT files for simple IP lists. At the bottom of the modal, there is a checkbox labeled 'I agree' followed by 'Cancel' and 'Add list' buttons.

The screenshot shows the same AWS GuardDuty service console. The 'Threat lists' section now displays a single entry: 'CustomThreatList' located at 's3://guard-duty-123/threat-list.txt'. The 'Format' is listed as 'TXT' and the 'Active' status is checked. The rest of the interface remains the same, with the 'GuardDuty' service bar and various navigation links visible.

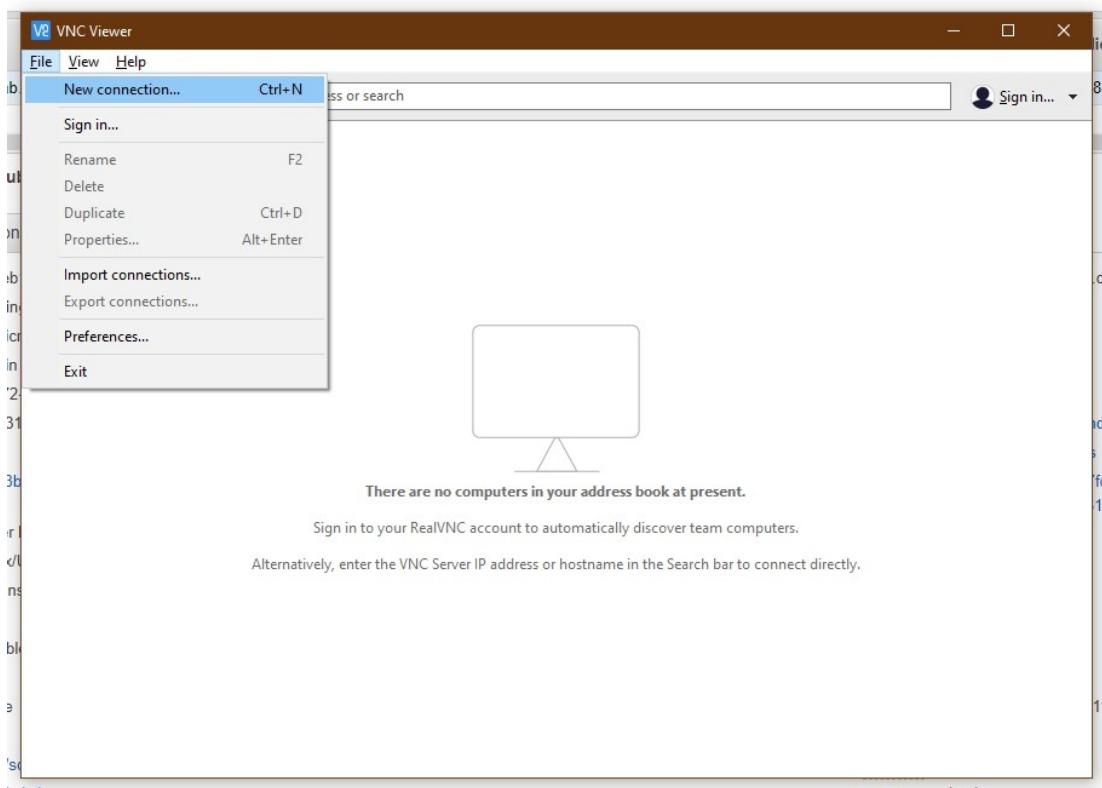
Step 37: From the PuTTY session connected to the Kali Linux, execute the below AWS CLI commands to get the S3 buckets and Security Groups list. This should be identified as an anomaly by the GuardDuty as the commands are run from Kali Linux, mainly used for penetration testing.

```
aws s3 ls  
aws ec2 describe-security-groups
```

Step 38: Download the VNC Viewer from the below URL and install it as with any other software on the Windows OS. We would be using this later to get the GUI access to the Kali Linux EC2 instance.

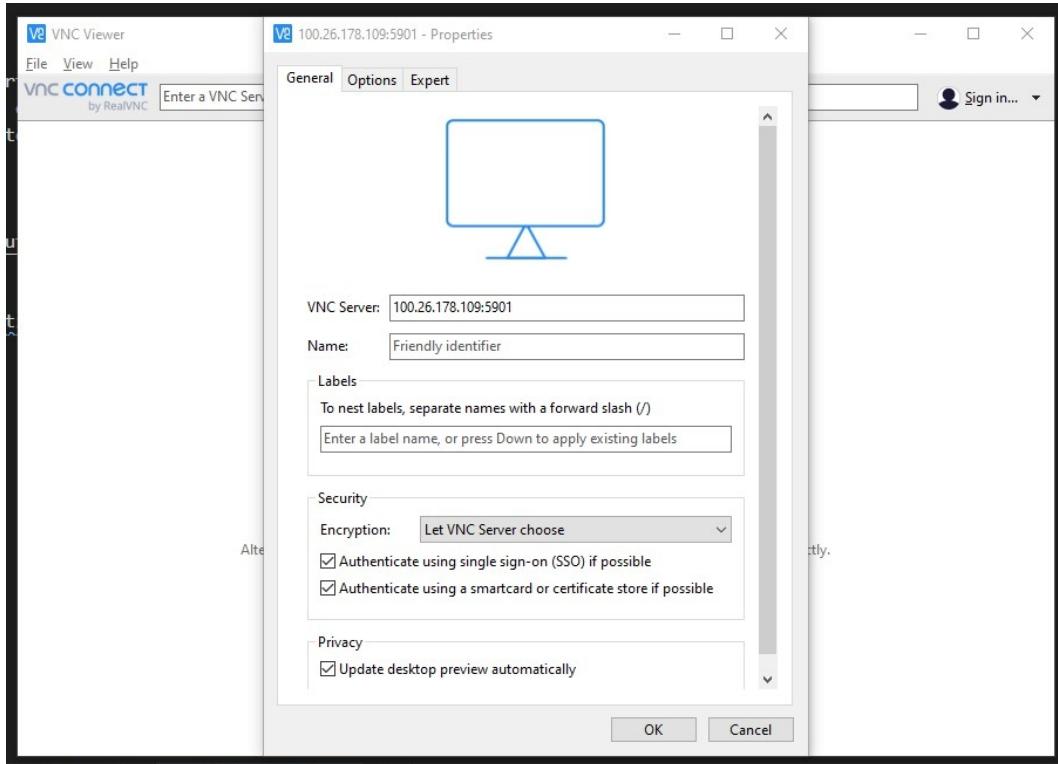
<https://www.realvnc.com/en/connect/download/viewer/>

Step 39: Start the VNC Viewer. Go to File -> New Connection.

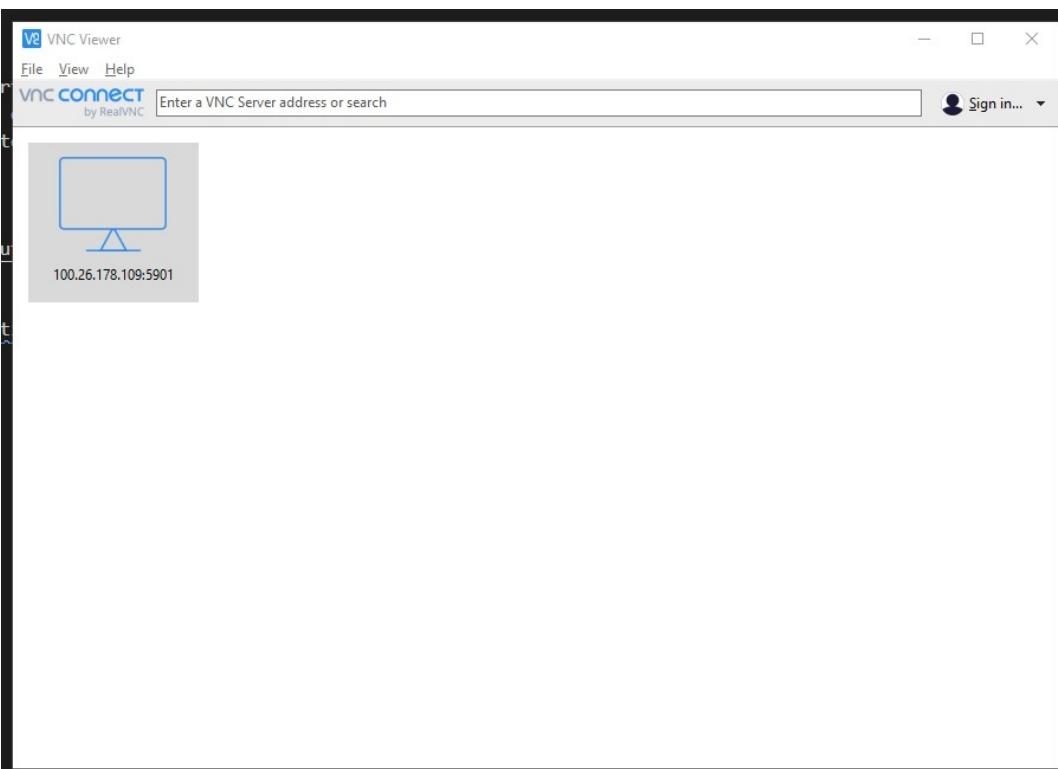


Step 40: Enter the VNC Server details in the below format and click on **OK**.

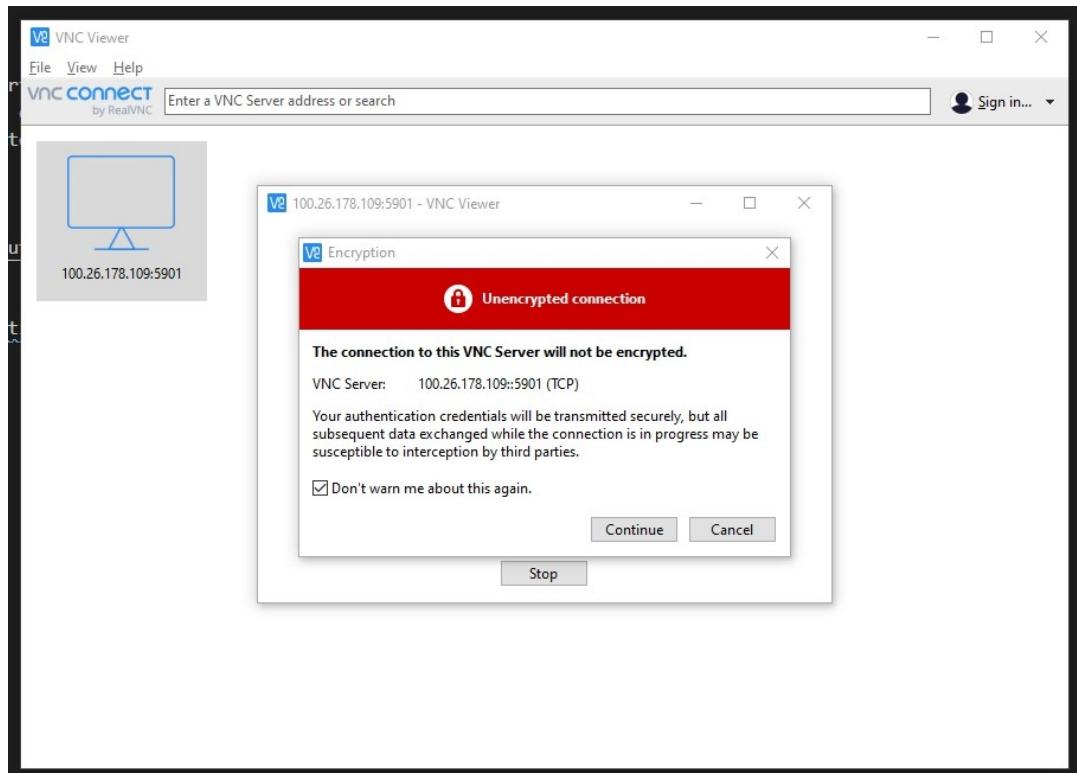
public-ip-of-ec2:5901



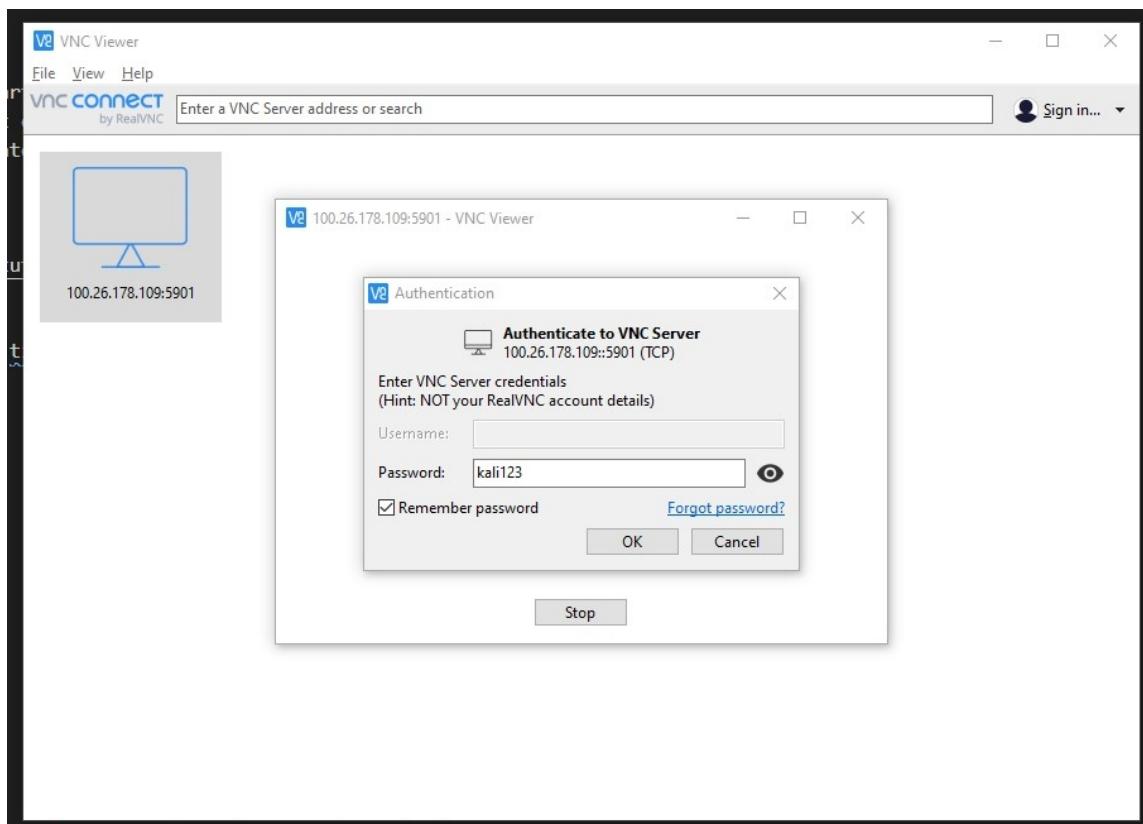
Step 41: An entry should be created, as shown below. Double click on it to connect to the Kali Linux.



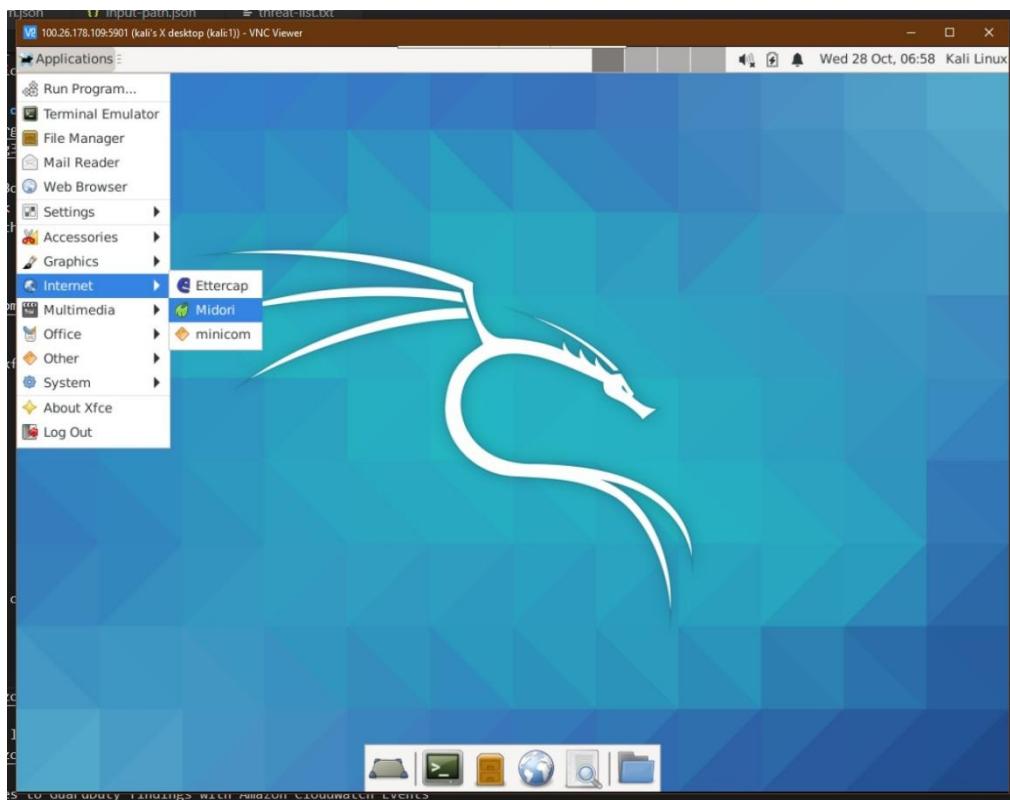
Step 42: When prompted with a warning on Unencrypted connection, select **Don't warn** and click on **Continue**.



Step 43: Enter the password as **kali123**, select **Remember password** and click on **OK**.

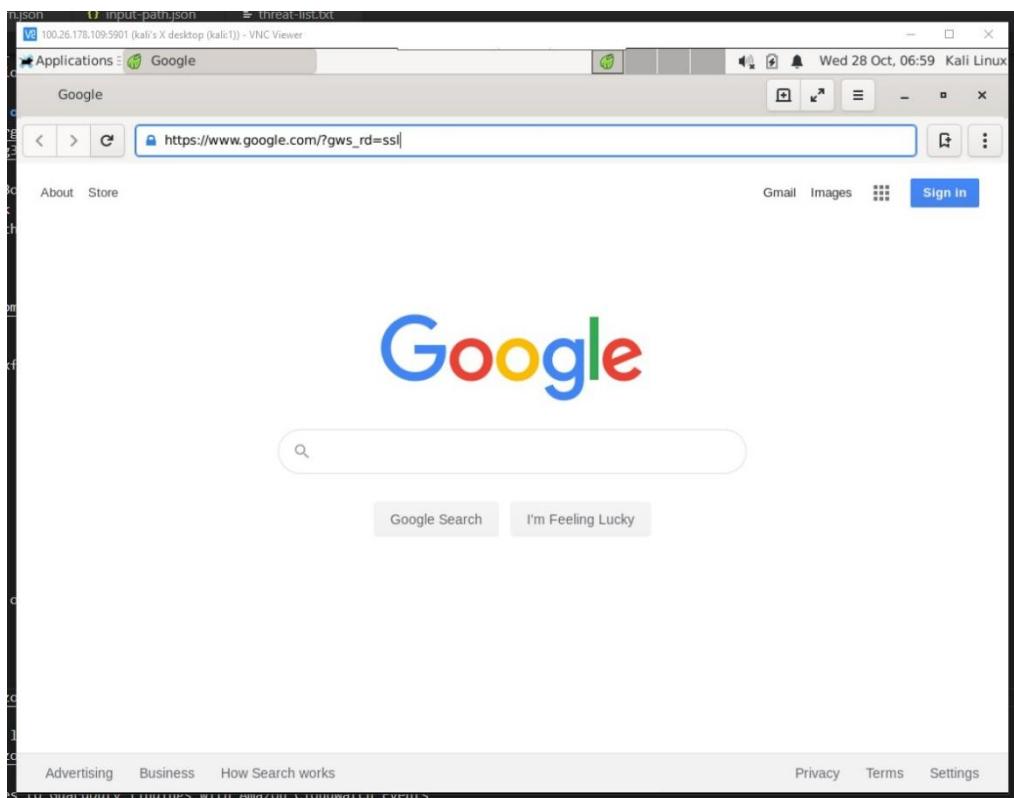


Step 44: The Kali Linux GUI will be displayed, as shown below. Navigate to Applications -> Internet -> Modori as shown below and start the browser.



Step 45: Navigate to google.com using the IP we got from one of the previous steps and the one added to the `threat-list.txt` file in S3. It would redirect to the Google page automatically from the IP address, as shown below. This activity also should be triggered as an anomaly by GuardDuty as we have included the Google IP in the threat list for GuardDuty.

Security Management in AWS



Step 46: From the EC2 Management Console, launch an EC2 instance and select **Microsoft Windows Server 2019 Base**.

The screenshot shows the 'Choose an Amazon Machine Image (AMI)' step of the AWS Launch Wizard. The search bar at the top contains 'windows'. Below it, a message says 'AWS Launch Wizard for SQL Server offers an easy way to size, configure, and deploy Microsoft SQL Server Always On availability groups. Use AWS Launch Wizard for this launch'.

The main list displays several AMI options under the 'Quick Start (19)' section:

- Microsoft Windows Server 2019 Base** - ami-0412e100c0177fb4b (Windows, Free tier eligible) - Select (64-bit (x86))
- Microsoft Windows Server 2019 Base with Containers** - ami-06ba345d99c295fc (Windows, Free tier eligible) - Select (64-bit (x86))
- Microsoft Windows Server 2019 with SQL Server 2017 Standard** - ami-0f8425d0d2f004135 (Windows) - Select (64-bit (x86))
- Microsoft Windows Server 2019 with SQL Server 2017 Enterprise** - ami-0ca834b35a62d5940 (Windows) - Select (64-bit (x86))
- Microsoft Windows Server 2019 with SQL Server 2019 Standard** - ami-0ff25146d6e1f112c (Windows) - Select (64-bit (x86))
- Microsoft Windows Server 2019 with SQL Server 2019 Enterprise** - ami-00e9414bf5fa13d6a (Windows) - Select (64-bit (x86))

At the bottom, there are links for 'Feedback', 'English (US)', '© 2008 - 2020 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Step 47: Select t2.micro and click on **Next**.

Security Management in AWS

Screenshot of the AWS EC2 Instance Creation Wizard - Step 2: Choose an Instance Type.

The screenshot shows a table of available instance types. The selected instance type is t2.micro (Free tier eligible). Other visible instance types include t2.nano, t2.small, t2.medium, t2.large, t2.xlarge, t2.2xlarge, t3.nano, t3.micro, t3.small, t3.medium, t3.large, t3.xlarge, and t3.2xlarge.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Buttons at the bottom: Cancel, Previous, Review and Launch (highlighted), Next: Configure Instance Details.

Step 48: Go with all the default options and click on Next.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: Request Spot Instances

Network: vpc-3b06e341 | Default (default)

Subnet: No preference (default subnet in any Availability Zone)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory

IAM role: None

CPU options: Specify CPU options

Shutdown behavior: Stop

Stop - Hibernate behavior: Enable hibernation as an additional stop behavior

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

Elastic Graphics: Add Graphics Acceleration
Additional charges apply.

Credit specification: Unlimited

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Storage

Step 49: Go with the default storage and click on Next.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0beb9a1dddbef49	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Buttons: Cancel, Previous, **Review and Launch**, Next: Add Tags

Security Management in AWS

Step 50: Tags are optional. Click on Next.

Key (128 characters maximum) Value (256 characters maximum)

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Step 51: Select the Security Group created in one of the previous steps. Then, click on Next.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
sg-0194f43816d90161b	AllowAll	AllowAll	Copy to new
sg-040f6c6ef9932db5	AllowHTTP	AllowHTTP	Copy to new
sg-037643ad9ca700a3	AllowICMP	AllowICMP	Copy to new
sg-0273390a0a287bc7e	AllowMQ	AllowMQ	Copy to new
sg-03836433adc5a2499	AllowMySQL	AllowMySQL	Copy to new
sg-016af5185bd8f31f1	AllowNFS	AllowNFS	Copy to new
sg-07bb6f03d39329a93	AllowRDP	AllowRDP	Copy to new
sg-07f84e04d18ea263d	AllowRDnSSH	AllowRDnSSH	Copy to new
sg-0088e1a32b6b5bd	AllowRedis	AllowRedis	Copy to new
sg-0fa7df1dab4d7ebcb	AllowSSH	AllowSSH	Copy to new
sg-028c8e845107860c	AllowSSHnEFS	AllowSSHnEFS	Copy to new
sg-0a767ae2ed445a4fe	AllowSSHnHTTP	AllowSSHnHTTP	Copy to new

Inbound rules for sg-0194f43816d90161b (Selected security groups: sg-0194f43816d90161b)

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Cancel Previous Review and Launch

Step 52: Review all the details and click on **Launch**.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Microsoft Windows Server 2019 Base - ami-0412e100c0177fb4b	Edit AMI
Free tier eligible	Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

[Edit instance type](#)

Security Groups

Security Group ID	Name	Description
sg-0194f43816d90161b	AllowAll	AllowAll

[Edit security groups](#)

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

[Cancel](#) [Previous](#) [Launch](#)

Step 53: Select the KeyPair, select I acknowledge and click on **Launch Instances**.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Microsoft Windows Server 2019 Base - ami-0412e100c0177fb4b	Edit AMI
Free tier eligible	Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)
t2.micro	-	1	1	EBS only

[Edit instance type](#)

Security Groups

Security Group ID	Name
sg-0194f43816d90161b	AllowAll

[Edit security groups](#)

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair
Select a key pair
my-keypair

I acknowledge that I have access to the selected private key file (my-keypair.pem), and that without this file, I won't be able to log into my instance.

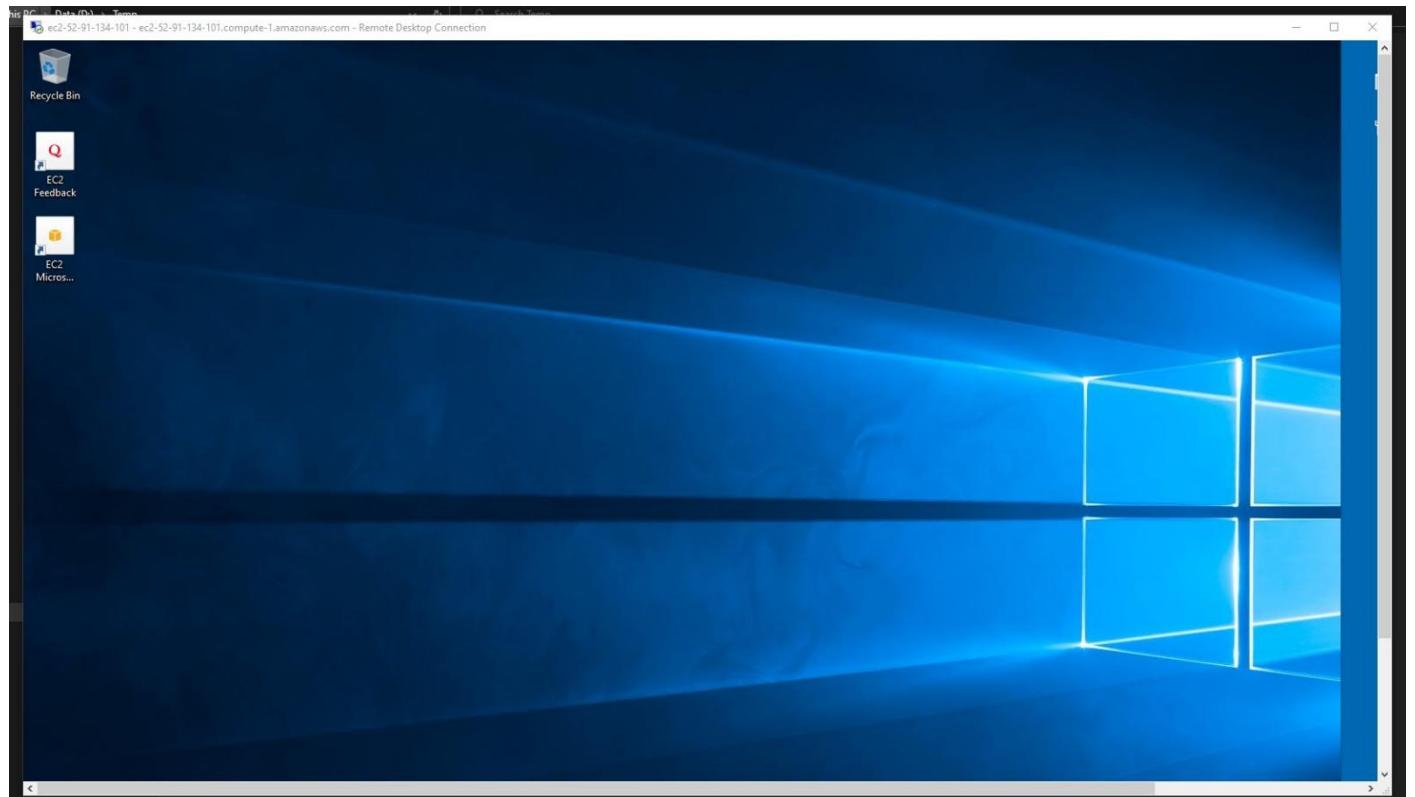
[Cancel](#) [Launch Instances](#)

[Feedback](#) [English \(US\) ▾](#) [© 2008 - 2020 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.](#) [Privacy Policy](#) [Terms of Use](#)

Step 54: In a few minutes, the EC2 would be in a **running** state.

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar lists various AWS services like New EC2 Experience, Limits, Instances, Images, AMIs, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and more. The main content area displays a table of EC2 instances. One instance is highlighted: i-06fc4a866ac44466b, which is an t2.micro instance running in us-east-1e. The instance has a Public DNS of ec2-52-91-134-101.compute-1.amazonaws.com and a Private IP of 172.31.61.94. The instance was launched on October 28, 2020, at 12:40:09 PM UTC+5:30 (less than one hour) by user 304000509264. It is currently terminated.

Step 55: Connect to the EC2 instance using the RDP protocol.



Step 56: Inside the EC2 instance, perform the below steps, which allows the software to be downloaded by IE.

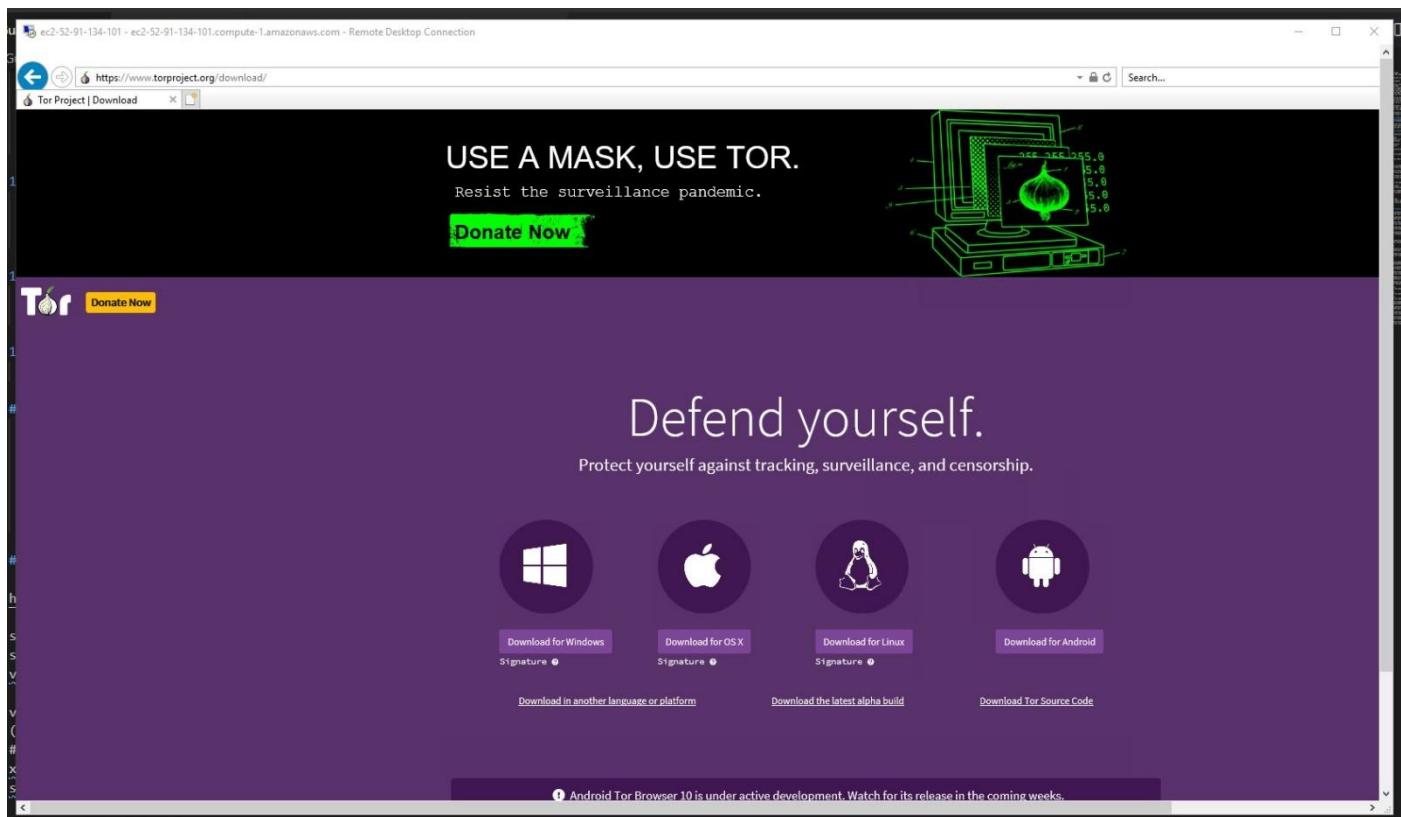
Go to Start > Server Manager > Local Server

Click on the link to the right of IE Enhanced Security Configuration

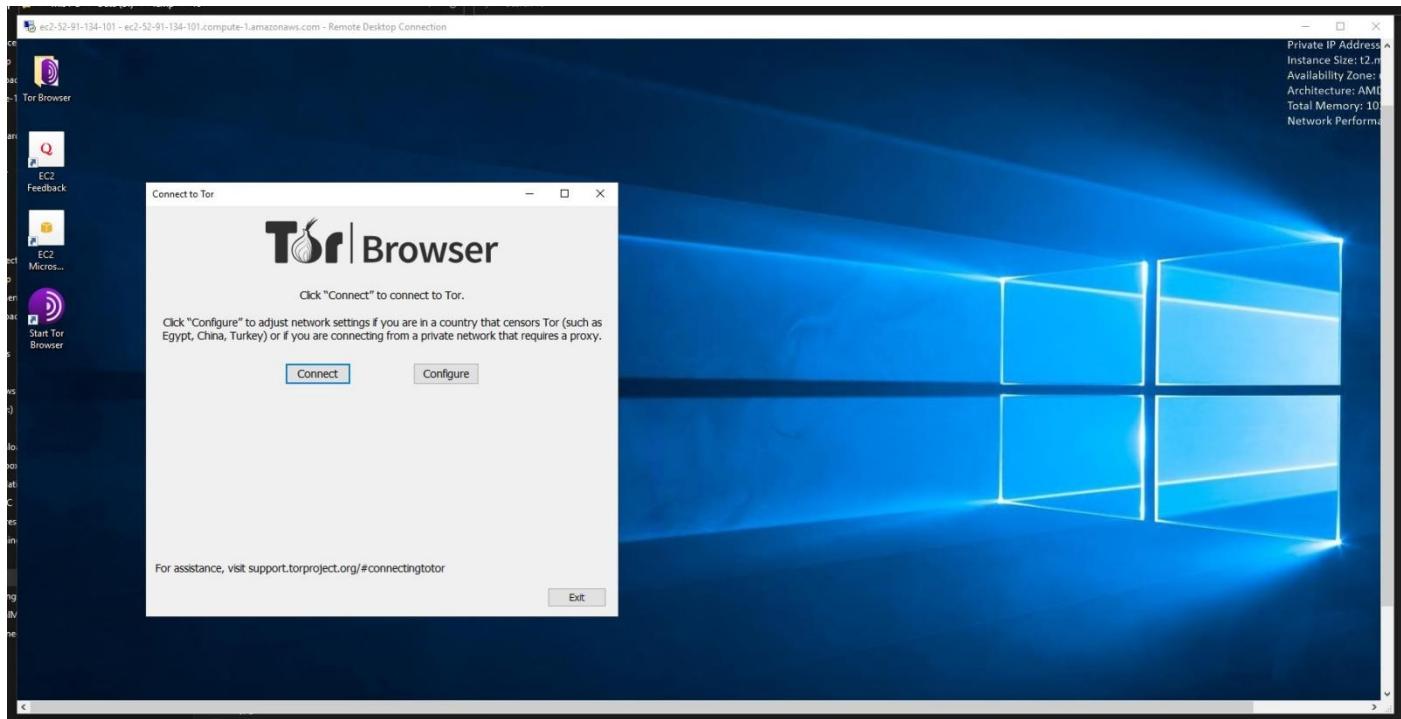
Navigate to the Administrators and Users section and Click on OK

Step 57: Download the Tor browser for Windows from the below URL and install it like any other application.

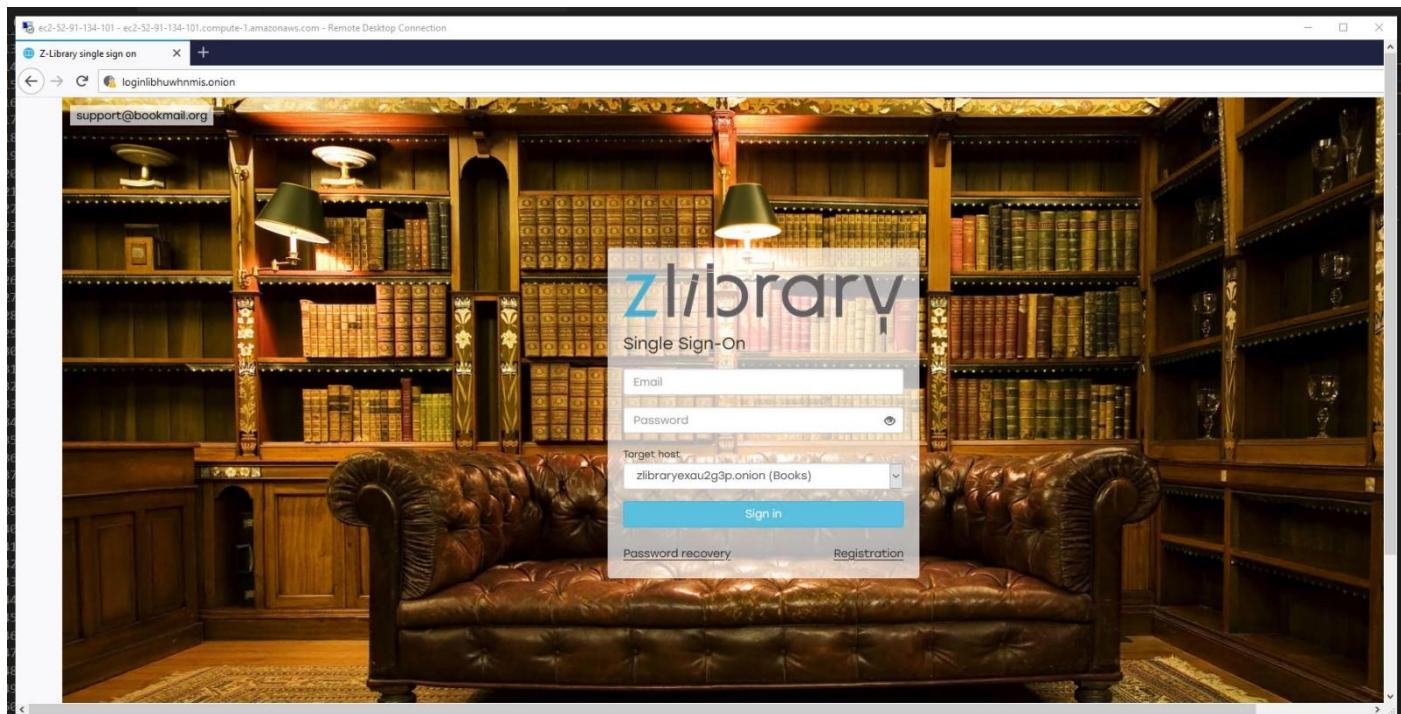
<https://torproject.org/download>



Step 58: Once the Tor browser has been installed, there would be an icon on the Desktop, as shown below. Use it to start the Tor browser. Click on the **Connect** button.



Step 59: In a few seconds, the Tor browser opens in the EC2 instance. Navigate to any onion site. Maybe to <http://zlibraryexau2g3p.onion> in the Tor browser. This should also trigger an anomaly in the GuardDuty as we are visiting a Tor site.



Step 60: Go back to the GuardDuty Management Console and you will find a bunch of findings. GuardDuty displays these findings as anomalies in different activities we performed.

Step 61: We will also get an email as shown below, since we have integrated GuardDuty events with SNS Notifications via the CloudWatch Rules.

Conclusion:

In this use case, we tried to perform a few actions which are typically performed by hackers

- Use Kali Linux to probe AWS resources
- Use Root IAM role to perform AWS activities
- Use a TOR Client on an EC2 instance
- Used a browser to reach a malicious IP address

In the above steps, we observed that the suspicious activities were immediately identified by GuardDuty as anomalies, and an email alert was also sent via SNS Topic.