

# Generate and Configure an AWS IAM User for EWP

## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
<b>2</b>	<b>CREATE AN IAM POLICY FOR EWP.....</b>	<b>5</b>
<b>3</b>	<b>CREATE AN IAM ROLE FOR EWP .....</b>	<b>7</b>
<b>4</b>	<b>CREATE AN IAM ARN FOR EWP.....</b>	<b>10</b>
<b>5</b>	<b>CREATE AN IAM GROUP.....</b>	<b>11</b>
<b>6</b>	<b>CREATE AN IAM USER .....</b>	<b>12</b>
<b>7</b>	<b>CREATE IAM KEYS FOR EWP .....</b>	<b>14</b>
<b>8</b>	<b>CHECKING POLICY USING AWS SIMULATOR.....</b>	<b>16</b>
<b>9</b>	<b>UNDERSTANDING IAM POLICY FOR EWP.....</b>	<b>18</b>
9.1	AWS AUTO-DISCOVERY .....	18
9.2	AWS CONTINUOUS ANALYTICS .....	18
<b>10</b>	<b>AWS CLONE AND SCAN.....</b>	<b>20</b>
<b>11</b>	<b>REFERENCES .....</b>	<b>21</b>
11.1	ANNEX -I .....	21
11.2	ANNEX -II .....	28

## About This Document

This document describes how to create an IAM user, an IAM group, an IAM role and an IAM policy that contains all required actions according to current AWS best practices for IAM usage.

For support information, visit <https://www.outpost24.com/support>

### Copyright

© 2018 Outpost24®. All rights reserved.

This document may only be redistributed unedited and unaltered. This document may be cited and referenced only if clearly crediting Outpost24® and this document as the source. Any other reproduction and redistribution in print or electronically is strictly prohibited without explicit permission.

### Trademark

Outpost24®, OUTSCAN™, and HIAB™ are trademarks of Outpost24® in Sweden and other countries.

# 1 Introduction

Elastic Workload Protector (EWP) requires an Amazon Web Service (AWS) Identity and an Access Management (IAM) user to connect to your AWS infrastructure, automatically discover your assets, perform vulnerability assessment using the *Clone & Scan Technology* and continuous monitoring through its *Workload Analytics*. This can be configured via AWS IAM.

We recommend creating an AWS IAM Role with an ARN, that can be configured in EWP following the steps bellow:

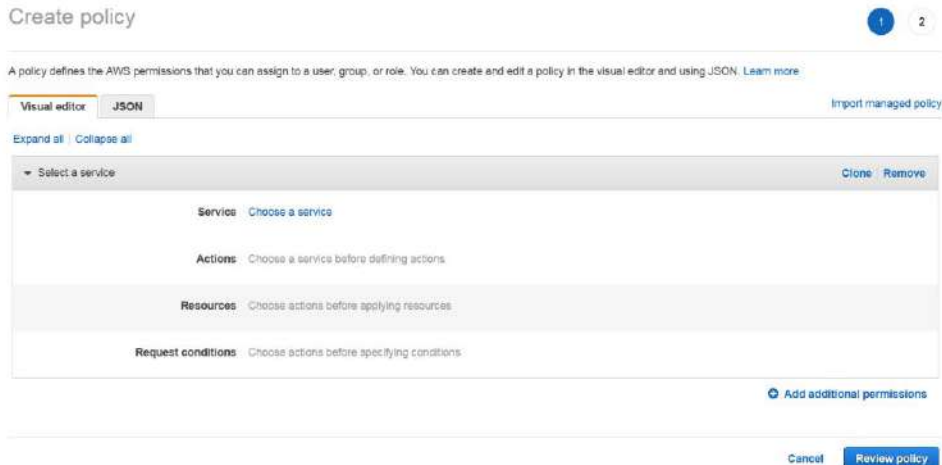
- ▶ Create IAM Policy with least privileges principles (refer to Create an IAM Policy for EWP)
- ▶ Create IAM Role (refer to Create an IAM Role for EWP)
- ▶ Attach IAM Policy to IAM Role (refer to Create an IAM ARN for EWP)

You can also choose to create an AWS IAM User with API Keys that can be configured in EWP following the steps bellow:

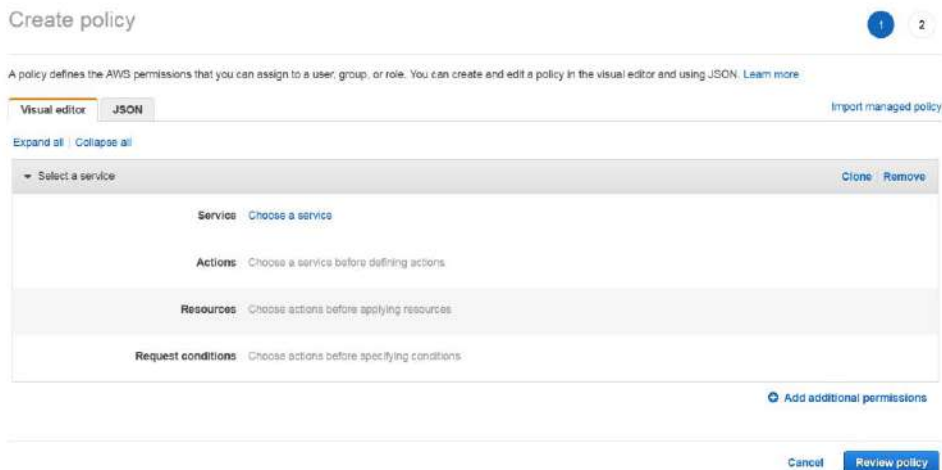
- ▶ Create IAM Policy with least privileges principles (refer to Create an IAM Policy for EWP)
- ▶ Create IAM users with API Keys (refer to Create an IAM Group & Create an IAM User)
- ▶ Use groups to assign permissions to IAM, by assigning an IAM policy to the Group containing the IAM User (refer to Create IAM Keys for EWP)

## 2 Create an IAM Policy for EWP

1. Click on **Policies** on the left of the AWS console and then click on the **Create Policy** button. This will open a page where you can create a new IAM policy.



The screenshot shows the 'Create policy' page in the AWS IAM console. The 'Visual editor' tab is selected. The page includes a description of policies, tabs for 'Visual editor' and 'JSON', and an 'Import managed policy' link. Below this is a section to 'Select a service' with fields for 'Service', 'Actions', 'Resources', and 'Request conditions'. At the bottom right, there are 'Cancel' and 'Review policy' buttons.



This is a duplicate of the previous screenshot, showing the 'Create policy' page in the AWS IAM console with the 'Visual editor' tab selected.

2. Click on the **JSON** tab. This opens an IAM policy editor where you can insert your policy.



The screenshot shows the 'Create policy' page in the AWS IAM console with the 'JSON' tab selected. A yellow error message is displayed at the top: 'This policy validation failed and might have errors converting to JSON: The policy must have at least one statement. For more information about the IAM policy grammar, see AWS IAM Policies'. Below the error message, the 'JSON' tab is active, and a text area contains the following JSON code:

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": []
4- }
  
```

At the bottom right, there are 'Cancel' and 'Review policy' buttons.

The policy for Elastic Workload Protector is explained later in this document and can be found in *Annex* section in JSON format.

Create policy 1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON: The policy must have at least one statement. For more information about the IAM policy grammar, see [AWS IAM Policies](#).

Visual editor **JSON** Import managed policy

```

127     ],
128     "Resource": [
129       "*"
130     ]
131   },
132   {
133     "Sid": "Stmt1493813470000",
134     "Effect": "Allow",
135     "Action": [
136       "sns:ListSubscriptionsByTopic",
137       "sns:ListTopics"
138     ],
139     "Resource": [
140       "*"
141     ]
142   }
143 ]
144 }
  
```

Create policy 1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON: The policy must have at least one statement. For more information about the IAM policy grammar, see [AWS IAM Policies](#).

Visual editor **JSON** Import managed policy

```

127     ],
128     "Resource": [
129       "*"
130     ]
131   },
132   {
133     "Sid": "Stmt1493813470000",
134     "Effect": "Allow",
135     "Action": [
136       "sns:ListSubscriptionsByTopic",
137       "sns:ListTopics"
138     ],
139     "Resource": [
140       "*"
141     ]
142   }
143 ]
144 }
  
```

3. Then click on the **Review policy** button on bottom right and fix **Policy Name** and **Description** if your policy is not valid.

4. To validate your policy, click on the **Create Policy** button.

Create policy 1 2

Review policy

Name\*  Use alphanumeric and \*+,@,\_, characters. Maximum 128 characters.

Description  Maximum 1000 characters. Use alphanumeric and \*+,@,\_, characters.

Summary

Service	Access level	Resource	Request condition
Allow (9 of 148 services) <a href="#">Show remaining 139</a>			
CloudTrail	Limited: List, Read	All resources	None
CloudWatch	Limited: Read	All resources	None
CloudWatch Logs	Limited: List	All resources	None
Config	Limited: List	All resources	None

### 3 Create an IAM Role for EWP





1. Log in to AWS console and enter IAM Service.
2. Click on **Role** on the left menu and then click the **Create role** button.



3. Once you entered Role creation wizard, then choose **Another AWS Account** as type of trusted entities.

Create role 1 2 3 4


Select type of trusted entity

 <b>AWS service</b> <small>EC2, Lambda and others</small>	 <b>Another AWS account</b> <small>Belonging to you or 3rd party</small>	 <b>Web identity</b> <small>Cognito or any OpenID provider</small>	 <b>SAML 2.0 federation</b> <small>Your corporate directory</small>
---	--	--	---


Allows entities in other accounts to perform actions in this account. [Learn more](#)


Specify accounts that can use this role


Account ID\*


Options  Require external ID (Best practice when a third party will assume this role)  
 Require MFA 

- Fill the form using “212828451924” as **Account ID**. Select **Require external ID** as **Options** and use the **AWS IAM External ID** provided in the **AWS Credentials** section of **EWP Inventory**.

 **AWS service**  
EC2, Lambda and others

 **Another AWS account**  
Belonging to you or 3rd party

 **Web identity**  
Cognito or any OpenID provider

 **SAML 2.0 federation**  
Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

---

Account ID\*  ⓘ

Options  **Require external ID** (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents “confused deputy” attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

**External ID**

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

- Select the AWS policy you previously created for EWP.

### Create role

1
2
3
4

▼ Attach permissions policies

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

Create policy ↻

Filter policies  Showing 1 result

	Policy name	Used as	Description
<input checked="" type="checkbox"/>	▶ EWP_Policy	Permissions policy (1)	Policy for use with EWP



6. Add a name to the AWS Role and set a description before clicking on the **Create role** button on the bottom right.

Create role 1 2 3 4

Review

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

**Role name\***   
Use alphanumeric and '+', '@', '\_' characters. Maximum 64 characters.

**Role description**   
Maximum 1000 characters. Use alphanumeric and '+', '@', '\_' characters.

**Trusted entities** The account:212828451924

**Policies** [EWP\\_Policy](#)

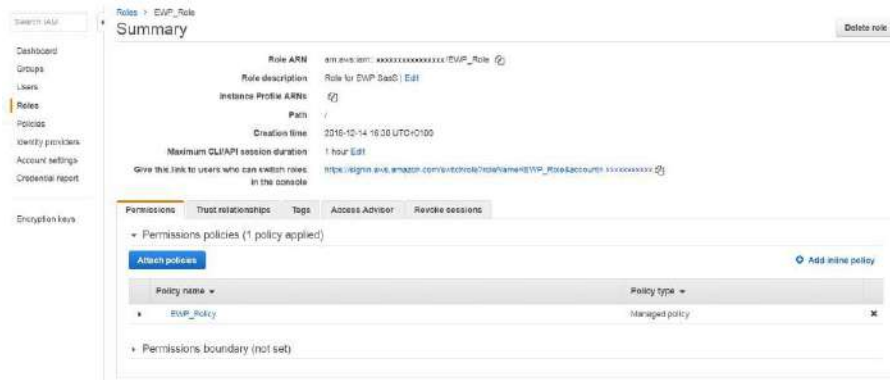
**Permissions boundary** Permissions boundary is not set.

*No tags were added.*

\* Required Cancel Previous Create role

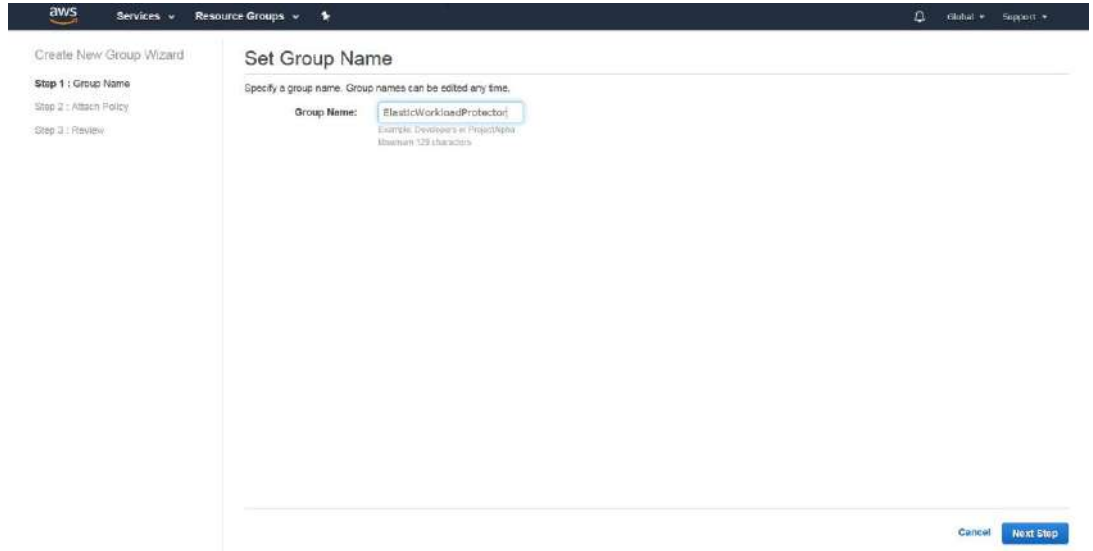
## 4 Create an IAM ARN for EWP

1. Log in to AWS console and enter IAM Service.
2. Click on **Role** on the left menu and then select the Role that have been created for EWP. Then select the **Role ARN** and use it in EWP.



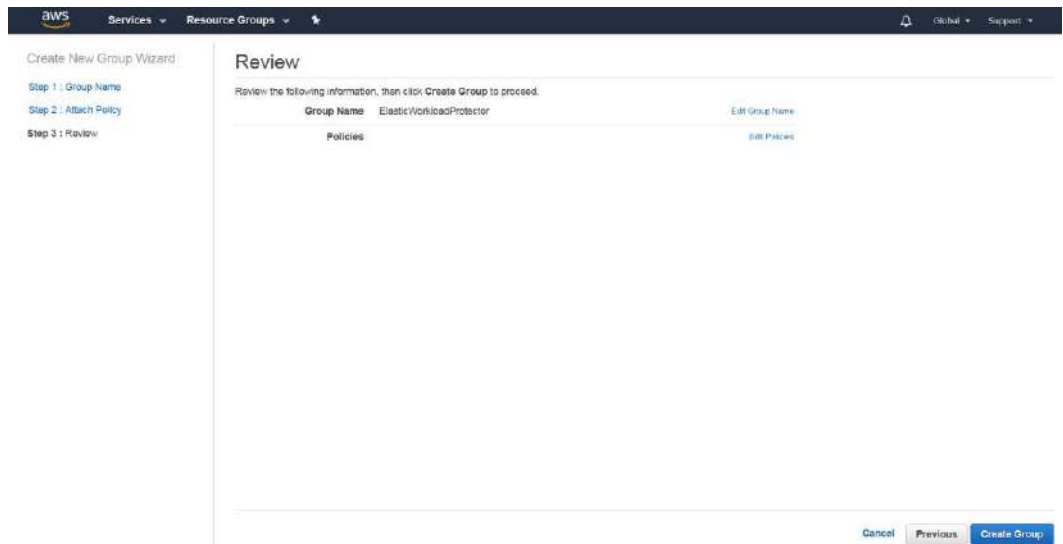
## 5 Create an IAM Group

1. Log in to AWS console and enter IAM Service.
2. Click on **Groups** on the left of the AWS console and then click on the **Create New Group** button. This opens a page where you can create a new IAM group.



The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar shows the 'Create New Group Wizard' with three steps: 'Step 1: Group Name', 'Step 2: Attach Policy', and 'Step 3: Review'. The main content area is titled 'Set Group Name' and contains the instruction 'Specify a group name. Group names can be edited any time.' Below this, there is a 'Group Name' field with the value 'ElasticWorkloadProtector' entered. A tooltip below the field provides an example: 'Example: Developers in ProjectAlpha' and notes 'Maximum 128 characters'. At the bottom right of the main area, there are 'Cancel' and 'Next Step' buttons.

3. Click on **Next Step** button until you reach **Create Group** button.

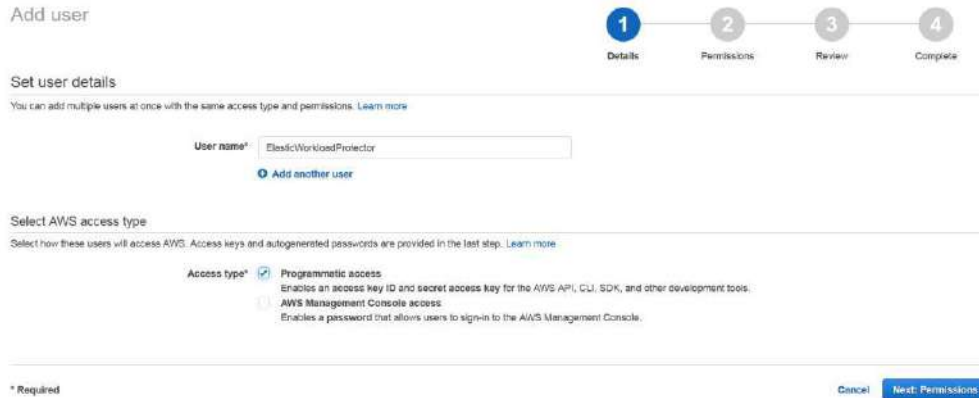


The screenshot shows the AWS IAM console interface at the 'Review' step. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'Review' and contains the instruction 'Review the following information, then click Create Group to proceed.' Below this, there is a table with two columns: 'Group Name' and 'Policies'. The 'Group Name' column contains the value 'ElasticWorkloadProtector' and has an 'Edit Group Name' link next to it. The 'Policies' column is currently empty and has an 'Add Policies' link next to it. At the bottom right of the main area, there are 'Cancel', 'Previous', and 'Create Group' buttons.

This is an empty group without any IAM policy. This will be set later.

## 6 Create an IAM User

1. Click on **Users** on the left of the AWS console and then click on the **Add User** button. This will open a page where you can create a new IAM user.



**Add user** 1 2 3 4  
Details Permissions Review Complete

**Set user details**  
You can add multiple users at once with the same access type and permissions. [Learn more](#)

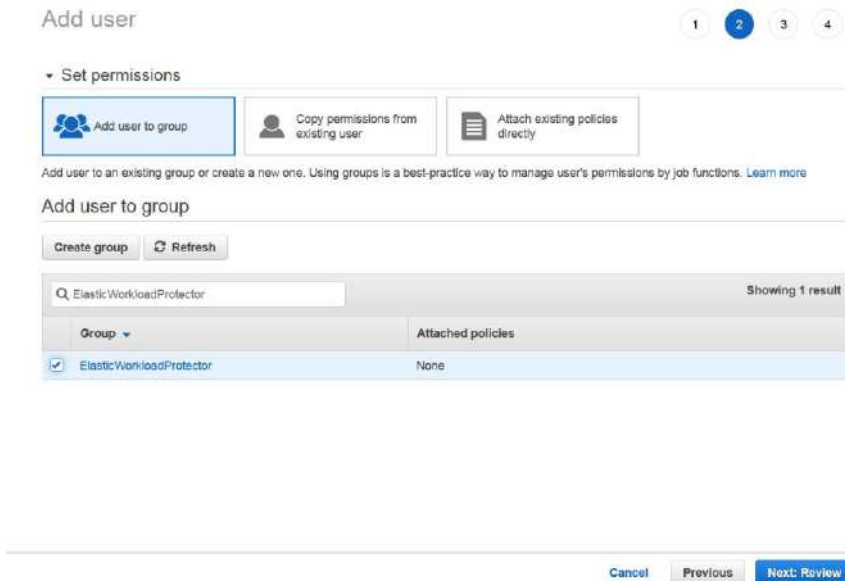
User name\*

**Select AWS access type**  
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*  **Programmatic access**  
 Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.  
 **AWS Management Console access**  
 Enables a password that allows users to sign-in to the AWS Management Console.

\* Required

2. Select the **Programmatic access** check box.
3. Click on **Add user to group** and select *ElasticWorkloadProtector* group in permissions step.



**Add user** 1 2 3 4

▼ Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Add user to group**

Q ElasticWorkloadProtector Showing 1 result

Group	Attached policies
<input checked="" type="checkbox"/> ElasticWorkloadProtector	None

## 4. Save the credentials in the last step of user creation.

Add user

1 Details 2 Permissions 3 Review 4 Complete

**Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://console.aws.amazon.com>

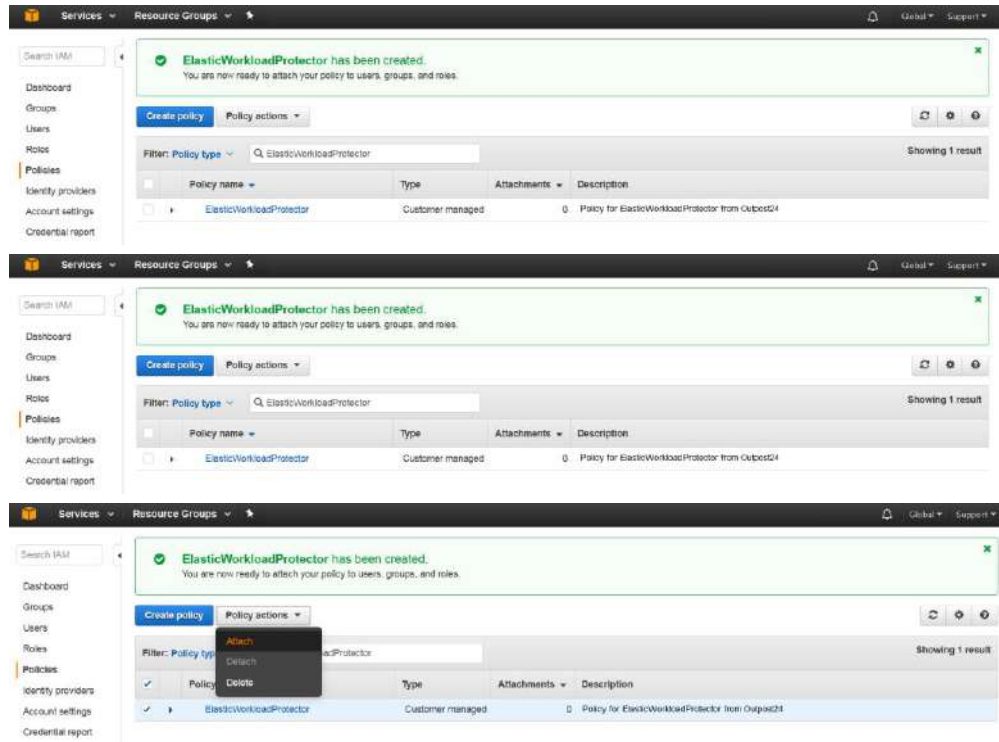
[Download .csv](#)

User	Access key ID	Secret access key
<input checked="" type="checkbox"/> ElasticWorkloadProtector	*****	***** <a href="#">Show</a>

- Created user ElasticWorkloadProtector
- Added user ElasticWorkloadProtector to group SecudIT-ElasticWorkloadProtector
- Created access key for user ElasticWorkloadProtector

## 7 Create IAM Keys for EWP

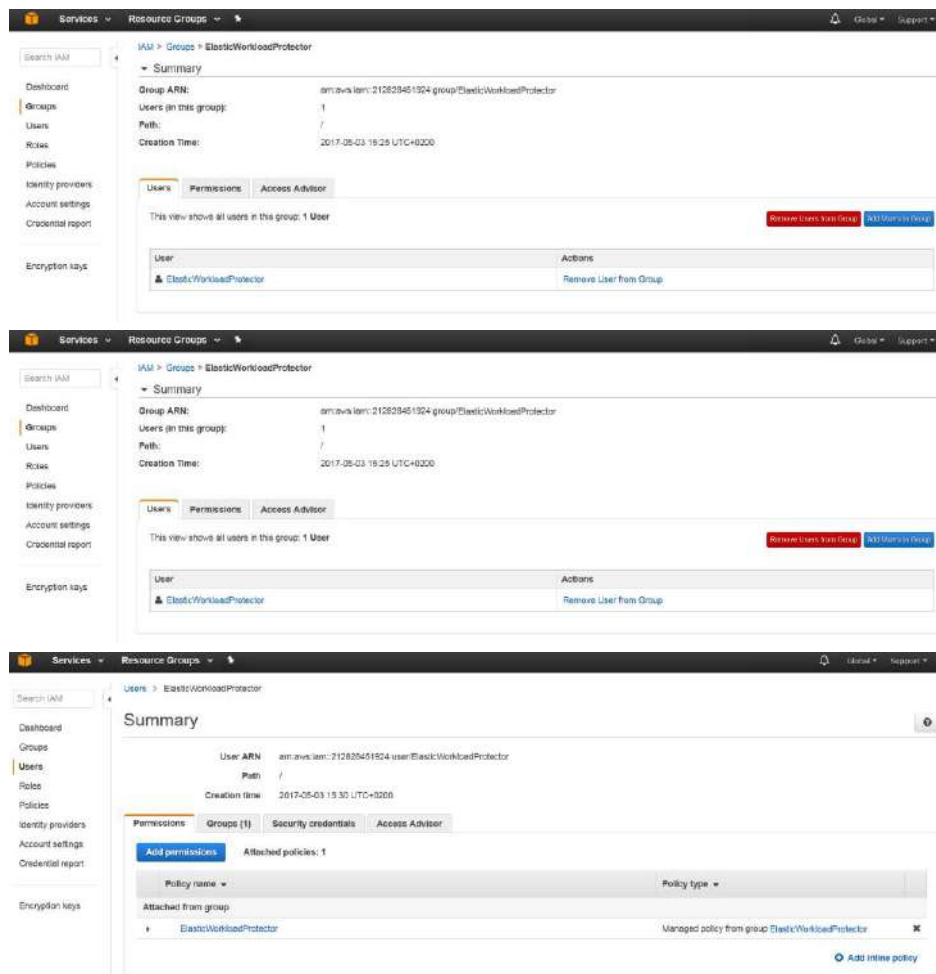
1. Select the previously created policy and attach it to the IAM group previously created.



2. Select the group and attach policy by clicking on the **Attach Policy** button.



3. You now have a user that is in a group with a specific policy.



The first screenshot shows the 'ElasticWorkloadProtector' group page in the AWS IAM console. The 'Users' tab is active, displaying a table with one user: 'ElasticWorkloadProtector'. The 'Actions' column for this user shows a 'Remove User From Group' link. Buttons for 'Remove Users from Group' and 'Add Users to Group' are visible.

The second screenshot is identical to the first, showing the 'Users' tab for the 'ElasticWorkloadProtector' group.

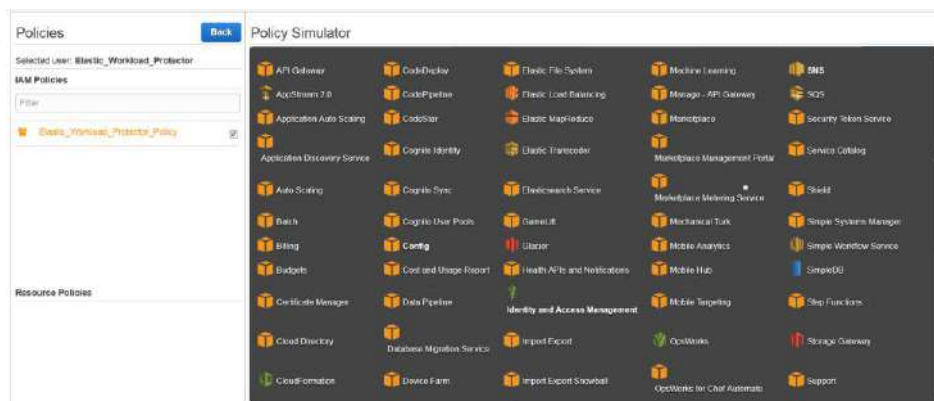
The third screenshot shows the 'Users' page for 'ElasticWorkloadProtector' with the 'Permissions' tab selected. It displays the 'Summary' for the user, including the User ARN, Path, and Creation time. Under the 'Attached policies' section, one policy is listed: 'ElasticWorkloadProtector', which is a 'Managed policy from group ElasticWorkloadProtector'. There is an 'Add inline policy' link at the bottom right of the policy list.

## 8 Checking Policy using AWS Simulator

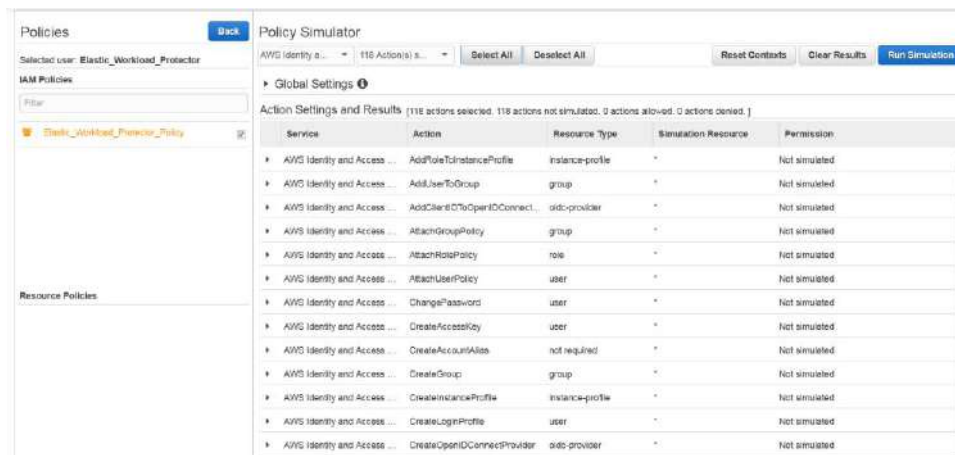
1. Enter IAM simulator and select your user on the left pane.



2. Select an AWS service.



3. Select all actions.





- Then click on the **Run Simulation** button on the top right corner.

AWS Identity a... 118 Action(s) a...

Global Settings ⓘ

Action Settings and Results [118 actions selected, 0 actions not simulated, 14 actions allowed, 104 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
AWS Identity and Access ...	GetPolicy	policy	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetPolicyVersion	policy	*	<b>allowed</b> 1 matching statements.
AWS Identity and Access ...	GetRole	role	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetRolePolicy	role	*	<b>allowed</b> 1 matching statements.
AWS Identity and Access ...	GetSAMLProvider	saml-provider	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetSSHPublicKey	user	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetServerCertificate	server-certificate	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetServiceLastAccessedDetails	not required	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetServiceLastAccessedDetail...	not required	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetUser	user	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	GetUserPolicy	user	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	ListAccessKeys	user	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	ListAccountAliases	not required	*	<b>denied</b> Implicitly denied (no matching st...
AWS Identity and Access ...	ListAttachedGroupPolicies	group	*	<b>denied</b> Implicitly denied (no matching st...

- You are then able to view the AWS permissions for the user.

## 9 Understanding IAM Policy for EWP

The EWP uses the AWS API to interact with your AWS infrastructure on AWS EC2, VPC, and AWS services. In order to do so, the different functionalities of the EWP require different permissions.

### 9.1 AWS Auto-Discovery

This module oversees the automatically discovering of your AWS assets and maintaining an up-to-date list of them.

To be able to list your assets on AWS EC2 and VPC, the following permissions are required on the EC2 service:

- ▶ DescribeInstances, DescribeInstanceStatus, DescribeInstanceAttribute
- ▶ DescribeSecurityGroups
- ▶ DescribeRouteTables, DescribeNetworkAcls, DescribeRouteTables, DescribeSubnets

### 9.2 AWS Continuous Analytics

This module performs continuous monitoring on your AWS environment, meaning that it checks the security of your AWS services according to security standards and best practices such as *CIS AWS Foundations* from the Center for Internet Security.

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the CloudWatch and CloudWatch Logs service:

- ▶ GetMetricStatistics, DescribeMetricFilters

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the EC2 service:

- ▶ DescribeFlowLogs
- ▶ DescribeVpcs

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the CloudTrail service:

- ▶ DescribeTrails
- ▶ GetTrailStatus
- ▶ GetEventSelectors

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the CloudWatchLogs service:

- ▶ DescribeMetricFilters

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the CloudWatch service:

- ▶ DescribeAlarms

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the Config service:

- ▶ DescribeConfigurationRecorderStatus,
- ▶ DescribeConfigurationRecorders

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on IAM service:

- ▶ ListAttachedUserPolicies, ListEntitiesForPolicy, ListPolicies, ListRolePolicies, ListRoles, ListUserPolicies, ListUsers, ListVirtualMFADevices
- ▶ GetAccountSummary, GenerateCredentialReport, GetAccountPasswordPolicy, GetCredentialReport, GetPolicyVersion, GetRolePolicy

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the KMS service:

- ▶ ListKeys
- ▶ GetKeyRotationStatus

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the S3 service:

- ▶ GetBucketAcl, GetBucketLogging, GetBucketPolicy

To be able to automatically configure checks on your assets and monitor them, the following permissions are required on the SNS service:

- ▶ ListSubscriptionsByTopic,
- ▶ ListTopics

## 10 AWS Clone and Scan

This module performs deep inspection vulnerability scan on production instance without any impact. According to the scans planification, it selects the instance to be analyzed, then it *clones and secludes* the instance by creating an AWS Image and launching an instance of the AWS Image in a specific Security Group with a specific AWS Key Pair.

Thus, the EWP has an authenticated access to the instance through the specific AWS Key Pair in the Security Group, configured to only allow connection from the EWP. Once the vulnerability assessment scan is over, the instance is then terminated, and the Image is deregistered.

To be able to clone and to seclude any instance you want to scan on AWS EC2 and VPC, the following permissions are required for the EC2 service:

- ▶ CreateSecurityGroup, AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress
- ▶ CreateTags
- ▶ CreateImage, DescribeImages, DeregisterImage, DeleteSnapshot
- ▶ RunInstances, StartInstances, StopInstances, TerminateInstances, RebootInstances, GetPasswordData
- ▶ DescribeKeyPairs, ImportKeyPair, DeleteKeyPair

## 11 References

AWS IAM Best Practice:

<http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

AWS IAM Policy Simulator:

<https://policysim.aws.amazon.com/home/index.jsp>

### 11.1 Annex -I

AWS Policy for Elastic Workload Protector in JSON format.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1493798226000",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "Stmt1493798278000",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateImage",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
```

```
    "ec2:CreateTags",
    "ec2:DeleteKeyPair",
    "ec2:DeleteSnapshot",
    "ec2:DeregisterImage",
    "ec2:DescribeImages",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceState",
    "ec2:DescribeInstances",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeTags",
    "ec2:DescribeVpcs",
    "ec2:GetPasswordData",
    "ec2:ImportKeyPair",
    "ec2:RebootInstances",
    "ec2:RunInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "Stmt1493805833000",
  "Effect": "Allow",
  "Action": [
    "iam:GenerateCredentialReport",
```

```
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812702000",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812834000",
    "Effect": "Allow",
    "Action": [
```

```
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812945000",
    "Effect": "Allow",
    "Action": [
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigurationRecorders"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813079000",
    "Effect": "Allow",
    "Action": [
        "kms:GetKeyRotationStatus",
        "kms:ListKeys"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813352000",
    "Effect": "Allow",
    "Action": [
```



```

        "logs:DescribeMetricFilters"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813470000",
    "Effect": "Allow",
    "Action": [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Viewing AWS Policy for Elastic Workload Protector Summary in AWS Console.

**Summary** Delete policy

Policy ARN: `arn:aws:iam::212828451924:policy/Elastic_Workload_Protector_Policy`  
 Description: AWS Policy for Elastic Workload Protector user.

Permissions | Attached entities (1) | Policy versions | Access Advisor

Policy summary | **JSON**

Service	Access level	Resource	Request condition
<b>Allow (9 of 100 services)</b>			
CloudTrail	Limited: List, Read	All resources	None
CloudWatch	Limited: Read	All resources	None
CloudWatch Logs	Limited: List	All resources	None
Config	Limited: List	All resources	None
EC2	Limited: List, Read, Write	All resources	None
IAM	Limited: List, Read	All resources	None
KMS	Limited: List, Read	All resources	None
S3	Limited: Read	All resources	None
SNS	Limited: List	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back CloudTrail

Policy summary JSON ⓘ

Q Filter Showing 2 results

Action	Resource	Request condition
List (1 of 2 actions)		
DescribeTrails	All resources	None
Read (1 of 4 actions)		
GetTrailStatus	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back CloudWatch

Policy summary JSON ⓘ

Q Filter Showing 1 result

Action	Resource	Request condition
Read (1 of 5 actions)		
GetMetricStatistics	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back CloudWatch Logs

Policy summary JSON ⓘ

Q Filter Showing 1 result

Action	Resource	Request condition
List (1 of 6 actions)		
DescribeMetricFilters	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back Config

Policy summary JSON ⓘ

Q Filter Showing 1 result

Action	Resource	Request condition
List (1 of 9 actions)		
DescribeConfigurationRecorderStatus	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back EC2

Policy summary JSON ⓘ

Q Filter Showing 27 results

Action	Resource	Request condition
List (11 of 59 actions)		
DescribeFlowLogs	All resources	None
DescribeImages	All resources	None
DescribeInstanceAttribute	All resources	None
DescribeInstances	All resources	None
DescribeInstanceState	All resources	None
DescribeKeyPairs	All resources	None
DescribeNetworkAcls	All resources	None
DescribeRouteTables	All resources	None
DescribeSecurityGroups	All resources	None
DescribeSnapshots	All resources	None
DescribeSubnets	All resources	None

Read (2 of 12 actions)		
DescribeTags	All resources	None
GetPasswordData	All resources	None
Write (15 of 149 actions)		
AuthorizeSecurityGroupEgress	All resources	None
AuthorizeSecurityGroupIngress	All resources	None
CreateImage	All resources	None
CreateKeyPair	All resources	None
CreateSecurityGroup	All resources	None
CreateTags	All resources	None
DeleteKeyPair	All resources	None
DeleteSnapshot	All resources	None
DeregisterImage	All resources	None
ImportKeyPair	All resources	None
RebootInstances	All resources	None
RunInstances	All resources	None
StartInstances	All resources	None
StopInstances	All resources	None
TerminateInstances	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back IAM

Policy summary JSON

Q Filter Showing 14 results

Action	Resource	Request condition
List (9 of 27 actions)		
GetAccountSummary	All resources	None
ListAttachedUserPolicies	All resources	None
ListEntitiesForPolicy	All resources	None
ListPolicies	All resources	None
ListRolePolicies	All resources	None
ListRoles	All resources	None
ListUserPolicies	All resources	None
ListUsers	All resources	None
ListVirtualMFADevices	All resources	None
ListVirtualMFADevices	All resources	None
Read (5 of 25 actions)		
GenerateCredentialReport	All resources	None
GetAccountPasswordPolicy	All resources	None
GetCredentialReport	All resources	None
GetPolicyVersion	All resources	None
GetRolePolicy	All resources	None

Permissions Attached entities (1) Policy versions Access Advisor

< Back KMS

Policy summary JSON

Q Filter Showing 2 results

Action	Resource	Request condition
List (1 of 4 actions)		
ListKeys	All resources	None
Read (1 of 9 actions)		
GetKeyRotationStatus	All resources	None

Permissions		
Attached entities (1)		
Policy versions		
Access Advisor		
← Back S3		
Policy summary		JSON
Q Filter		Showing 2 results
Action	Resource	Request condition
Read (2 of 22 actions)		
GetBucketAct	All resources	None
GetBucketLogging	All resources	None

Permissions		
Attached entities (1)		
Policy versions		
Access Advisor		
← Back SNS		
Policy summary		JSON
Q Filter		Showing 2 results
Action	Resource	Request condition
List (2 of 5 actions)		
ListSubscriptionsByTopic	All resources	None
ListTopics	All resources	None

## 11.2 Annex -II

The below appendix is for specific IAM policy for EWP Workload Analytics + Auto-Discovery in JSON format.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1493798226000",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "Stmt1493798278000",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",

```

```
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493805833000",
    "Effect": "Allow",
    "Action": [
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUserPolicies",
        "iam:ListUsers",
```

```
        "iam:ListVirtualMFADevices"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812702000",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812834000",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493812945000",
    "Effect": "Allow",
    "Action": [
```

```
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigurationRecorders"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813079000",
    "Effect": "Allow",
    "Action": [
        "kms:GetKeyRotationStatus",
        "kms:ListKeys"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813352000",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeMetricFilters"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "Stmt1493813470000",
    "Effect": "Allow",
    "Action": [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
    ]
}
```

```
    ],  
    "Resource": [  
        "*"   
    ]  
  }  
]  
}
```