Outpost24

Vulnerability Management made easy

Generate and Configure an AWS IAM User for EWP

Version: 1.1

2018-12-21

Table of Contents

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

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:

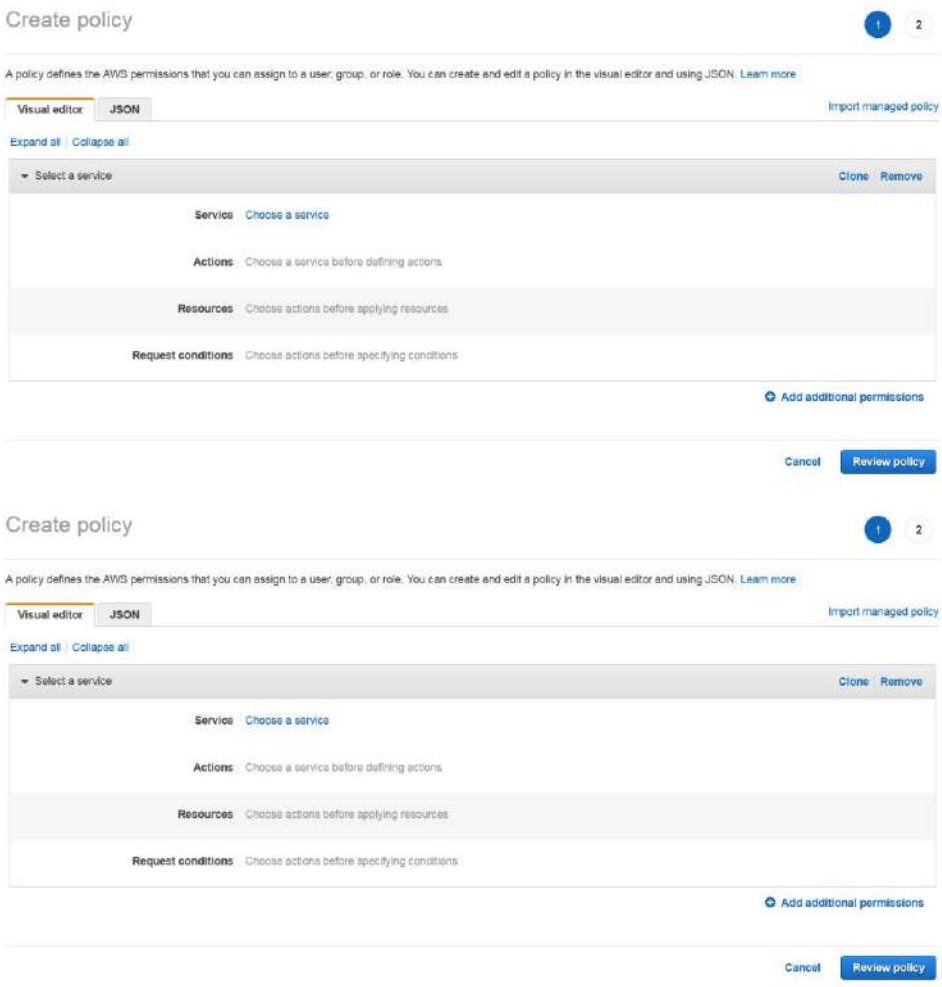
- Create IAM Policy with least privileges principles (refer to Create an IAM Policy for EWP)
- Create IAM Role (refer to Create an IAM Role for EWP)
- Attach IAM Policy to IAM Role (refer to Create an IAM ARN for EWP)

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

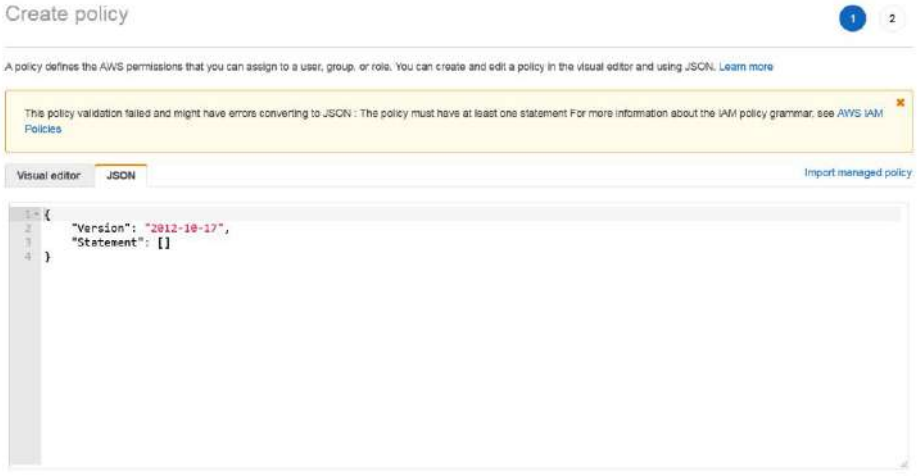
- Create IAM Policy with least privileges principles (refer to Create an IAM Policy for EWP)
- Create IAM users with API Keys (refer to Create an IAM Group & Create an IAM User)
- Use groups to assign permissions to IAM, by assigning an IAM policy to the Group containing the IAM User (refer to Create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

2 Create an IAM Policy for EWP

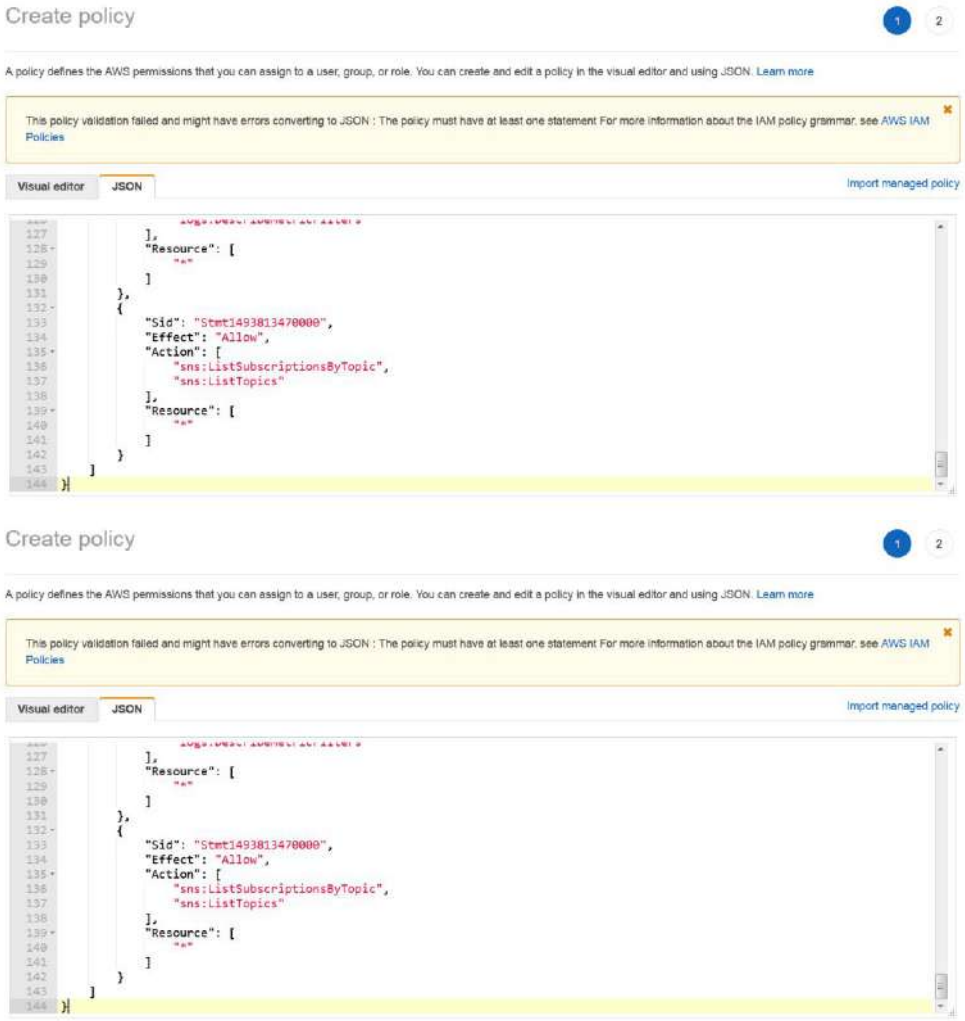
1. Click on **Policies** on the left of the AWS console and then click on the **Create Policy** button. This will open a page where you can create a new IAM policy.



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

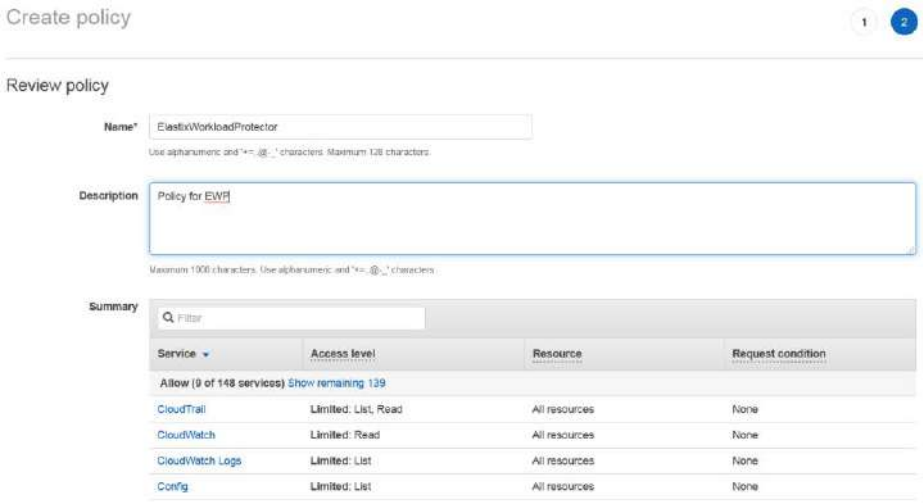


The policy for Elastic Workload Protector is explained later in this document and can be found in *Annex* section in JSON format.



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

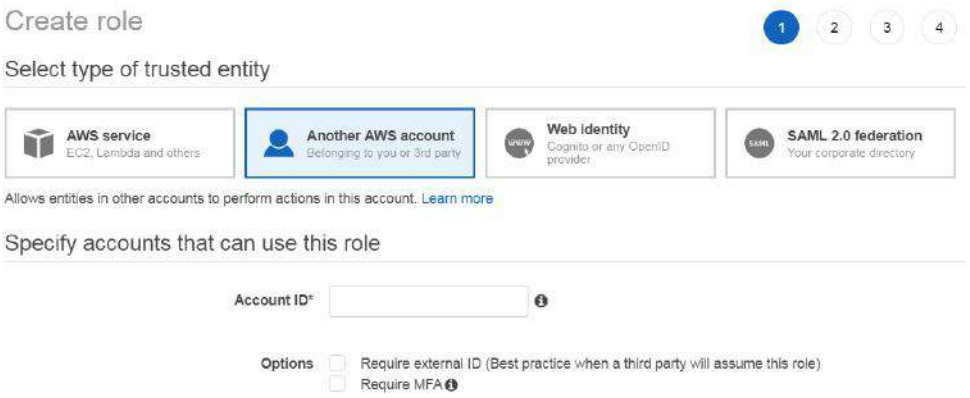
4. To validate your policy, click on the **Create Policy** button.



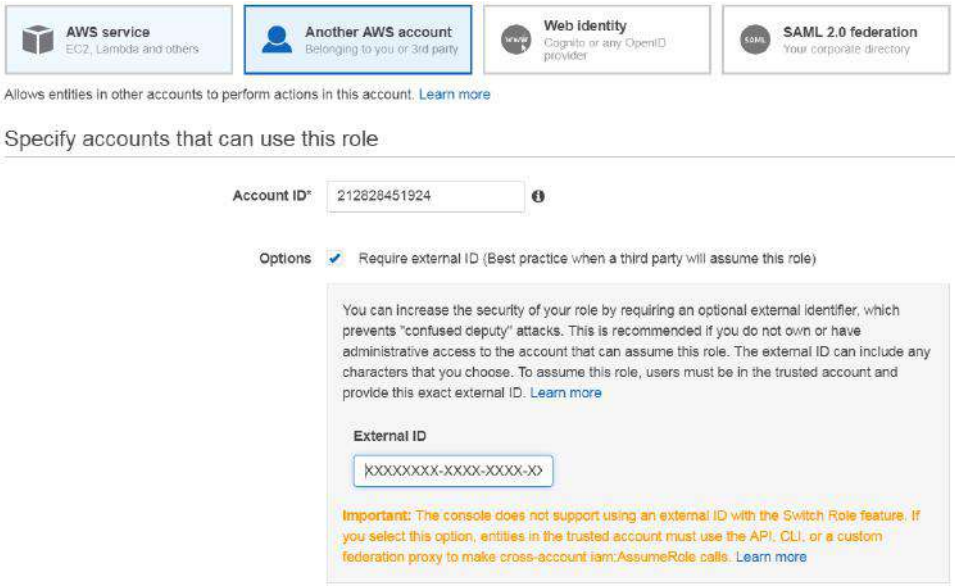
3 Create an IAM Role for EWP

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.

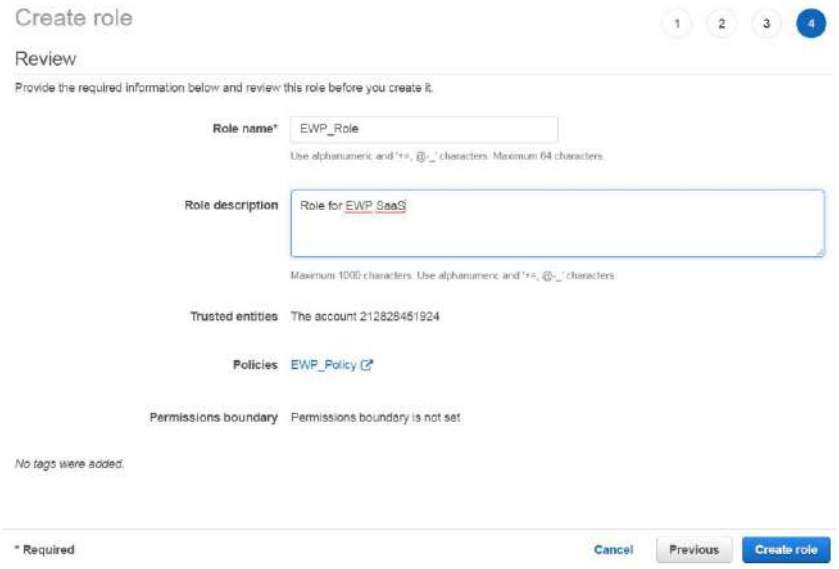


4. Fill the form using “212828451924” as **Account ID**. Select **Require external ID** as **Options** and use the **AWS IAM External ID** provided in the **AWS Credentials** section of **EWP Inventory.**



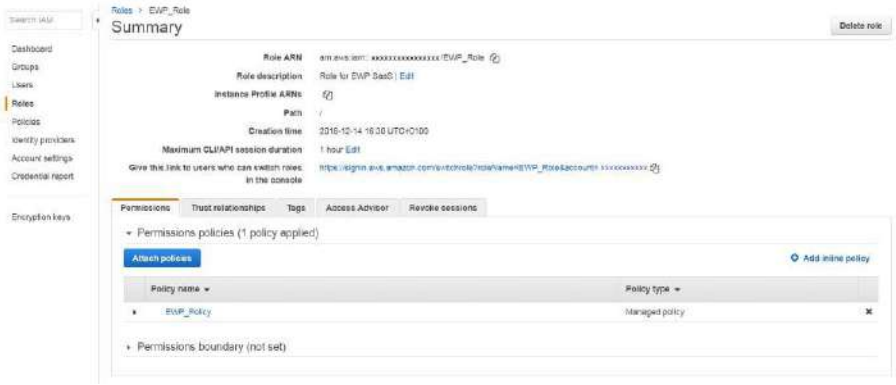
5. Select the AWS policy you previously created for EWP.

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



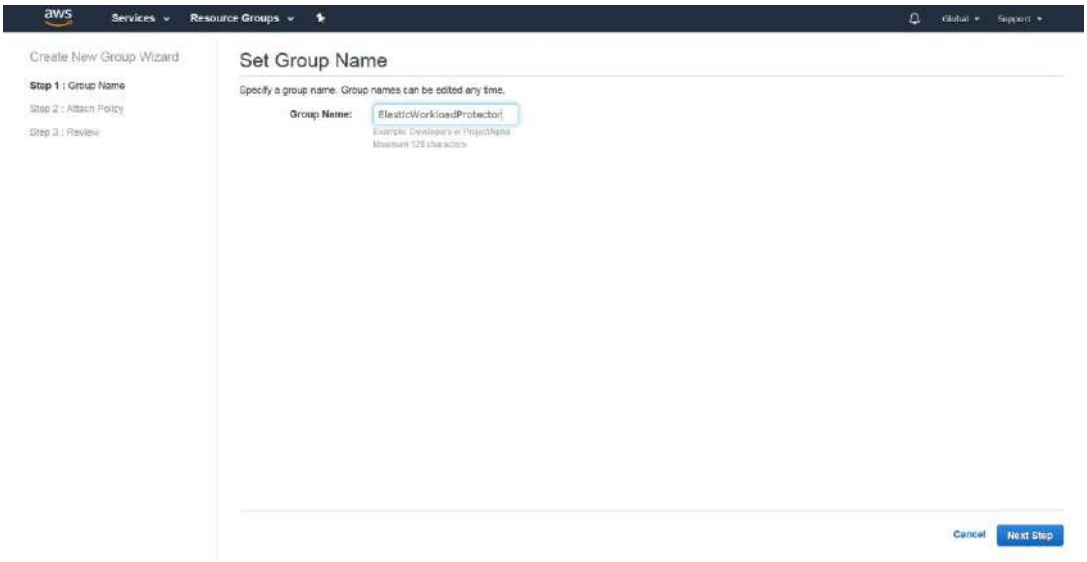
4 Create an IAM ARN for EWP

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**.**

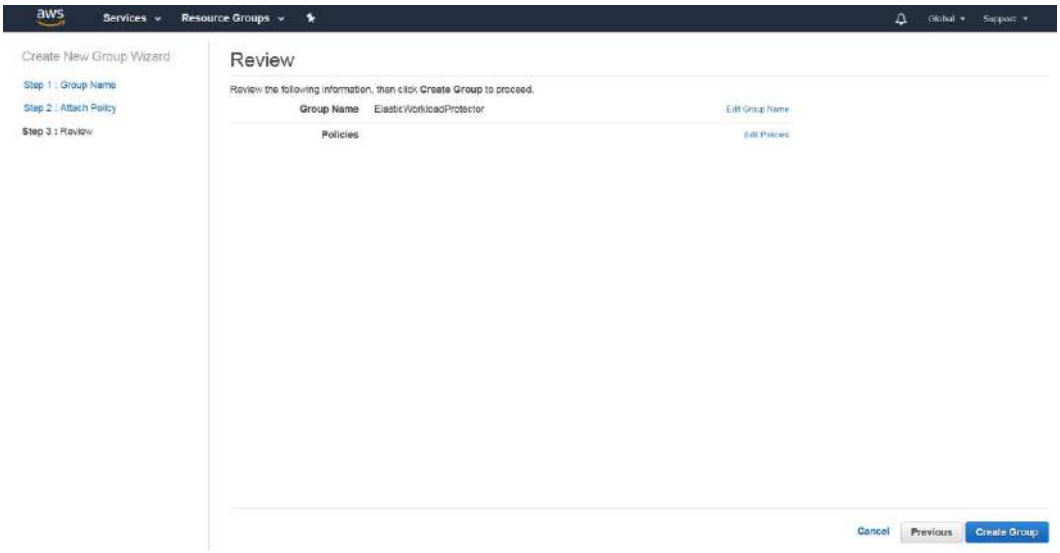


5 Create an IAM Group

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.



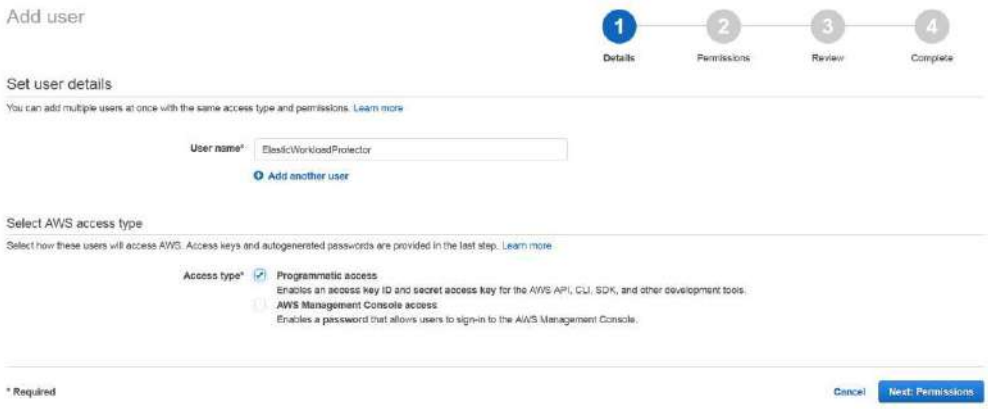
3. Click on **Next Step** button until you reach **Create Group** button.



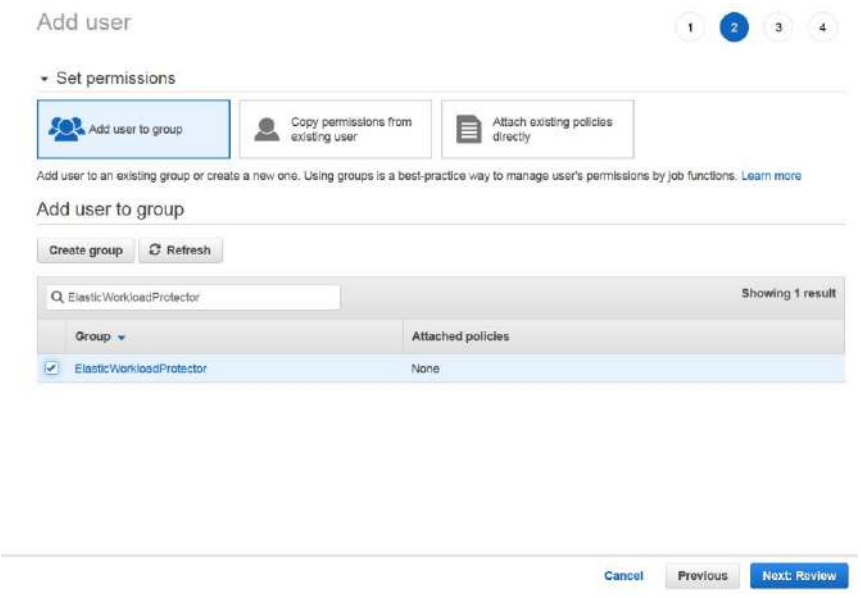
This is an empty group without any IAM policy. This will be set later.

6 Create an IAM User

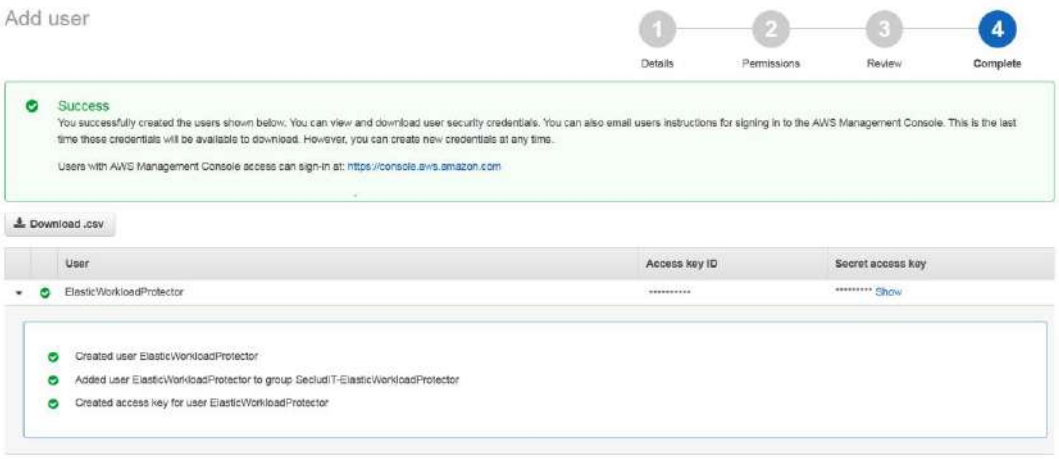
1. Click on **Users** on the left of the AWS console and then click on the **Add User** button. This will open a page where you can create a new IAM user.



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

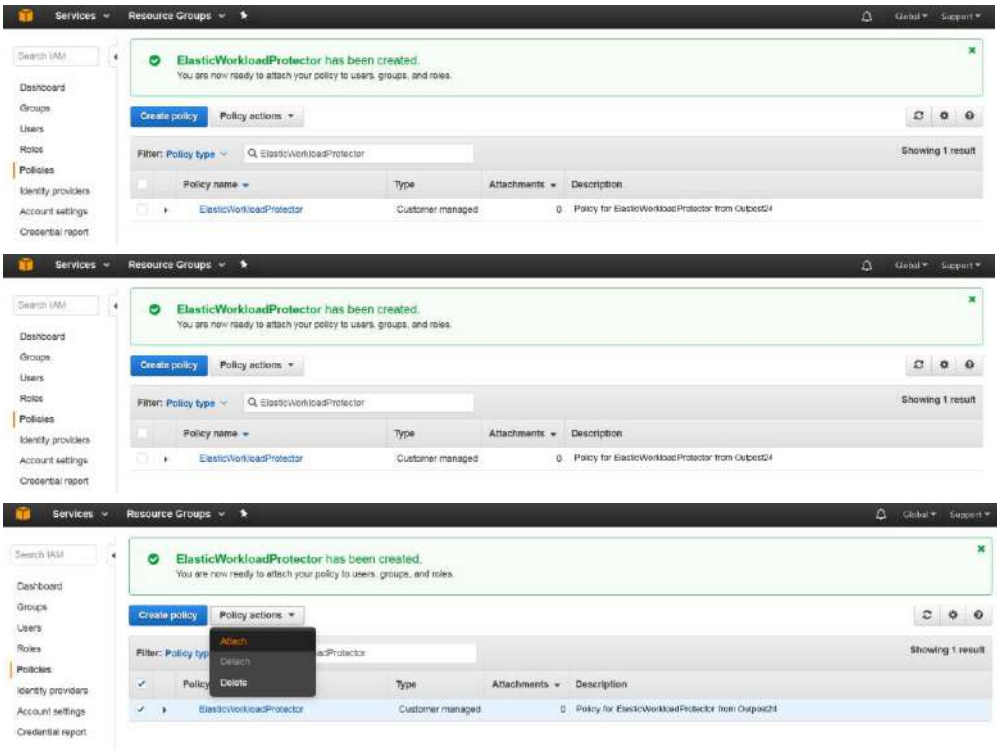


4. Save the credentials in the last step of user creation.



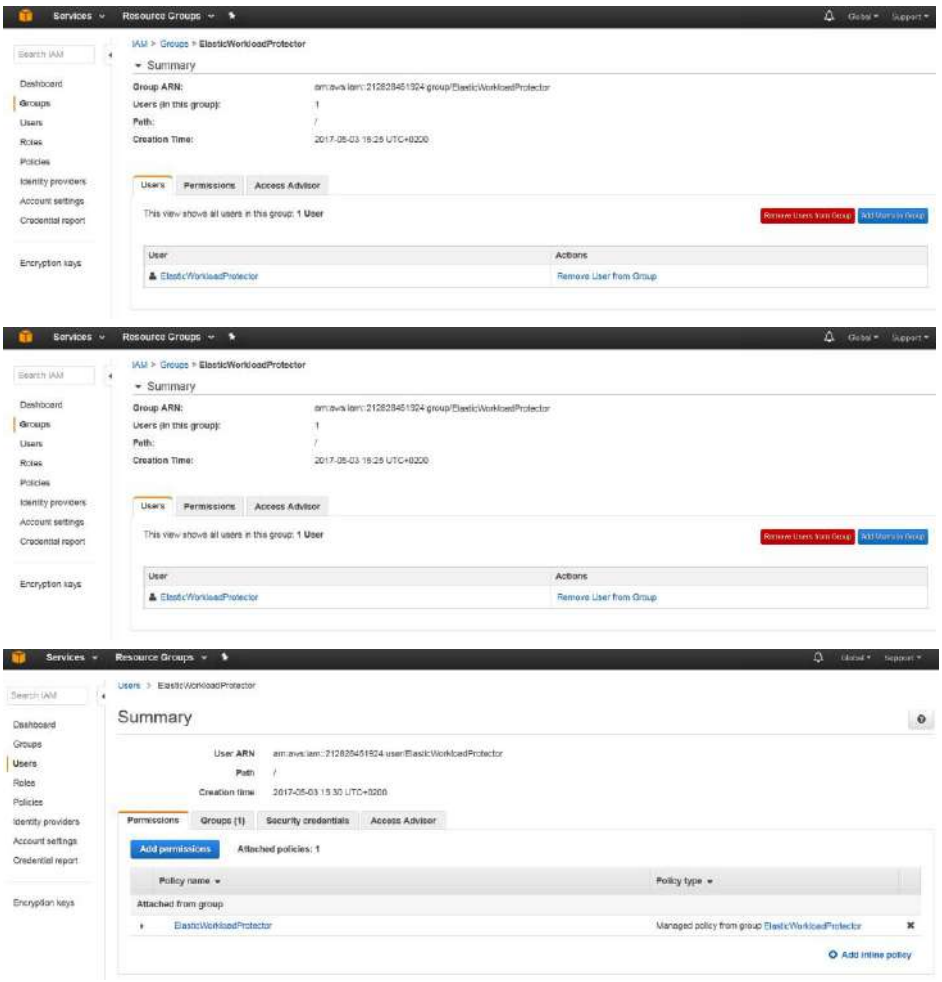
7 Create IAM Keys for EWP

1. Select the previously created policy and attach it 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.

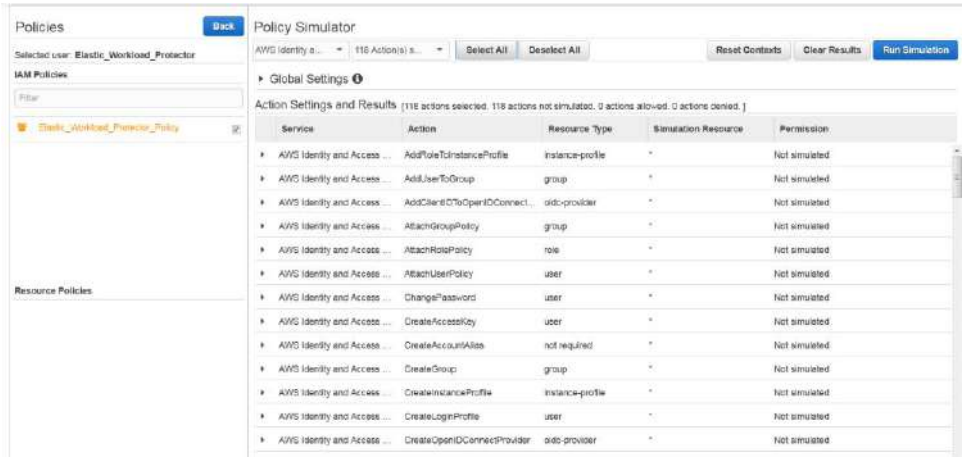


8 Checking Policy using AWS Simulator

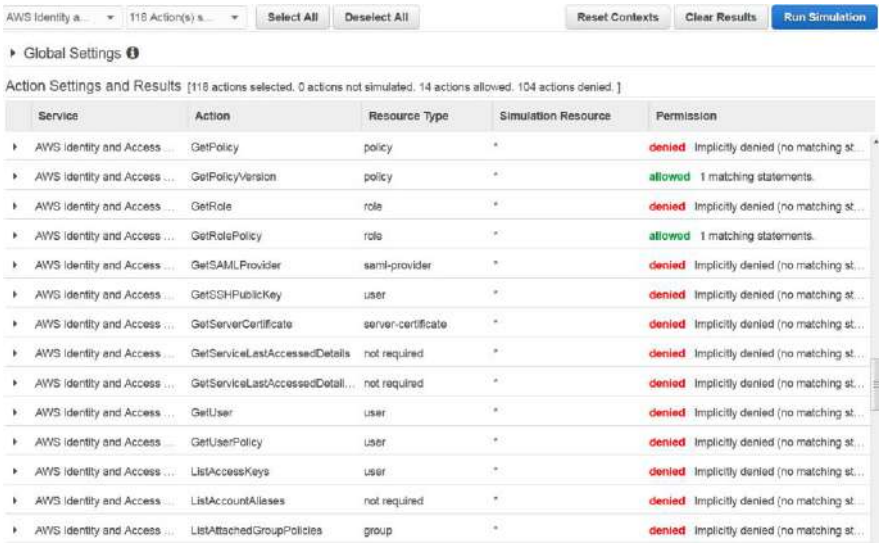
1. Enter IAM simulator and select your user on the left pane.

2. Select an AWS service.

3. Select all actions.



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



5. 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 *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",
```

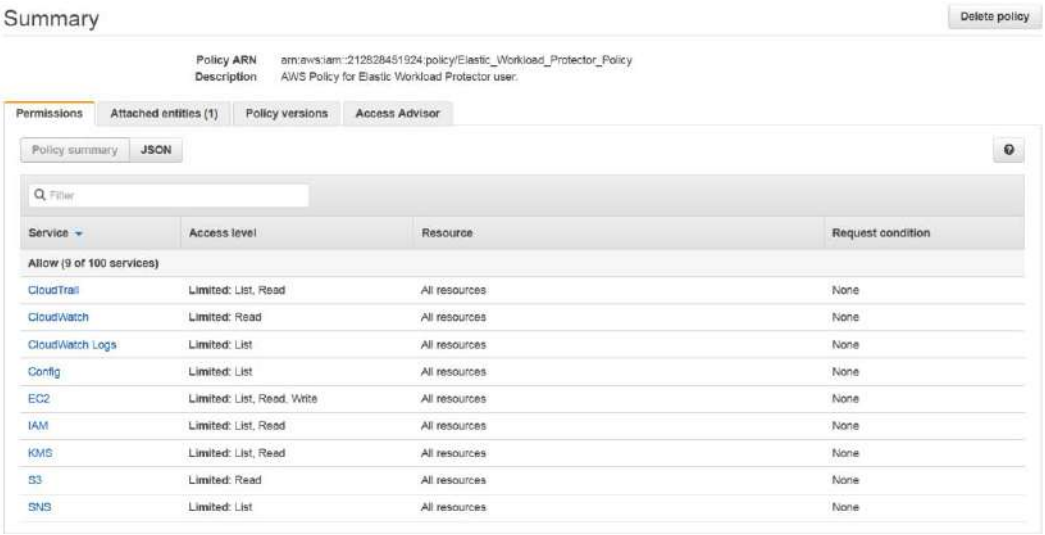
```
            "ec2:CreateTags",
            "ec2:DeleteKeyPair",
            "ec2:DeleteSnapshot",
            "ec2:DeregisterImage",
            "ec2:DescribeImages",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeInstances",
            "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",
```

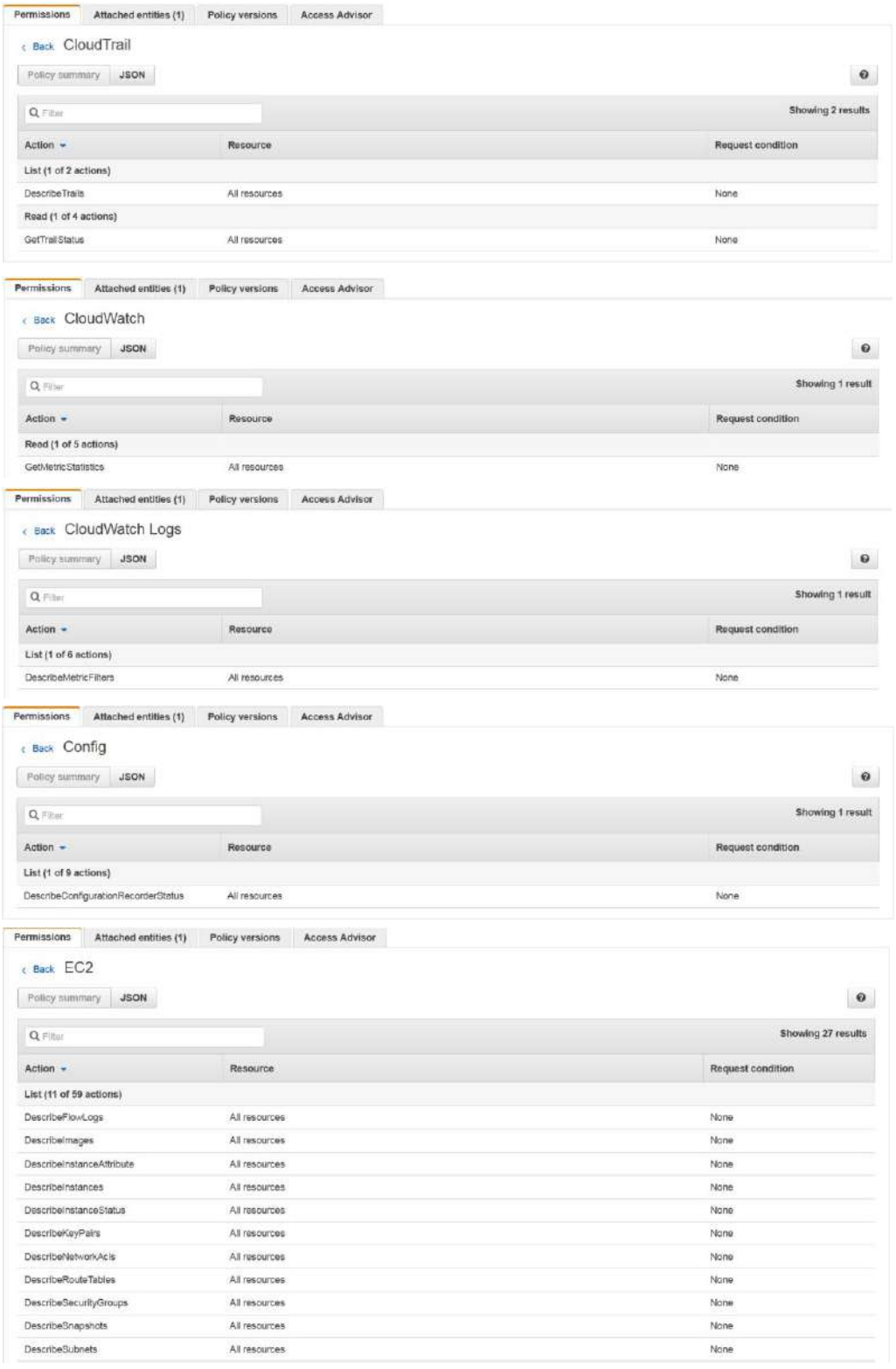
```
            "iam:GetAccountPasswordPolicy",
            "iam:GetAccountSummary",
            "iam:GetCredentialReport",
            "iam:GetPolicyVersion",
            "iam:GetRolePolicy",
            "iam:ListAttachedUserPolicies",
            "iam:ListEntitiesForPolicy",
            "iam:ListPolicies",
            "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.





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

Back CloudTrail

Policy summary | JSON

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

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

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

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

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
DescribeInstanceStatus	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

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

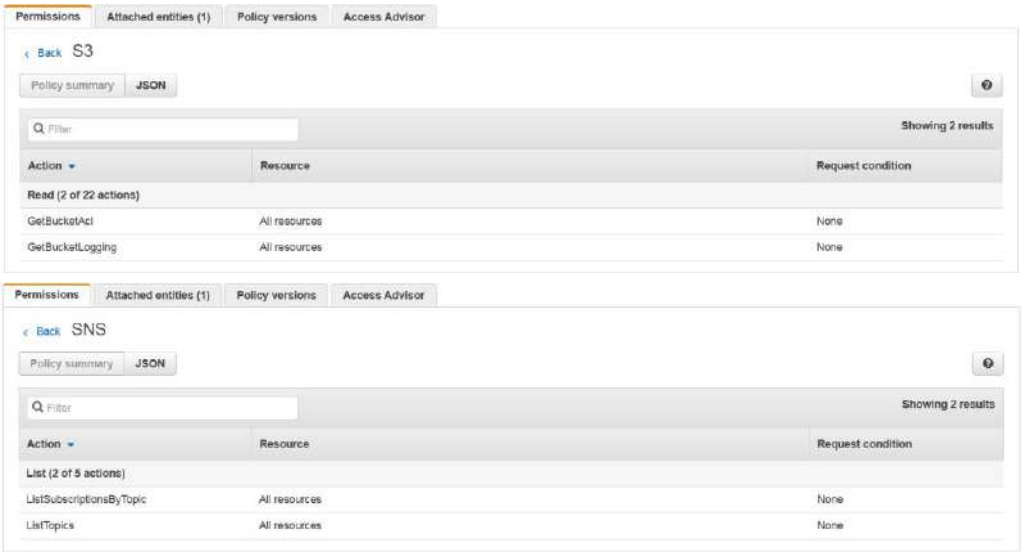
Permissions | Attached entities (1) | Policy versions | Access Advisor

‹ Back KMS

Policy summary | JSON

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



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": [
                    "*"
                ]
            }
        ]
    }
```