Contact Information
ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Resources page on the ForeScout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/legal/intellectual-property-patents-trade marks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Table of Contents

Amazon Web Services Plugin Overview .............................................. 6
  Use Cases .................................................................................. 7
    Providing Consolidated Visibility ........................................... 7
    Encryption .............................................................................. 7
    Dynamic Segmentation of Instances .................................. 7
    Security Management of EC2 Instances ............................... 7
    AWS Account ....................................................................... 7
    IAM Roles and Users .............................................................. 8
    Network .................................................................................. 8
  How It Works ............................................................................ 8
  Polling ...................................................................................... 8

What to Do .................................................................................. 9
  Additional Amazon Web Services Documentation ...................... 9

Requirements ........................................................................... 9
  CounterACT Software Requirements ...................................... 9
  AWS Requirements ................................................................. 10
  Networking Requirements ...................................................... 11
  About Support for Dual Stack Environments ........................... 11

Define AWS Users ..................................................................... 11
  Specifying Permissions Using Standard AWS Policies ................. 11
  Specifying Permissions Using Generic Custom Policies ............... 13
  Specifying Minimal Permissions Using Specific Custom Policies .... 14
    EC2 Instance: Manual Poll .................................................. 14
    EC2 Instance: Take Action on a Resource ............................ 14
    VPC: Manual Poll ............................................................... 15
    VPC: Take Action on a Resource ......................................... 15
    IAM User: Manual Poll ........................................................ 16
    IAM User: Take Action on a Resource ................................. 16
    IAM Role: Manual Poll ....................................................... 17
    Config: Manual Poll .............................................................. 17
    Polling of All Relevant Resources ...................................... 17
    Actions on All Resources ..................................................... 18
    Deploying Lambda Artifacts on AWS .................................. 19
    Complete Recommended Minimal JSON Permissions for AWS Plugin .... 19
  Access AWS Credentials ........................................................ 21
  Enable AWS Config on AWS Account ........................................ 21

Configure the Plugin ................................................................ 22
  Add an AWS Connection .......................................................... 23
  About Delta Polling ................................................................. 28
  Verify That the Plugin Is Running .......................................... 29
  Test the AWS Connection ...................................................... 29
  Manually Deploy Delta Polling Artifacts ...................................... 30
Hybrid Cloud Module: Amazon® Web Services (AWS) Plugin

Configuration Guide

- Manually Poll EC2 Instances .................................................. 31
- Edit the AWS Connection .................................................... 33
- Remove the AWS Connection ................................................. 34

**Configure AWS Policy Templates** ........................................... 35
- Access AWS Policy Templates .................................................. 35
- Policy Template Procedure .................................................... 36
- AWS Policy Templates ........................................................... 41
  - EC2 Instances Policy Templates .............................................. 41
  - IAM Users and Roles Policy Templates ...................................... 41
  - VPCs Policy Templates ........................................................ 42
- OTHER Policy Templates ........................................................ 42
- Update the AMI Whitelist ...................................................... 42

**Detecting Cloud Endpoints – Host Properties** ......................... 44
- AWS Properties ................................................................. 44
- AWS EC2 Properties ............................................................ 45
- AWS IAM Role Properties ..................................................... 48
- AWS IAM User Properties ..................................................... 48
- AWS Service Properties ........................................................ 50
- AWS VPC Properties ............................................................ 50

**Managing AWS Cloud Endpoints** ........................................ 51
- Access AWS IAM Role Inventory .............................................. 52
- Access AWS EC2 Inventory ..................................................... 53
- Access AWS IAM User Inventory .............................................. 55
- Access AWS VPC Inventory ..................................................... 56

**Run Policy Actions** ............................................................. 57
- Manually Run AWS Actions on EC2 Instance .............................. 57
  - Apply EC2 Security Groups Action ........................................... 58
  - Disable EC2 Termination Protection Action ............................... 61
  - Enable EC2 Termination Protection Action ................................ 62
  - Start EC2 Instance Action ...................................................... 64
  - Stop EC2 Instance Action ..................................................... 66
- Manually Run AWS IAM Actions .............................................. 68
  - Activate User Access Key Action ............................................. 70
  - Deactivate User Access Key Action ......................................... 71
  - Delete User Access Key Action .............................................. 73
  - Enforce Password Policy Action ........................................... 75
- Manually Run AWS VPC Actions .............................................. 78
  - Detach Internet Gateway(s) Action .......................................... 79

**Best Practices for Working with the AWS Plugin** ....................... 81

**Hybrid Cloud Module Information** ........................................ 82

**Additional CounterACT Documentation** ................................. 82
Documentations Downloads .............................................................. 82
Documentation Portal ....................................................................... 83
CounterACT Help Tools..................................................................... 83
Amazon Web Services Plugin Overview

The Amazon Web Services Plugin is a component of the ForeScout CounterACT® Hybrid Cloud Module. See Hybrid Cloud Module Information for details about the module.

The AWS Plugin connects to the Amazon® Web Services (AWS) public cloud environment to retrieve information on Elastic Compute Cloud (EC2) instances and other AWS entities such as Identity and Access Management (IAM) users and Virtual Private Clouds (VPCs). The EC2 instances, IAM users, and VPCs follow similar rules as any other endpoint discovered by CounterACT where one can define policies and actions on those entities. CounterACT's integration with AWS brings the detailed visibility, control, compliance, and orchestration capabilities of CounterACT to EC2 instances and the associated AWS cloud configurations.

The AWS Plugin enables:

- Visibility of endpoints, IAM users, and VPCs in Amazon’s public cloud
- Creating and applying CounterACT policies across the AWS entities
- Maintaining the security and compliance of cloud instances, IAM users, and VPCs
- Applying security groups to instances, enforcing password policies, and a range of other policy actions

In this guide, the terms "endpoint" and "instances" are used interchangeably.

This plugin assists IT with a number of important challenges when it comes to cloud operations. By integrating CounterACT with AWS, you can:

- Have full visibility of your AWS instances and their properties. Since disparate teams may be starting and stopping instances in a public cloud environment, it is important for all of IT to have a good understanding of what resources are being used in the cloud. Regular checks provide valuable information on how and when AWS cloud resources are being used.

- Use the CounterACT Asset Inventory to review the distribution of endpoints in the cloud and mitigate them as required. For example, endpoints with out-of-date Amazon Machine Images (AMIs) are quickly identified for remediation.

- Enable/Disable Termination Protection for AWS EC2 instances to prevent accidental termination (deletion) of an EC2 instance. The CounterACT operator implements this by establishing a policy in which all compliant and critical EC2 assets have termination protection enabled. See Disable EC2 Termination Protection Action and Enable EC2 Termination Protection Action for details.

- Collect information about the AWS environment across multiple AWS regions and multiple AWS accounts, all from a common deployment. This includes fine grained details such as the creation of new IAM users, lack of password changes, the presence of Internet Gateways in a VPC, and many more AWS operational details.
Discover cloud-based endpoints early, allowing identification and compliance checking of the workload itself. A non-compliant endpoint can be stopped, assigned to a quarantined security group, and/or the AWS account team can be notified. If remediation activities fail, the endpoint can be fully isolated and stopped to prevent further damage.

Use Cases
This section describes sample use cases supported by this plugin. To understand how this plugin helps you achieve these goals, see How It Works.

Providing Consolidated Visibility
Integrating with AWS extends CounterACT’s capability to see and control instances running in AWS. This allows visibility for campus, data center, and cloud endpoints from the same CounterACT device (depending on the scale of the environment).

Encryption
Policy templates are provided to verify that EC2 Elastic Block Storage (EBS) is encrypted. EBS volumes associated with an EC2 instance are collected. An optional action to stop non-compliant EC2 instances is also provided.

Dynamic Segmentation of Instances
Instances can be segmented or isolated based on their classification and compliance posture. For example, tags can be used to classify and group instances that belong to a particular group such as testing, development, and production. Additionally, instances can be classified based on their function such as web, application, or database tier.

Security Management of EC2 Instances
The AWS plugin makes it easy for you to detect EC2 instances configured with either default or non-compliant security groups. You can then take action to remediate that by applying stricter security policies using your own well-defined security groups, making that security group compliant.

AWS Account
Policy templates are provided to verify that Multi-Factor Authentication (MFA) is enabled for the root user, to continuously monitor if the password has not been changed, and to verify that AWS Config is enabled for an AWS account.
IAM Roles and Users

IAM users, group, and roles and associated properties can be collected. Policy templates are provided to continuously monitor for any IAM role being created or modified, to continuously monitor for any IAM user being created or modified, to verify that a password policy is enabled for every user, and implement an action to enable a password policy for users who do not have a password policy set.

Network

VPCs configured for an AWS account and the associated properties, such as subnets, Internet gateways, and VPC peers, can be collected. Policy templates are provided to verify that no EC2 instance has a public IP address that is an Internet-facing address, to monitor external ELB associated with a VPC, and to monitor VPC peering connections and allow peering connections between central VPCs and sub-VPCs. An action to allow for termination of an Internet gateway is also provided.

How It Works

This plugin uses well-defined APIs from AWS to provide visibility of AWS EC2 instances, IAM users, and VPCs.

Once the configuration is completed using an AWS account with the appropriate IAM credentials and permissions, CounterACT starts communicating with one or more AWS accounts and retrieves information on EC2 instances running in AWS under that account as well as the IAM users and VPCs. Instance-related properties are collected as CounterACT host properties while other cloud entities such as IAM users and VPCs are also displayed as logical endpoints in CounterACT. The query and collection of AWS entities and associated properties are invoked at configured time intervals.

Polling

To support continual updates of AWS properties, AWS 2.0 combines full polling with an optional delta polling mechanism. This ensures that AWS state changes are recognized in near real-time by CounterACT. The full poll gathers all aspects of the AWS environment from AWS APIs. The AWS APIs expose multiple attributes of the entities associated with an AWS account.

Since this data can be quite extensive, the full poll takes place at longer intervals with the default being 30 minutes. The optional delta polling was added in AWS 2.0 so that EC2 instance state changes are recognized immediately by CounterACT. The delta poll leverages the functionality exposed by AWS Config, Lambda functions, and CloudWatch logs to quickly capture EC2 state changes. Since this only looks for delta changes to EC2, it takes place over shorter intervals with a default of one minute.

CounterACT requires a range of different permissions to enable polling services, including the ability to deploy delta polling into the AWS environment.

See Specifying Permissions Using Standard AWS Policies for additional details about AWS permissions, as well as Best Practices for Working with the AWS Plugin for more information.
What to Do

This section describes steps you should take to set up your system when integrating with AWS environments:

1. Verify that you have met system requirements. See Requirements.
2. Define AWS Users.
3. Configure the Plugin.
4. Use the in-depth information reported by the plugin to manage virtual devices:
   - Configure AWS Policy Templates
   - Detecting Cloud Endpoints – Host Properties
   - Managing AWS Cloud Endpoints
   - Run Policy Actions

Additional Amazon Web Services Documentation

To use the AWS plugin, you should have a good understanding of Amazon Web Services and EC2 concepts, functionality, and terminology, and understand how CounterACT policies and other basic features work. For more information on installation, configuration, and general guides, see:

https://aws.amazon.com/documentation/

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- AWS Requirements
- Networking Requirements

CounterACT Software Requirements

The plugin requires the following CounterACT release and other CounterACT components:

- CounterACT version 8.0.1 or above
- Hybrid Cloud Module version 1.2.0 or above with the AWS component running
AWS Requirements

This plugin requires the following AWS components:

- An Amazon Web Services online account is required.
- You will need one AWS Access Key ID and Secret Key to configure the AWS plugin. These are associated with a User profile on AWS. The access key ID is a unique identifier associated with a secret key. These two keys are used by the AWS plugin to communicate with AWS on behalf of that user.
- If you are using a proxy server with Basic Authentication, you will need that proxy's credentials.
- The plugin requires the following AWS services:
  - **Amazon EC2** – Amazon Elastic Compute Cloud (Amazon EC2) is a web service that enables you to launch and manage Linux / UNIX and Windows server instances in Amazon’s public cloud.
  - **Amazon VPC** – Amazon Virtual Private Cloud (VPC) is a web service for provisioning a logically isolated section of AWS Cloud where you can launch AWS resources in a virtual network you define. You control your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
  - **CloudWatch** - CloudWatch is a web service that enables you to monitor and manage various metrics. It also allows the configuration of alarm actions based on the metrics data.

There are two user permissions options that can be used on CounterACT:

- Read-only permissions (CounterACT will support visibility only)
- Full permissions (CounterACT will support both visibility and control)

For further information about AWS EC2, refer to the [AWS EC2 User Guide](#).
Networking Requirements

The following must be configured on enterprise firewalls to support communication between CounterACT and AWS regional access points.

- Outgoing communication on port 443/TCP must be allowed
- The *.amazonaws.com domain must be reachable with HTTPS
- (Optional) Proxy communication, for example, port 8080 is open

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component.** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

Define AWS Users

To allow CounterACT to query AWS, define a user with the Identity and Access Management (IAM) service. Specify the credentials of this user when you define CounterACT connections to AWS.

Because the plugin detects and manages a range of AWS entities, the AWS user used by CounterACT should have full access across a range of permissions. If there is no need to manage AWS entities through CounterACT actions, the AWS user used by CounterACT only needs read-only permissions.

The permissions are described in the following sections:

- Specifying Permissions Using Standard AWS Policies
- Specifying Permissions Using Generic Custom Policies
- Specifying Minimal Permissions Using Specific Custom Policies

For all JSON examples in the permissions sections, copy them from the permissions sections and paste them unchanged into the AWS Console for the AWS Account.

In addition, AWS Config needs to be manually enabled on your AWS account, per region. See [Enable AWS Config on AWS Account](#).

Specifying Permissions Using Standard AWS Policies

The range of AWS permissions needed by CounterACT are listed in this section.

Review [Polling](#) for additional details on the differences.
<table>
<thead>
<tr>
<th>Item</th>
<th>Resources</th>
<th>Permission Needed</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover resource (FULL POLL)</td>
<td>EC2 Instances, VPC, Peering Connections</td>
<td>AmazonEC2ReadOnlyAccess</td>
<td></td>
</tr>
<tr>
<td>Discover resource (FULL POLL)</td>
<td>IAM Users, IAM Roles</td>
<td>IAMReadOnlyAccess</td>
<td></td>
</tr>
<tr>
<td>Discover resource (FULL POLL)</td>
<td>AWS Config</td>
<td>AWSConfigUserAccess</td>
<td></td>
</tr>
<tr>
<td>Discover modification to a resource (DELTA POLL)</td>
<td>EC2 Instances</td>
<td>CloudWatchLogsReadOnlyAccess</td>
<td>This is determined by reading CloudWatch logs that are populated by CloudWatch Events. Prerequisite: CloudWatch Event Rules/Lambda functions and CloudWatch Log groups need to be deployed on that account/region.</td>
</tr>
<tr>
<td>Discover modification to a resource (DELTA POLL)</td>
<td>VPC, Peering Connections, IAM Users, IAM Roles</td>
<td>CloudWatchLogsReadOnlyAccess</td>
<td>This is determined by reading CloudWatch logs that are populated by AWS Config. Prerequisite: AWS Config needs to be enabled on that account/region, and CloudWatch Event Rules/Lambda functions and CloudWatch Log groups need to be deployed on that account/region.</td>
</tr>
<tr>
<td>Perform action on a resource</td>
<td>EC2 Instances, VPC</td>
<td>AmazonEC2FullAccess</td>
<td></td>
</tr>
<tr>
<td>Perform action on a resource</td>
<td>IAM User</td>
<td>IAMFullAccess</td>
<td></td>
</tr>
</tbody>
</table>
Deploy AWS to CounterACT delta polling update functionality

<table>
<thead>
<tr>
<th>Per Account/Per Region</th>
<th>AWSLambdaFullAccess</th>
</tr>
</thead>
</table>
| This enables the CounterACT AWS plugin to create a Lambda function in AWS so that CounterACT delta polling has updated information related to EC2 instances.

The permission policies in this table are standard policies present in AWS.

Ideally, you need to use the following policies for CounterACT to perform all of the functions listed above:

- AWSConfigUserAccess
- CloudWatchLogsReadOnlyAccess
- AmazonEC2FullAccess
- IAMFullAccess
- AWSLambdaFullAccess

Specifying Permissions Using Generic Custom Policies

Alternatively, you could also choose to create a custom policy. The JSON example below allows read access on ELBs and read/write access on all resources on the other seven services listed.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:*",
                "config:*",
                "ec2:*",
                "elasticloadbalancing:Describe*",
                "events:*",
                "iam:*",
                "lambda:*",
                "logs:*
            ],
            "Resource": "*"
        }
    ]
}
```
Specifying Minimal Permissions Using Specific Custom Policies

This section contains the permissions for various operations, using the principle of the least or minimal privilege.

The following JSON examples are for the current set of operations that the plugin performs. A later version of the plugin, using newer APIs, will necessitate an update of these permissions.

Note that these various individual permissions can be in common JSON. For additional details see AWS postings on these topics such as:


**EC2 Instance: Manual Poll**

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeVolumes",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

**EC2 Instance: Take Action on a Resource**

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```
"Effect": "Allow",
"Action": [
  "ec2:StartInstances",
  "ec2:ModifyNetworkInterfaceAttribute",
  "ec2:ModifyInstanceAttribute",
  "ec2:StopInstances"
],
"Resource": "*"
]

VPC: Manual Poll

{ "Version": "2012-10-17",
 "Statement": [
  { "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInternetGateways",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcPeeringConnections",
      "ec2:DescribeNetworkAcls",
      "ec2:DescribeRouteTables",
      "ec2:DescribeEgressOnlyInternetGateways",
      "elasticloadbalancing:DescribeLoadBalancers"
    ],
    "Resource": "*"
  }
]

VPC: Take Action on a Resource

{ "Version": "2012-10-17",
 "Statement": [
  { "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteEgressOnlyInternetGateway",
      "ec2:DetachInternetGateway"
    ],
    "Resource": "*"
  }
]
IAM User: Manual Poll

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:ListGroupsForUser",
        "iam:ListAccountAliases",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListMFADevices",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:ListVirtualMFADevices"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM User: Take Action on a Resource

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys"
      ],
      "Resource": "*"
    }
  ]
}
```
IAM Role: Manual Poll

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "iam:ListRoles",
         "Resource": "*"
      }
   ]
}
```

Config: Manual Poll

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "config:DescribeDeliveryChannels",
         "Resource": "*"
      }
   ]
}
```

Polling of All Relevant Resources

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeImages",
            "ec2:DescribeAddresses",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeFlowLogs",
            "ec2:DescribeVolumes",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeInternetGateways",
         ]
      }
   ]
}
```
Actions on All Resources

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "iam:DeleteAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DetachInternetGateway"
      ],
      "Resource": "*"
    }
  ]
}
```
Deploying Lambda Artifacts on AWS

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lambda:GetFunction",
                "lambda:CreateFunction",
                "lambda:AddPermission",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:PassRole",
                "events:PutRule",
                "events:PutTargets",
                "events:DescribeRule",
                "logs:DescribeLogGroups",
                "logs:PutMetricFilter",
                "logs:CreateLogGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Complete Recommended Minimal JSON Permissions for AWS Plugin

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "config:DescribeDeliveryChannels",
                "ec2:DescribeImages",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceAttribute",
```
"ec2:DescribeRegions",
"ec2:DescribeFlowLogs",
"ec2:DescribeVolumes",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups",
"ec2:DescribeInternetGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeNetworkAcls",
"ec2:DescribeRouteTables",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:StartInstances",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:StopInstances",
"ec2:DeleteEgressOnlyInternetGateway",
"ec2:DetachInternetGateway",
"elasticloadbalancing:DescribeLoadBalancers",
"events:PutRule",
"events:PutTargets",
"events:DescribeRule",
"iam:ListGroupsForUser",
"iam:ListAccountAliases",
"iam:ListUsers",
"iam:ListGroup",
"iam:ListMFADevices",
"iam:GetUser",
"iam:GetGroup",
"iam:ListVirtualMFADevices",
"iam:ListRoles",
"iam:DeleteAccessKey",
"iam:UpdateAccountPasswordPolicy",
"iam:UpdateAccessKey",
"iam:ListAccessKeys",
"iam:GetRole",
"iam:CreateRole",
"iam:PassRole",
"lambda:GetFunction",
"lambda:CreateFunction",
"lambda:AddPermission",
"logs:FilterLogEvents",
"logs:DescribeLogGroups",
"logs:PutMetricFilter",
"logs:CreateLogGroup",
"logs:DescribeLogStreams",
"logs:GetLogEvents"
### Access AWS Credentials

**To access your AWS credentials:**

1. Go to [https://console.aws.amazon.com](https://console.aws.amazon.com) and log in using your username and password.

2. Select **Services**.


4. In the IAM Resources section, select the **Users** link. The Users page opens.

5. Each user has a unique Access Key ID. Select a user. The Users: [Name of User] page opens.

6. Select the **Security credentials** tab. The sign-in credentials display.

7. In the Access Keys section, the AWS Access key ID displays. Access Keys allow control of the credentials you will need to configure in the CounterACT AWS Module. Copy the **Access key ID** and locate the corresponding Secret Access Key.

### Enable AWS Config on AWS Account

AWS Config needs to be manually enabled on your AWS account, per region. For global entities, such as IAM, the AWS Config recording only occurs on a selected “home” region.

The following figure displays settings that record all resources in the region and monitor global resources such as IAM. You also need to configure an Amazon S3 bucket and an AWS Config role, however the AWS plugin only uses CloudWatch logs and does not rely on the S3 buckets for information.
Alternatively, you can select resources as needed. The AWS plugin uses information from the following resources.

**Configure the Plugin**

Configure the plugin to ensure that CounterACT can communicate with AWS API access points.

To begin configuration of the AWS plugin, you must meet the corresponding **Requirements** first. Removing a configured connection will stop endpoint discovery and property learning of virtual machines unique to the connection, but any actions will remain enabled.
Add an AWS Connection

This section describes how to add an AWS connection from CounterACT. Verify that you have access to your AWS credentials before adding a connection. The Access Key ID corresponds to your AWS EC2 account on the AWS online portal.

**To add an AWS connection:**

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options pane opens.

2. From the Options pane, select **AWS**. The AWS pane opens.

3. Select **Add**. The Add AWS Connection wizard opens. If you have not set up your AWS credentials, see **Add an AWS Connection**.
4. Enter values for the following parameters, which are used to connect to AWS and retrieve information about endpoints in the cloud.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Key ID</strong></td>
<td>Enter the credentials of the IAM user you want this connection to use when it connects to AWS. The Access Key ID and the Secret Access Key were given to you when you created a user profile in your AWS account. The username of the IAM user is not required.</td>
</tr>
<tr>
<td><strong>Secret Access Key</strong></td>
<td>Verify Secret Access Key by re-entering it.</td>
</tr>
<tr>
<td><strong>Verify Secret Access Key</strong></td>
<td>Confirm the accuracy of the Secret Access Key by re-entering it.</td>
</tr>
<tr>
<td><strong>Connecting CounterACT Device</strong></td>
<td>Indicates the CounterACT device that connects to AWS using these connection settings. The device specified in this field is the only CounterACT device that communicates with AWS. In the drop-down list, select an IP Address listed under the Appliances folder. Only one IAM user is allowed for a connecting device.</td>
</tr>
<tr>
<td><strong>Account Nickname</strong></td>
<td>Add an optional label or nickname to distinguish this connection from other AWS connections.</td>
</tr>
</tbody>
</table>

5. Select **Next**. The Proxy Server Definitions pane opens.
It is optional to enter proxy server information. If using a proxy server with Basic Authentication, you will need the proxy credentials (see AWS Requirements).

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Proxy Server</td>
<td>If your environment routes internet communications through proxy servers, select this box.</td>
</tr>
<tr>
<td>Proxy Server Host</td>
<td>Enter the host IP address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Select the port number of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Username</td>
<td>(Optional) For proxies using Basic Authentication, enter the proxy server’s username.</td>
</tr>
<tr>
<td>Proxy Server Password</td>
<td>(Optional) For proxies using Basic Authentication, enter the proxy server’s password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the proxy server’s password.</td>
</tr>
</tbody>
</table>

6. Select Next. The Verifying AWS account configuration screen opens and a list of available regions is retrieved for the connected account. The following successful results are for a user who has all Discovery-related permissions (AmazonEC2ReadOnlyAccess, IAMReadOnlyAccess, and AWSConfigUserAccess). Errors are displayed if the user does not have all the required permissions.
7. Select Close to close the Verifying AWS account configuration screen. The Regions pane opens.
8. To select the regions you want to query, do one of the following:
   - Check **Select Active** to automatically select all active AWS regions.
   - Check **Select All** to select all the regions in the list.
   - Select individual regions from the list.

9. Select **Next**. The **Verifying VPC configuration for CIDR subnet conflicts** screen opens.

10. Select **Close** to close the **Verifying VPC configuration for CIDR subnet conflicts** screen. The Advanced pane opens.

11. Set the communication controls between CounterACT and AWS.

<table>
<thead>
<tr>
<th><strong>Query Interval (seconds)</strong></th>
<th>Specify how frequently the plugin should query AWS for an EC2 full poll.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delta Poll of EC2 instances</strong></td>
<td>Enable Delta Polling of EC2 instances. This check box enables AWS Lambda functions and the CloudWatch monitoring service. See <a href="#">About Delta Polling</a>.</td>
</tr>
</tbody>
</table>
Delta Poll interval (seconds) | Specify the Delta Polling interval. Using this interval, the AWS plugin reaches out to CloudWatch log streams to get the most recent logs. See About Delta Polling.


13. If Delta Polling is enabled, the following confirmation screen appears.

14. Select OK to continue. When Delta Polling is enabled, AWS Lambda functions, and CloudWatch Event Rules are created for each of the selected AWS regions. See About Delta Polling.

15. In the AWS pane, select Apply and confirm the changes.

Allow 1-2 minutes for the changes to take effect.

About Delta Polling

The delta polling mechanism recognizes state changes to the EC2 instance, such as a change from the Running to the Stopped state. Many attributes (other than EC2 instance state) can also change.
Amazon exposes these attributes through AWS Config, which is a recording of any configuration changes on the AWS account. The AWS plugin leverages the functionality exposed by AWS Config to identify changes to EC2 properties, to IAM users, IAM groups, and IAM roles, and to VPC properties.

Delta polling works as follows:

1. AWS Config records changes to EC2/IAM/VPC and sends them to CloudWatch event rules.
2. The CloudWatch event rules receive the changes and forward them to the Lambda function.
3. The Lambda function logs the changes to the CloudWatch event logs.
4. The delta polling mechanism reads the CloudWatch logs at every delta polling interval.

Note the following:

- Changes to EC2 state information are reflected in CounterACT in approximately a minute. This delay is due to delta polling.
- Changes to EC2, VPC, and IAM configuration propagated through AWS Config are reflected in CounterACT in approximately 10 minutes. This delay is due to AWS Config.

**Verify That the Plugin Is Running**

After configuring the plugin, verify that it is running.

**To verify:**

1. Select **Tools>Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

**Test the AWS Connection**

Using the configured settings, CounterACT attempts to connect to AWS and retrieve sample data associated with the IAM user in the AWS regions specified in the connection. The test functionality also displays whether CloudWatch Event Rules have been configured to receive EC2 state change notifications and receive AWS Config notifications.

**To test the AWS connection:**

1. In the AWS pane, select an AWS connection and select **Test**. The Testing AWS Connection screen opens. The following successful results are for a user who has all Discovery-related permissions (AmazonEC2ReadOnlyAccess, IAMReadOnlyAccess, and AWSConfigUserAccess). Errors are displayed if the user does not have all the necessary permissions.
2. After viewing the results, select Close.

- It is recommended you test the AWS connection after the AWS plugin has been running for 1-2 minutes.

**Manually Deploy Delta Polling Artifacts**

Use Deploy to see if any specific region does not have Lambda functions, CloudWatch Event Rules, or CloudWatch Logs configured. The deploy mechanism deploys the CloudWatch Event Rule that is needed to consume events from AWS Config. Errors are displayed if the user does not have all the required permissions.

To manually deploy Delta Polling artifacts on an AWS account:

1. In the AWS pane, select an AWS connection and select Deploy.

2. The Deploying CloudWatch rules and Lambda functions on selected entries screen opens. The following successful results are for a user who has all the required permissions.
3. After viewing the results, select Close.

Manually Poll EC2 Instances

Use Poll when you do not want to wait for the scheduled poll. The full poll collects information from AWS, such as EC2 instance-related data. The poll results depend on the access permissions of the user. If the user does not have read permissions to EC2 or IAM, an error displays.

To manually poll all EC2 instances for an account:

1. In the AWS pane, select an AWS connection and select Poll.

2. The Performing full poll of all AWS entities on selected regions screen opens. The following successful results are for a user who has both AmazonEC2ReadOnlyAccess and IAMReadOnlyAccess permissions. There are no errors even though this user does not have AWSConfigUserAccess permissions. However in this case, no AWS Config-related information displays.
3. After viewing the results, select **Close**.

4. The following failed poll is for a user who has only `AmazonEC2ReadOnlyAccess` permissions.

5. After viewing the results, select **Close**.
6. The following failed poll is for a user who has only IAMReadOnlyAccess permissions.

![Performing full poll of all AWS entities on selected regions](image)

7. After viewing the results, select **Close**.

**Edit the AWS Connection**

Use **Edit** when you want to edit a connection.

**To edit the AWS connection:**

1. In the AWS pane, select an AWS connection and select **Edit**. The Edit AWS Connection dialog box opens with four tabs: General, Proxy Server Definition, Regions, and Advanced.
2. Make your edits and select **OK** or select another tab, make your edits and select **OK**.

**Remove the AWS Connection**

Use **Remove** when you want to remove a connection. Any actions that may have been launched will remain active and will not be undone.

To **remove the AWS connection**:

1. In the AWS pane, select an AWS connection and select **Remove**. The Remove AWS dialog box opens.

2. To remove the connection, select **Ok**.
Configure AWS Policy Templates

The AWS plugin provides additional endpoint properties and actions that are useful for management of AWS virtual devices. Use these properties and actions to construct customized policies for detecting, managing, and remediating endpoints based on the AWS integration.

Before applying the templates, it is recommended that you have a basic understanding of CounterACT policies. For more information about creating custom policies, see the CounterACT Templates and Policy Management chapters in the CounterACT Administration Guide.

Access AWS Policy Templates

Use the templates in this section for AWS policies.

To access AWS policy templates:

1. Log in to the CounterACT Console and select Policy.


4. Expand the folders to see the policy templates for EC2 Instances, IAM Users and Roles, VPCs, and OTHER, as well as the policy template for AWS Asset Classification.

5. For a generic policy template procedure, see Policy Template Procedure. For lists of all the policy templates, see AWS Policy Templates.

Policy Template Procedure

Use this policy template procedure to create an AWS policy.

To create an AWS policy using a template:

1. Select an AWS policy.

2. Select Next. The Name dialog box opens.
3. Enter the name of the new policy. Optionally, add a description. Select **Next**. The Scope pane opens.

4. AWS policy templates for non-EC2 instances do not need an IP segment to be explicitly selected. Hence, **Hosts without a known IP address** has been preselected in the Scope Pane. For EC2 instances, select **Add**. Otherwise, go to Step 8.
5. Use The IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

6. In the IP Address Range dialog box, select **OK**.

7. To add other IP address ranges, select **Add** in the Scope pane. To delete, select an entry for **Hosts inspected by the policy** and select **Remove**.

8. In the Scope pane, select **Next**. The Sub-Rules pane opens.
9. Select **Add**. The Policies --> Sub-Rule: New rule dialog box opens as well as the Policies --> Sub-Rule dialog box.

10. Enter the name of the new rule. Optionally, add a description.
11. Select **OK**.
12. To edit the policy name or condition, select **Edit** under Name.

13. To add a condition, select **Add** under Condition. See [Detecting Cloud Endpoints – Host Properties](#).

14. To add an action, select **Add** under Actions. See [Run Policy Actions](#).

15. Select **OK** in the Policies -- > Sub-Rule dialog box.

16. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

17. In the Policy Manager, select **Apply**.
AWS Policy Templates

The AWS policy templates are organized in folders as follows:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 Instances</td>
<td>Use the templates in this folder to create policies on EC2 instances.</td>
</tr>
<tr>
<td></td>
<td>There is a sub-folder called EC2 Event. Use the templates in this folder to create policies on EC2 instance events.</td>
</tr>
<tr>
<td>IAM Users and Roles</td>
<td>Use the templates in this folder to create policies on IAM users and roles.</td>
</tr>
<tr>
<td></td>
<td>There is a sub-folder called IAM Event. Use the templates in this folder to create policies on IAM User and role events.</td>
</tr>
<tr>
<td>VPCs</td>
<td>Use the templates in this folder to create policies on VPCs.</td>
</tr>
<tr>
<td></td>
<td>There is a sub-folder called VPC Event. Use the templates in this folder to create policies on VPC events.</td>
</tr>
<tr>
<td>OTHER</td>
<td>Use the templates in this folder to create policies on other AWS resources.</td>
</tr>
<tr>
<td>AWS Asset Classification</td>
<td>Use this template to classify all AWS resources.</td>
</tr>
</tbody>
</table>

EC2 Instances Policy Templates

The EC2 Instances policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 Event &gt; AWS EC2 Instance State</td>
<td>Identify EC2 instances with a specific state.</td>
</tr>
<tr>
<td>AWS EC2 Encryption Compliance</td>
<td>Identify if EC2 instances are encryption-compliant.</td>
</tr>
<tr>
<td>AWS EC2 Instance by Region</td>
<td>Classify EC2 instances by region.</td>
</tr>
<tr>
<td>AWS EC2 Instance by Type/Size</td>
<td>Classify EC2 instances by type/size.</td>
</tr>
<tr>
<td>AWS EC2 Instance Public IP</td>
<td>Identify EC2 instances with a public IP address.</td>
</tr>
<tr>
<td>AWS EC2 Instance Termination Protection</td>
<td>Identify EC2 instances that have Termination Protection enabled.</td>
</tr>
</tbody>
</table>

IAM Users and Roles Policy Templates

The IAM Users and Roles policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Event &gt; AWS IAM Role Created</td>
<td>Identify when an IAM role is created.</td>
</tr>
<tr>
<td>IAM Event &gt; AWS IAM User Created</td>
<td>Identify when an IAM user is created.</td>
</tr>
<tr>
<td>AWS IAM Root Password</td>
<td>Identify if the root account is compliant with the password policy.</td>
</tr>
</tbody>
</table>
AWS IAM User Console Access
Identify if the IAM user has console access enabled.

AWS IAM User Console Password
Identify if the IAM user’s console access is compliant.

AWS IAM User MFA
Identify if the IAM user is MFA-compliant.

VPCs Policy Templates
The VPCs policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC Event &gt; AWS VPC State</td>
<td>Identify when a VPC is created or deleted.</td>
</tr>
<tr>
<td>AWS VPC ELB</td>
<td>Identify VPCs with ELB configured.</td>
</tr>
<tr>
<td>AWS VPC Flowlog</td>
<td>Identify VPCs with Flowlogs configured.</td>
</tr>
<tr>
<td>AWS VPC Internet Gateway Compliance</td>
<td>Identify if VPCs are compliant with respect to Internet Gateways.</td>
</tr>
<tr>
<td>AWS VPC Peering Status</td>
<td>Identify VPCs with peering connections.</td>
</tr>
</tbody>
</table>

OTHER Policy Templates
The OTHER policy template is as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Config Compliance</td>
<td>Identify if your account/region is AWS Config-compliant.</td>
</tr>
</tbody>
</table>

Update the AMI Whitelist
The AMI Whitelist lists the “good” Amazon Machine Images (AMIs).

**To update the AMI whitelist:**

1. Log in to the CounterACT Console and select **Options** from the Tools menu. The Options pane opens.

2. In the left pane, select **Lists**. In the right pane, all the AMIs are listed.
3. Select an item and select **Edit**. Alternately, double-click the item. The Edit List dialog box opens.

4. To add additional values to the list, select **Add**. The Add Value dialog box opens.

5. Paste the AMI Name from the AWS online portal into the field, for example, ami-b70554c8, and select **OK**.
6. Copy/paste additional AMIs from the AWS online portal into the Edit List dialog box (if applicable).

7. When finished, select **OK** in the Edit List dialog box.

8. Select **Apply** in the Lists pane.

---

### Detecting Cloud Endpoints – Host Properties

There are many AWS-specific host properties available. These properties are displayed in the Condition pane accessible through the policy templates. In the CounterACT Console, some properties are also visible in the profile section within the Home tab.

Host properties are organized into the following groups:

- **AWS Properties**
- **AWS EC2 Properties**
- **AWS IAM Role Properties**
- **AWS IAM User Properties**
- **AWS Service Properties**
- **AWS VPC Properties**

For more information about setting conditions, see the *CounterACT Administration Guide*.

### AWS Properties

The AWS properties are common properties, such as Account Name, that are added to EC2, IAM, or VPC hosts.

**To access the AWS properties:**

1. When configuring policies, select **Add** under Condition in the Sub-Rule dialog box.

2. Expand the AWS folder in Properties.
The properties are as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AWS Account Name</strong></td>
<td>Indicates the nickname of the AWS account to which this host corresponds, as internally configured in the CounterACT Console.</td>
</tr>
<tr>
<td><strong>AWS Account Region</strong></td>
<td>Indicates the region of the AWS account.</td>
</tr>
<tr>
<td><strong>AWS Resource State</strong></td>
<td>Indicates the most recently reported state of the AWS Resource.</td>
</tr>
<tr>
<td><strong>AWS Resource Tag</strong></td>
<td>Indicates an internal tag to differentiate between EC2/IAM and VPC hosts.</td>
</tr>
</tbody>
</table>

**AWS EC2 Properties**

To access the AWS EC2 properties:

1. When configuring policies, select Add under Condition in the Sub-Rule dialog box.
2. Expand the AWS EC2 folder in Properties.
The properties are as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EC2 Attached Block Devices</strong></td>
<td>Indicates the Elastic Block Storage (EBS) volumes attached to this EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 AMI Launch Index</strong></td>
<td>Indicates the order in which the EC2 instance was launched. The first or only instance has an index value of 0.</td>
</tr>
<tr>
<td><strong>EC2 Dedicated Tenancy</strong></td>
<td>Indicates that the instance runs on single-tenant, dedicated hardware.</td>
</tr>
<tr>
<td><strong>EC2 Elastic Network Interfaces</strong></td>
<td>Indicates the Elastic Network Interfaces of the EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 IAM Role</strong></td>
<td>Indicates the Identity and Access Management (IAM) role associated with this EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Instance ID</strong></td>
<td>Indicates the EC2 instance ID of the endpoint.</td>
</tr>
<tr>
<td><strong>EC2 Internet Gateway Information</strong></td>
<td>Provides information about the Internet gateways on this EC2 instance's VPC.</td>
</tr>
<tr>
<td><strong>EC2 Kernel ID</strong></td>
<td>Indicates the operating system kernel associated with the AMI.</td>
</tr>
<tr>
<td><strong>EC2 Key Pair Name</strong></td>
<td>Indicates the key pair required for logging in to the instance securely.</td>
</tr>
<tr>
<td><strong>EC2 Launch Details</strong></td>
<td>Indicates the launch details of the EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Lifecycle</strong></td>
<td>Indicates whether this is a Normal or Spot EC2 instance. A Normal instance is usually launched and terminated at a user’s request. A Spot Instance is launched when the bid price is higher than the Spot Price. If the Spot Price goes over the bid price, it may be terminated.</td>
</tr>
<tr>
<td><strong>EC2 Location</strong></td>
<td>Provides location information of the AWS EC2 endpoint.</td>
</tr>
<tr>
<td><strong>EC2 Last State Transition Reason</strong></td>
<td>Indicates the reason for the last change of EC2 instance state. For example, if the last instance state was Terminated, the reason might be: User initiated shutdown.</td>
</tr>
<tr>
<td><strong>EC2 Instance Name</strong></td>
<td>Indicates the EC2 instance name of the endpoint.</td>
</tr>
<tr>
<td><strong>EC2 AMI Owner</strong></td>
<td>Indicates the AWS account number belonging to the owner of the Amazon Machine Image (AMI) used for this EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Placement Group</strong></td>
<td>Indicates the cluster group to which this instance belongs, if it is a cluster instance.</td>
</tr>
<tr>
<td><strong>EC2 Platform</strong></td>
<td>Indicates the platform of the EC2 instance, such as Windows or empty.</td>
</tr>
<tr>
<td><strong>EC2 Public DNS</strong></td>
<td>Indicates the public hostname of the EC2 instance, which resolves to the public IP address or Elastic IP address of the instance.</td>
</tr>
<tr>
<td><strong>EC2 Public IP</strong></td>
<td>Indicates the public IP address of the EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 RAM disk ID</strong></td>
<td>Indicates the RAM disk associated with the image, if a specific one was selected.</td>
</tr>
<tr>
<td><strong>EC2 Secondary Private IP</strong></td>
<td>Indicates the secondary private IP addresses assigned to a network interface attached to this EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Security Group</strong></td>
<td>Indicates the security groups to which the EC2 instance belongs.</td>
</tr>
<tr>
<td><strong>EC2 State</strong></td>
<td>Indicates the most recent power state of the EC2 instance. This value may be influenced by the Query Interval configured for the CounterACT connection to AWS.</td>
</tr>
<tr>
<td><strong>EC2 Subnet</strong></td>
<td>Indicates the AWS subnet into which the EC2 instance was launched.</td>
</tr>
<tr>
<td><strong>EC2 Tags</strong></td>
<td>Indicates the tags given to the EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Termination Protection</strong></td>
<td>Indicates whether termination protection is enabled. When protection is enabled, this EC2 instance cannot be terminated using the console, API, or CLI.</td>
</tr>
<tr>
<td><strong>EC2 Instance Type</strong></td>
<td>Indicates the type of EC2 instance by CPU capacity, memory, and storage. For example, m1.small, c1.xlarge.</td>
</tr>
<tr>
<td><strong>EC2’s Virtual Private Cloud</strong></td>
<td>Indicates the Virtual Private Cloud (VPC) into which the EC2 instance was launched.</td>
</tr>
</tbody>
</table>
EC2 CloudWatch Monitoring
Indicates the level of CloudWatch monitoring (basic or detailed) that is enabled for this instance.

AWS IAM Role Properties
This section describes the AWS IAM Role properties.

To access the AWS IAM Role properties:
1. When configuring policies, select Add under Condition in the Sub-Rule dialog box.
2. Expand the AWS IAM Role folder in Properties.

The property is as follows:

| AWS IAM Role | Indicates the friendly name that identifies the AWS role. |

AWS IAM User Properties
This section describes the AWS IAM User properties.

To access the AWS IAM User properties:
1. When configuring policies, select Add under Condition in the Sub-Rule dialog box.
2. Expand the AWS IAM User folder in Properties.
The properties are as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM User Access Keys</td>
<td>Provides information about the access keys that are associated with the user.</td>
</tr>
<tr>
<td>IAM Console Access Enabled</td>
<td>Indicates if Console access is enabled for the user.</td>
</tr>
<tr>
<td>IAM MFA Devices</td>
<td>Provides information about the MFA devices.</td>
</tr>
<tr>
<td>IAM MFA Enabled</td>
<td>Indicates if Multi-Factor Authentication (MFA) is enabled for the user.</td>
</tr>
<tr>
<td>IAM Password Policy</td>
<td>Provides information about the account password policy.</td>
</tr>
<tr>
<td>IAM User ARN</td>
<td>Indicates the Amazon Resource Name (ARN) that identifies the user.</td>
</tr>
<tr>
<td>IAM User Creation Date</td>
<td>Indicates the date and time the user was created.</td>
</tr>
<tr>
<td>IAM Groups</td>
<td>Provides information about the groups to which the user belongs.</td>
</tr>
<tr>
<td>IAM User ID</td>
<td>Indicates the stable and unique string that identifies the user.</td>
</tr>
<tr>
<td>IAM User Name</td>
<td>Indicates the friendly name that identifies the user.</td>
</tr>
<tr>
<td>IAM User Password Last Used</td>
<td>Indicates the date and time the password was last used to sign in to an AWS website.</td>
</tr>
<tr>
<td>IAM User Path</td>
<td>Indicates the path to the user.</td>
</tr>
</tbody>
</table>
AWS Service Properties

To access the AWS Service properties:

1. When configuring policies, select Add under Condition in the Sub-Rule dialog box.
2. Expand the AWS Service folder in Properties.

The property is as follows:

<table>
<thead>
<tr>
<th>AWS Config</th>
<th>Indicates if AWS Config is enabled on this account/region.</th>
</tr>
</thead>
</table>

AWS VPC Properties

To access the AWS VPC properties:

1. When configuring policies, select Add under Condition in the Sub-Rule dialog box.
2. Expand the AWS VPC folder in Properties.
The properties are as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Peering Connection</strong></td>
<td>Provides information about the VPC peering connection.</td>
</tr>
<tr>
<td><strong>VPC Flowlog Enabled</strong></td>
<td>Indicates if VPC flowlog is enabled.</td>
</tr>
<tr>
<td><strong>VPC ID</strong></td>
<td>Indicates the stable and unique string that identifies the VPC.</td>
</tr>
<tr>
<td><strong>VPC Internet Gateway Information</strong></td>
<td>Provides information about Internet gateways on this VPC.</td>
</tr>
<tr>
<td><strong>VPC Load Balancer Information</strong></td>
<td>Provides information about load balancers on this VPC.</td>
</tr>
<tr>
<td><strong>VPC Name</strong></td>
<td>Indicates the friendly name that identifies the VPC.</td>
</tr>
<tr>
<td><strong>VPC Network ACL</strong></td>
<td>Indicates the VPC network ACL.</td>
</tr>
<tr>
<td><strong>VPC Route Tables</strong></td>
<td>Provides information about route tables on this VPC.</td>
</tr>
<tr>
<td><strong>VPC Subnet Information</strong></td>
<td>Provides information about subnets on this VPC.</td>
</tr>
</tbody>
</table>

**Managing AWS Cloud Endpoints**

Once the AWS plugin has been configured, you can view and manage the virtual endpoints from the Asset Inventory view in the CounterACT Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instance properties. The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
• View virtual machine endpoints that were detected with specific attributes
• Incorporate inventory detections into policies

See Working with Inventory Detections in the CounterACT Administration Guide or the CounterACT Help for information about how to work with the CounterACT Asset Inventory.

Access AWS IAM Role Inventory

Use the AWS IAM Role inventory to view IAM role-related summary and detailed information.

To access the AWS IAM Role inventory:

1. Log in to the CounterACT Console and select Asset Inventory.

2. In the Views pane, select AWS IAM Role.

3. The AWS IAM Role information displays. To view details, select a specific AWS IAM Role.
Access AWS EC2 Inventory

Use the AWS EC2 inventory to view EC2-related summary and detailed information.

To access the AWS EC2 inventory:

1. Log in to the CounterACT Console and select Asset Inventory.

2. In the Views pane, expand the AWS EC2 folder.
3. Select an AWS EC2 item, for example, EC2 Launch Details, to view the real-time inventory information. For details, select a specific AWS EC2.

4. To view more inventory information, select another AWS EC2 item, for example, EC2 Instance Type, EC2 Location, EC2 Security Group, EC2 State, or EC2’s Virtual Private Cloud.
Access AWS IAM User Inventory

Use the AWS IAM User inventory to view IAM user-related summary and detailed information.

To access the AWS IAM User inventory:

1. Log in to the CounterACT Console and select **Asset Inventory**.
2. In the Views pane, expand the **AWS IAM User** folder.
3. Select an AWS IAM User item, for example, IAM User Name, to view the real-time inventory information. For details, select a specific IAM User Name.
4. To view more inventory information, select another AWS IAM item, for example, IAM Groups.
Access AWS VPC Inventory

Use the AWS VPC inventory to view VPC-related summary and detailed information.

**To access the AWS VPC inventory:**

1. Log in to the CounterACT Console and select **Asset Inventory**.
2. In the Views pane, expand the **AWS VPC** folder.

3. Select an AWS VPC item, for example, VPC Name, to view the real-time inventory information. For details, select a specific VPC Name.

4. To view more inventory information, select another AWS VPC item, for example, VPC Internet Gateway Information, VPC Load Balancer Information, or VPC Subnet Information.
Run Policy Actions

Policy actions are organized into the following groups:

- Manually Run AWS Actions on EC2 Instance
- Manually Run AWS IAM Actions
- Manually Run AWS VPC Actions

Manually Run AWS Actions on EC2 Instance

Use the actions in this section for visibility and control of AWS. While AWS EC2 actions can be launched as part of a policy, you can also manually run an action.

To manually run an AWS EC2 action:

1. Log in to the CounterACT Console, select Home, and select All Hosts.

2. In the All Hosts pane, select a host entry.

3. Right-click an endpoint, select AWS EC2, and select an action.
4. Select the following links for information on the AWS EC2 actions.
   - Apply EC2 Security Groups Action
   - Disable EC2 Termination Protection Action
   - Enable EC2 Termination Protection Action
   - Start EC2 Instance Action
   - Stop EC2 Instance Action

**Apply EC2 Security Groups Action**

Use this action to set security groups for an AWS endpoint.

A security group acts as a firewall that controls the traffic for one or more EC2 instances. Each security group has a set of rules that you define and these rules specify the kind of connections, such as the IP addresses, ports, or protocols that are allowed. These rules are defined in the AWS console.

By applying a security group action to a cloud instance, that instance is allowed to send/receive traffic based on the security group's rules.

**To run the Apply EC2 Security Groups action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Apply EC2 Security Groups**. The Specify Apply EC2 Security Groups parameters dialog box opens to the Parameters tab.
3. In the Append or overwrite field, select one of the following:
   - **Append this list to the current Security Group list**, which adds the selected security groups to the current Security Group list.
   - **Overwrite the current Security Group list with this list**, which replaces the current Security Group list with the list you have selected. This option is useful for isolating a non-compliant endpoint by applying it only with restrictive security groups.

4. When **Specify Security Groups** is selected, check one or more security groups in the table. To select all security groups, select **Select All**. To clear all security groups, select **Clear All**. To filter the security groups, enter text in the **Search** field to match security group names. Or, to select all security groups, check **Select all Security Groups**.

5. Select **OK** or select the **Schedule** tab to schedule the action. The Specify Apply EC2 Security Groups parameters dialog box opens.
6. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
- **Customize action start time**, which opens the Action Scheduler dialog box.
7. Set parameters and select OK.
8. In the Specify Apply EC2 Security Groups parameters dialog box, select OK.

**Disable EC2 Termination Protection Action**

Use this action to remove (disable) termination protection from an EC2 instance.

If termination protection is disabled, it is possible to terminate EC2 instances through the AWS Console, API, or CLI.

Enabling termination protection prevents accidental termination of EC2 instances.

To run the Disable EC2 Termination Protection action:

1. Log in to the CounterACT Console, select Home, and select All Hosts.
2. In the All Hosts pane, right-click an endpoint, select AWS EC2, and select Disable EC2 Termination Protection. The Specify Disable EC2 Termination Protection parameters dialog box opens.

3. For the Action Schedule, select one of the following:
   - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
   - **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.

5. In the Specify Disable EC2 Termination Protection parameters dialog box, select **OK**.

**Enable EC2 Termination Protection Action**

Use this action to apply (enable) termination protection for an EC2 instance. Enabling termination protection prevents accidental termination of EC2 instances.

If termination protection is disabled, stopping EC2 instances may also terminate them. You can start or stop the selected EC2 instance through the AWS Console, API, or CLI.

If termination protection is enabled, stopping EC2 instances will not terminate them.

**To run the Enable EC2 Termination Protection action:**

1. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Enable EC2 Termination Protection**. The Specify Enable EC2 Termination Protection parameters dialog box opens.
2. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
- **Customize action start time**, which opens the Action Scheduler dialog box.
3. Set parameters and select **OK**.

4. In the Specify Enable EC2 Termination Protection parameters dialog box, select **OK**.

**Start EC2 Instance Action**

Use this action to start an EC2 instance that is not in the running state.

**To run the Start EC2 Instance action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Start EC2 Instance**. The Specify Start EC2 Instance parameters dialog box opens.
3. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.

- **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.

5. In the Specify Start EC2 Instance parameters dialog box, select **OK**.

**Stop EC2 Instance Action**

Use this action to stop an EC2 instance that is in the running state.

**To run the Stop EC2 Instance action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Stop EC2 Instance**. The Specify Stop EC2 Instance parameters dialog box opens.
3. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.

- **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.

5. In the Specify Stop EC2 Instance parameters dialog box, select **OK**.

**Manually Run AWS IAM Actions**

Use the actions in this section for visibility and control of AWS IAM users. Control actions such as Activate/Deactivate User Access Key allow remediation upon non-compliance, allowing automated polices.

While AWS IAM actions can be launched as part of a policy, you can also manually run an action.
To manually run an AWS IAM action:

1. Log in to the CounterACT Console, select Home, and select All Hosts.

2. In the All Hosts pane, select a host entry.

3. Right-click an AWS endpoint, select AWS IAM, and select an action.
4. Select the following links for information on AWS IAM actions:
   - Activate User Access Key Action
   - Deactivate User Access Key Action
   - Delete User Access Key Action
   - Enforce Password Policy Action

**Activate User Access Key Action**

Use this action to activate an access key for the AWS IAM user.

**To run the Activate User Access Key action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Activate User Access Key**. The Specify Activate User Access Key parameters dialog box opens.

3. For the Action Schedule, select one of the following:
   - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
   - **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select OK.

5. In the Specify Activate User Access Key parameters dialog box, select OK.

**Deactivate User Access Key Action**

Use this action to deactivate an access key for the AWS IAM user.

**To run the Deactivate User Access Key action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Deactivate User Access Key**. The Specify Deactivate User Access Key parameters dialog box opens.
3. For the Action Schedule, select one of the following:
   - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
   - **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.

5. In the Specify Deactivate User Access Key parameters dialog box, select **OK**.

**Delete User Access Key Action**

Use this action to permanently delete an access key for the AWS IAM user.

To run the **Delete User Access Key** action:

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Delete User Access Key**. The Specify Delete User Access Key parameters dialog box opens.
3. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.

- **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select OK.

5. In the Specify Delete User Access Key parameters dialog box, select OK.

**Enforce Password Policy Action**

Use this action to enforce the password policy for AWS IAM users with no password policy set.

**To run the Enforce Password Policy action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Enforce Password Policy**. The Specify Enforce Password Policy parameters dialog box opens.
3. Set the password policy parameters.

| Allow Users to Change Password | Specify if users can change their own password or not. |
| Expire Passwords               | Specify if passwords will expire or not.               |
| Hard Expiry                    | Specify if passwords have a hard expiry or not.       |
| Max Password Age               | Specify the value for maximum password age. The password expiration period must be a whole number between 1 and 1095 days, inclusive. |
| Minimum Password Length        | Specify the value for minimum password length. The minimum password length must be a whole number greater than or equal to 6. |
| Password Reuse Prevention      | Specify the value for password reuse prevention. The number of passwords to remember must be between 1 and 24, inclusive. |
| Require Lowercase Characters   | Specify if the password must contain lowercase characters or not. |
| Require Numbers                | Specify if the password must contain numbers or not.  |
| Require Symbols                | Specify if the password must contain symbols or not.  |
| Require Uppercase Characters   | Specify if the password must contain uppercase characters or not. |
4. Select the **Schedule** tab.

4. Select the **Schedule** tab.

5. For the Action Schedule, select one of the following:
   - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
   - **Customize action start time**, which opens the Action Scheduler dialog box.
6. Set parameters and select OK.
7. In the Specify Enforce Password Policy parameters dialog box, select OK.

**Manually Run AWS VPC Actions**

Use the actions in this section for visibility and control of AWS VPCs. While AWS VPC actions can be launched as part of a policy, you can also manually run an action.

**To manually run an AWS VPC action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, select a host entry.

3. Right-click an AWS endpoint, select **AWS VPC**, and select an action.
4. Select the following link for information on AWS VPC actions:
   
   - **Detach Internet Gateway(s) Action**

**Detach Internet Gateway(s) Action**

Use this action to detach (terminate) the Internet gateway or egress-only Internet gateway from the AWS VPC.

**To run the Detach Internet Gateway(s) action:**

1. Log in to the CounterACT Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an AWS endpoint, select **AWS VPC**, and select **Detach Internet Gateway(s)**. The Specify Detach Internet Gateway(s) parameters dialog box opens.
3. For the Action Schedule, select one of the following:

- **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.
- **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.
5. In the Specify Detach Internet Gateway(s) parameters dialog box, select **OK**.

### Best Practices for Working with the AWS Plugin

The following are some helpful guidelines to follow when using the AWS plugin.

1. **Create an AWS user account** – Ask your AWS management personnel to create a new AWS user account with programmatic access for you. Programmatic access will create an access key ID and secret access key that is required when configuring the AWS plugin. The recommended number of AWS accounts for a single appliance is five.

2. **Level of Access** – The AWS user used by CounterACT should have full access across a range of permissions. Refer to [Specifying Permissions Using Standard AWS Policies](#).

3. **AWS Regions** – If you want complete visibility across all regions, while performing sync during configuration, choose all the regions available. For a restrictive view, pick specific regions only.
4. **Set Communications with AWS (Polling)** – When configuring the AWS plugin, it is recommended to use the default setting for *Query Interval*. Depending on the amount of data, the polling of EC2 instances can take 30 minutes for 20,000 instances.

5. **CounterACT Active Discovery** – If you do not want CounterACT to perform Active Discovery such as NMAP, HPS Inspection, or WMI on EC2 instances, make sure your EC2 instances are not reachable from CounterACT or their IP segment is not included in any base classification policy.

**Hybrid Cloud Module Information**

The Amazon Web Services plugin is installed with the CounterACT Hybrid Cloud Module.

The ForeScout CounterACT® Hybrid Cloud Module provides See, Control and Orchestrate functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

The Hybrid Cloud Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release. Plugins listed above are installed and rolled back with the Hybrid Cloud Module.

Refer to the *ForeScout CounterACT Hybrid Cloud Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

**Additional CounterACT Documentation**

For information about other CounterACT features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

**Documentation Downloads**

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)
Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

2. Select Downloads or Documentation.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide
Select **CounterACT Help** from the **Help** menu.

**Plugin Help Files**

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.

2. Select the plugin and then select **Help**.

**Documentation Portal**

Select **Documentation Portal** from the **Help** menu.

**Identifying Your Licensing Mode in the Console**

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.