ForeScout® Amazon® Web Services (AWS) Plugin
Configuration Guide

Version 1.1.1 and above
Table of Contents

Amazon Web Services Plugin Overview ........................................................ 4
  Use Cases ................................................................................................... 5
    Providing Consolidated Visibility ............................................................ 5
    Dynamic Segmentation of Instances ......................................................... 5
    Security Management of EC2 Instances .................................................. 5
    Detect and Prevent Unauthorized Access to and from EC2 Instances .......... 5
  How It Works ............................................................................................... 5

What to Do ................................................................................................... 6
  Additional Amazon Web Services Documentation ...................................... 6

Requirements ............................................................................................... 6
  CounterACT Software Requirements ......................................................... 7
  AWS Requirements ..................................................................................... 7
  Networking Requirements .......................................................................... 8

Define AWS Users ...................................................................................... 8

Install the Plugin .......................................................................................... 9

Configure the Plugin .................................................................................... 9
  Add an AWS Connection .......................................................................... 9
  Test the AWS Connection ....................................................................... 13

Configure AWS Policy Templates ................................................................ 14
  AWS EC2 AMI Classification Template .................................................... 14
  Updating the AMI Whitelist ...................................................................... 17
  AWS EC2 External Instance Classification Template .................................. 19

Detecting Cloud Endpoints – Host Properties .......................................... 21
  AWS CloudWatch Flow Logs .................................................................. 21
  AWS EC2 ............................................................................................... 24

Managing AWS Cloud Endpoints .............................................................. 26
  AWS Admission Events .......................................................................... 27
  Manually Run AWS Actions on any EC2 Instance .................................... 27
    EC2 Security Group Action .................................................................... 28
    Disable EC2 Termination Protection Action .......................................... 29
    Enable EC2 Termination Protection Action ............................................ 31
    Start an EC2 Instance .......................................................................... 32
    Stop an EC2 Instance .......................................................................... 33

Best Practices for Working with the AWS Plugin ...................................... 35
**Additional CounterACT Documentation** ........................................ 35
  - Documentation Portal ................................................................. 35
  - Customer Support Portal ............................................................. 36
  - CounterACT Console Online Help Tools ....................................... 36
Amazon Web Services Plugin Overview

CounterACT® integrates with Amazon® Web Services (AWS), bringing the detailed visibility, control and compliance capabilities of CounterACT to instances in the public cloud. The AWS Plugin connects to Amazon’s public cloud environment to retrieve information on Elastic Compute Cloud (EC2) instances. The instances follow the same rules as any other endpoint discovered by CounterACT where one can define policies and actions on those endpoints.

CounterACT AWS Plugin enables:

- Visibility of endpoints in Amazon’s public cloud
- Creating and applying CounterACT policies
- Maintaining security of cloud endpoints
- Enforcing compliance on endpoints

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

This plugin lets you integrate CounterACT with AWS so that you can:

- Have full visibility of your AWS instances and their properties. Since it is often much easier to start and stop instances in a public cloud environment, it’s important to have a good understanding of what resources are being used in the cloud. Regular checks provide valuable information on how AWS cloud resources are being utilized. See Manually Run AWS Actions on any EC2 Instance for details.

- Review of data collected from AWS Flow Logs to gain insightful information on communications between instances. This information can be used to detect and prevent unauthorized access to an instance and determine if action needs to be taken. Flow Logs can also be used to discover short-lived instances that may have existed between the polling of AWS. See AWS CloudWatch Flow Logs for details.

- Discover cloud-based endpoints early, thus allowing identification and compliance checking prior to being given full network access. A non-compliant endpoint may be stopped, assigned to a quarantined security group, and the EC2 user may be notified. If automated remediation fails, the endpoint is isolated and stopped to prevent further damage. See EC2 Security Group Action for details.

- Use the CounterACT Inventory to review the distribution of endpoints in the cloud and mitigate as required. For example, endpoints with out-of-date Amazon Machine Images (AMI) are quickly identified for remediation. See Manually Run AWS Actions on any EC2 Instance for details.

- 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 where all compliant and critical EC2 assets have termination protection enabled. See Disable EC2 Termination Protection Action, Enable EC2 Termination Protection Action for details.
Use Cases

This section describes 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 both campus endpoints and AWS EC2 instances potentially on the same CounterACT Device.

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, production, etc. 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 by using your own well-defined security groups, thus making that security group compliant.

Detect and Prevent Unauthorized Access to and from EC2 Instances

This plugin integrates with AWS CloudWatch Flow Logs service to provide deeper visibility of traffic flows for an EC2 instance. It captures incoming and outgoing flows for an instance and records information such as source IP, destination IP, port number, etc., and reports if the flow was accepted or denied.

This information can be used to detect and even prevent any unauthorized access to an EC2 instance. For example, if you find an EC2 instance sending requests or data to an unauthorized machine, that instance can easily be quarantined by replacing its current security groups with a more restrictive security groups.

The AWS CloudWatch Flow Logs can also identify misconfigurations of an EC2 instance. For example, if a database instance is communicating on port 80 (typically used for web traffic), it can be flagged as non-compliant and can be quarantined by applying a security group action isolating the endpoint and preventing further usage of that port.

How It Works

This plugin uses well-defined APIs from AWS to provide visibility of AWS EC2 instances. Once the configuration is complete using AWS Identity and Access Management (IAM) credentials, CounterACT starts communicating with one or more AWS accounts and retrieves information on EC2 instances running in AWS under that
account. Many instance-related properties are collected as CounterACT host properties and cloud instances are displayed as endpoints in CounterACT. The queries are invoked based on configured time intervals.

The AWS plugin also pulls CloudWatch Flow Logs information if it is enabled for that AWS account. This information is shown when using the CounterACT session-as-a-server and session-as-a-client properties in policies.

See 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. Install the Plugin
4. Configure the Plugin
5. Use the in-depth information reported by the plugin to manage virtual devices:
   - Configure AWS Policy Templates
   - Managing AWS Cloud Endpoints
   - Manually Run AWS Actions on any EC2 Instance

**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. Installation, configuration and general guides relating to AWS can be found at:

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

**Requirements**

This section describes system requirements, including:

- CounterACT Software Requirements
- AWS Requirements
- Networking Requirements
CounterACT Software Requirements
This plugin requires the following CounterACT release and other CounterACT components.

- CounterACT version 7.0.0
- Service Pack 2.3.2 or above

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. See Define AWS Users.
- If you are using a proxy server with Basic Authentication, you will need that proxy’s credentials.
- The plugin requires the following AWS services and the user must have the related permissions:
  - **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. 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)
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. The AWS plugin uses this service to gather flow log data.

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

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

Because the plugin detects and manages EC2 instances, the AWS user used by CounterACT should have either full EC2 access (AmazonEC2FullAccess). The following example shows an AWS policy that explicitly grants full access to all AWS functions related to EC2 instances.

```json
{
    "Statement": [{
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*"
    }]
}
```
Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Navigate to the Customer Support, Base Plugins page and download the plugin .fpi file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select Options from the Tools menu.
5. Select Install. The Open dialog box opens.
6. Browse to and select the saved plugin .fpi file.
7. Select Install.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select Close. The plugin is listed in the Plugins pane.

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 access your AWS credentials:

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 and the sign-in credentials display.

7. In the Access Keys section, the AWS Access key ID displays. Copy the **Access key ID**.

8. Proceed to the next section to create an AWS connection.

**To add an AWS connection:**

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

2. Select **AWS** from the Options pane. The right pane opens to display two tabs: AWS Accounts and AWS Regions.

3. In the AWS Accounts tab, select **Add**. The Policy 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>Access Key ID</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>Secret Access Key</td>
<td>Verify Secret Access Key Confirm the accuracy of the Secret Access Key by re-entering it.</td>
</tr>
<tr>
<td>Connecting CounterACT Device</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 the AWS. In the drop-down, select an IP Address listed under the Appliances folder. Only one IAM user is allowed per connecting device.</td>
</tr>
<tr>
<td>Account Nickname</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.

6. It is optional to enter proxy server information. If using a proxy server with Basic Authentication, you will need that proxy's credentials (see AWS Requirements).

<table>
<thead>
<tr>
<th>Parameter</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 IP Address</td>
<td>Enter the IP address of the proxy server.</td>
</tr>
</tbody>
</table>
Proxy Server Port | Select the port number of the proxy server.
---|---
Proxy Server Username | (Optional) For proxies using Basic Authentication, enter the proxy server’s username.
Proxy Server Password | (Optional) For proxies using Basic Authentication, enter the proxy server’s password.
Verify Password | Verify the proxy server’s password.

7. Select **Next**. The Advanced pane opens.

8. Set the communication controls between CounterACT and AWS.

| Query Interval (seconds) | Specify how frequently the plugin should query AWS.
| Flow Log Collection | Check the box if you choose to enable flow log collection. This allows the collection of information about the IP traffic going to and from network interfaces in your VPC. For more information about flow logs, refer to Amazon VPC Flow Logs.
| Flow Log Query Interval (seconds) | Indicate the interval of flow logs collection. It is recommended that you set it for 8 hours / 28800 seconds (default).

- Flow Log collection may require considerable amount of time and hardware/network resources.

9. Select **Finish**. The new account displays in the AWS Accounts pane.

10. In the CounterACT Enterprise Manager, select **Apply** and confirm the changes.
11. After the account has been added, navigate to the AWS Regions tab and select **Sync** to retrieve the available AWS regions.

12. The Synchronizing AWS Regions dialog box displays the results. When finished, select **Close**.

13. In the AWS Regions pane, all the regions are now selected by default. Determine which regions that you would like the AWS account to discover EC2 instances. Make your selections based on the User Region, Access Key ID, Region Name, or Account Nickname. If you do not know which regions, use the default setting.

14. Select **Apply** and confirm the changes.

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

**Test the AWS Connection**

Using the configured settings, CounterACT attempts to connect to AWS and retrieve a list of all endpoints associated with the IAM user in the AWS regions specified in the connection.

**To test the AWS connection:**

1. Select the AWS Accounts tab and then select **Test**. CounterACT tests the AWS Connection to the Connected Device.
2. After viewing the test results, select Close.

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

**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 *Console User Guide*.

- **AWS EC2 AMI Classification Template**
- **AWS EC2 External Instance Classification Template**

**AWS EC2 AMI Classification Template**

Use the AWS EC2 AMI Classification template to create a CounterACT policy that classifies AWS EC2 instances based on their Amazon Machine Image (AMI). Instances where AMI does not match the ones you specify may be considered unauthorized machines. The policy template includes a configurable notification action to be sent for each rogue machine detected by CounterACT.

- Consider adding the "Apply EC2 Security Groups" action to isolate the unauthorized machine.
To create an AWS EC2 AMI Classification policy:

1. Log in to the CounterACT Console and select the Policy tab.
3. Select Templates and expand the AWS folder.
4. Select AWS EC2 AMI Classification.

5. Select Next. The Policy Name dialog box opens. Enter the name of the new policy and (optional) description.
6. Select **Next**. The Scope pane opens.

7. Enter the IP Address information and then select **OK**. The Sub-Rules pane opens.

8. Double-click the Unauthorized AMI sub-rule to open it. The [Name of AWS EC2 AMI Classification policy] Unauthorized AMI dialog box opens.
9. In this page, you can add conditions and actions. A list of these properties can be found in Detecting Cloud Endpoints – Host Properties.

10. Select OK. In the [Name of AWS EC2 AMI Classification policy] Unauthorized AMI dialog box, select OK.


Updating the AMI Whitelist

The AMI Whitelist lists the “good” AMIs. The default AWS EC2 AMI Classification policy template checks this list to find out if an instance’s AMI is listed in the whitelist or not.

Once the AWS EC2 AMI Classification template has been set up, the AMI classification itself needs to be configured into the EC2 instance. You will need to access the Error! Hyperlink reference not valid. and obtain the AMI ID of all sanctioned AMIs. Once the AMI IDs are available, you can then update the AMI whitelist.

To update the AMI whitelist:

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

2. In the left pane, select Lists. In the right pane, all the AMIs are listed.
3. Select an item and then 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 ID from the Error! Hyperlink reference not valid. into the field and then 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.

8. Select Apply in the Lists pane.
## AWS EC2 External Instance Classification Template

Use the AWS EC2 External Instance Classification template to create a CounterACT policy that classifies AWS EC2 instances as external ("internet-facing") or internal. AWS EC2 instances that match the policy rule are mapped to the "Internet Facing AWS EC2 Instances" group. The rule is meant to identify an EC2 instance that is communicating, or is meant to communicate, to the outer network by checking for allocation of a Public IP address. These instances are grouped into the "External Instances" group by default.

To create an AWS EC2 External Instance Classification policy:

1. Login to the CounterACT Console and select the **Policy** tab.
2. Select **Add**. The Policy Wizard opens.
3. Select Templates and expand the **AWS** folder.
4. Select **AWS EC2 External Instance Classification**.
5. Select **Next**. The Name pane opens. Enter the name of the new policy.
6. Select **Next**. The Scope pane opens.
7. Enter the **IP Address information** and then select **OK**. The Sub-Rules pane opens.

8. Double-click the Unauthorized AMI sub-rule to open it. The [Name of AWS EC2 External Instance Classification policy] EC2 Internet Facing Instance dialog box opens.
9. In this page, you can add conditions and actions. A list of these properties can be found in Detecting Cloud Endpoints – Host Properties.

10. Select OK. In the [Name of AWS EC2 External Instance Classification policy] EC2 Internet Facing Instance dialog box, select OK.


Detecting Cloud Endpoints – Host Properties

When the AWS plugin is installed, there are many AWS-specific host properties that are 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.

AWS CloudWatch Flow Logs

This plugin integrates with AWS CloudWatch Flow Logs service to provide deeper visibility of traffic flow between instances. It captures incoming and outgoing flows for an instance and records information such as source IP, destination IP, port number, etc., and reports if the flow was accepted or denied.

CounterACT parses these Flow Logs and identifies specific information about the to-and-from communications for an EC2 instance. This information helps identify unusual communication. For example, if you find EC2 instances are sending requests
from an unauthorized machine, those instances can easily be quarantined by applying a restrictive security group.

The AWS CloudWatch Flow Logs can also identify misconfigurations of an EC2 instance. For example, if a database instance is communicating on port 80, it can be flagged as non-compliant and can be quarantined by applying a security group action isolating the endpoint and preventing further usage of that port.

In order to utilize this feature, you must have the Flow Log Collection enabled (checked) in AWS the accounts configuration.

All instances detected via Flow Logs, will be initially displayed as online, even though their current status may be listed as stopped or terminated.

To enable flow log collection:

1. In the CounterACT Console, select Options from the Tools menu.
2. Select AWS from the Options pane. The right pane opens to display two tabs: AWS Accounts and AWS Regions.
3. In the AWS Accounts tab, select an item and then select Edit.
4. The Edit AWS Connection dialog box opens. Select the Advanced tab.

5. Select the Flow Log Collection checkbox and set the Flow Log Query Interval. It is recommended to set the interval to 28800 seconds. This is equivalent to an 8-hour interval.

6. Select OK.
7. In the AWS pane, select Apply.

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

When creating or editing a policy, you can set the traffic details of EC2 instances through the Conditions dialog box.

To access the AWS CloudWatch Flow Logs properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the EC2 CloudWatch Flow Logs folder in the Properties tree.

The following properties are available:

- EC2 Traffic as a Client
- EC2 Traffic as a Server

EC2 Traffic as a Client

Information on the outgoing traffic from the selected EC2 instance (acting as a client) is presented as a list of items (one item per Destination IP address). This information is derived from the communication observed in Flow Logs.

Each item has a distinct Destination IP address, a collection of Source and Destination Ports, as well as a collection of IANA Protocols and Associated actions used to communicate with that Destination.

CounterACT displays communication details with up to 100 destinations.
**EC2 Traffic as a Server**

Information on the incoming traffic to the selected EC2 instance (acting as a server), presented as a list of items (one item per each Source IP address). This information is derived from the communication observed in Flow Logs. Each item has a distinct Source IP address, a collection of Source and Destination Ports, as well as a collection of IANA Protocols and Associated actions used to communicate with that Source.

*CounterACT displays communication details with up to 100 sources.*

For more information about setting conditions, refer to the **CounterACT Console Guide**.

**AWS EC2**

This section describes the properties that are available when you install this module.

**To access the AWS EC2 properties:**

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the AC2 EC2 folder in the Properties tree.

<table>
<thead>
<tr>
<th><strong>AWS CloudWatch Monitoring</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AWS Virtual Private Cloud</strong></td>
<td>Indicates the Virtual Private Cloud into which the endpoint was launched.</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 AMI Owner</strong></td>
<td>Indicates the AWS account number of the owner of the Amazon Machine Image used for this EC2 instance.</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>EC2 Attached Block Devices</strong></td>
<td>Indicates the Elastic Block Storage volumes attached to this EC2 instance.</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 role associated with this EC2 instance.</td>
</tr>
<tr>
<td><strong>EC2 Instance ID</strong></td>
<td>Indicates the instance ID of the EC2 endpoint.</td>
</tr>
<tr>
<td><strong>EC2 Instance Name</strong></td>
<td>Indicates the instance name of the EC2 endpoint.</td>
</tr>
<tr>
<td><strong>EC2 Instance Type</strong></td>
<td>Indicates the CPU capacity, memory, and storage of this AWS endpoint. For example, m1.small, c1.xlarge.</td>
</tr>
<tr>
<td><strong>EC2 Kernel ID</strong></td>
<td>The operating system kernel associated with the AMI.</td>
</tr>
<tr>
<td><strong>EC2 Key Pair Name</strong></td>
<td>Indicates the key pair used to log in to the instance securely.</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 Launch Details</strong></td>
<td>Indicates 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 automatically when the bid price is higher than the Spot Price, and may be terminated if the Spot Price goes over the bid price.</td>
</tr>
<tr>
<td><strong>EC2 Location</strong></td>
<td>Indicates location information of the AWS endpoint.</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>The operating system platform, such as Windows.</td>
</tr>
<tr>
<td><strong>EC2 Public DNS</strong></td>
<td>Indicates the public hostname of the AWS endpoint, which resolves to the public IP address or Elastic IP address of the endpoint.</td>
</tr>
<tr>
<td><strong>EC2 Public IP</strong></td>
<td>Indicates the public IP address of the AWS endpoint.</td>
</tr>
<tr>
<td><strong>EC2 RAM disk ID</strong></td>
<td>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 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 this AWS endpoint 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 ID</strong></td>
<td>Indicates the AWS ID of the subnet that the EC2 instance was launched into, if applicable. A subnet is a range of IP addresses in a Virtual Private Cloud.</td>
</tr>
<tr>
<td><strong>EC2 Tags</strong></td>
<td>Indicates the tags given to the AWS endpoint.</td>
</tr>
</tbody>
</table>
For more information about setting conditions, refer to the CounterACT Console Guide.

Managing AWS Cloud Endpoints

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

To access the inventory:
1. Log in to the CounterACT Console and select the Inventory tab.
2. In the Views pane, expand the AWS EC2 folder.
3. Select an AWS EC2 item to view the real-time inventory information, for example, EC2 Launch Details.

Refer to Working with Inventory Detections in the CounterACT Console User’s Manual or the Console, Online Help for information about how to work with the CounterACT Inventory.
AWS Admission Events

After adding and testing the AWS Connection, it is helpful to review the host profile, including admission events.

To review the host profile:
1. Login in to the CounterACT Console and select All Hosts.
2. The Detections pane opens. Select a host to review the profile of the host.
3. In the Profile tab, right-click on the Admission field. Information about the new EC2 endpoint opens in a pop-up.

4. If you require further information, double-clicking the item in the table opens the Host Details dialog box.
5. Select the All policies tab and then select Show host log. The Host Log dialog box opens.
6. Enter the parameters for running the log on and then select OK.
7. The Host Log is displayed with all the information. You can export or print the results.

Manually Run AWS Actions on any EC2 Instance

While AWS actions can be launched as part of a policy, you can also manually run the policy.

To manually run an AWS Action:
1. Login to the CounterACT Console and select All Hosts in the Home tab.
2. In the Detections pane, select a host entry.
3. Hover the mouse over the icon in the Action column. The status of the Action opens.
4. Right-click on an AWS endpoint, select AWS and then select the action you want done.
5. Click on the links to access further instructions on the AWS Actions.
   - EC2 Security Group Action
   - Disable EC2 Termination Protection Action
   - Enable EC2 Termination Protection Action
   - Start an EC2 Instance
   - Stop an EC2 Instance

**EC2 Security Group Action**

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 what kind of connections, such as IP addresses, ports, protocols, etc., 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 start the Apply EC2 Security Groups action:**

1. Login to the CounterACT Console and select All Hosts in the Home tab.

2. In the Detections pane, right-click on an endpoint, select AWS and then select Apply EC2 Security Groups. The Specify EC2 Security Groups parameters dialog box opens.
3. Select a Security Group(s) or Select All.
4. In the Append or overwrite field, select either:
   – Append this list to the current Security Group list – Add the selected IP address to the current Security Group list.
   – Overwrite the current Security Group with this list – Selecting this option replaces the current Security Group with the selected one. This is useful for isolating a non-compliant endpoint by applying it only with restrictive security groups.
5. 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 via the AWS Console, API, or CLI.

Enabling termination protection prevents accidental termination of EC2 instances.

**To run a Disable EC2 Termination Protection action:**

1. Login to the CounterACT Console and select All Hosts in the Home tab.
2. In the Detections pane, right-click on an endpoint, select AWS and then select **Disable EC2 Termination Protection**. The Specify Disable EC2 Termination Protection parameters dialog box opens.
3. Set the parameters for the selected IP address’ action schedule
   - Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.
   - Customize action start time – selecting the radio button and then selecting the Define button opens the Action Scheduler dialog box.
     a. The Action Scheduler dialog box opens.
b. Set parameters and then select **OK**.

4. 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 from an EC2 instance.

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

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

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

1. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Enable EC2 Termination Protection**. The Specify Enable EC2 Termination Protection parameters dialog box opens.

2. Set the parameters for the selected IP address’ action schedule
   
   – Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.
   
   – Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

   a. The Action Scheduler dialog box opens.

   ![Action Scheduler Dialog](image)

   b. Set parameters and then select **OK**.

   ![Action Scheduler Dialog](image)
3. In the Specify Enable EC2 Termination Protection parameters dialog box, select **OK**.

### Start an EC2 Instance

Use this action to start an EC2 instance.

**To run a Start an EC2 Instance action:**

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.

2. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Start EC2 Instance**. The Specify Start EC2 Instance parameters dialog box opens.

3. Set the parameters for the selected IP address’ action schedule
   - **Start action when host matches policy condition** – implements the policy when the policy condition(s) is met by the host.
   - **Customize action start time** – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

   **a.** The Action Scheduler dialog box opens.
Stop an EC2 Instance

This section covers how to stop a virtual computing environment (instance).

To run a Stop an EC2 Instance action:

1. Login to the CounterACT Console and select All Hosts in the Home tab.
2. In the Detections pane, right-click on an endpoint, select AWS and then select Stop EC2 Instance. The Specify Stop EC2 Instance parameters dialog box opens.
3. Set the parameters for the selected IP address’ action schedule
   - Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.
   - Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.
   a. The Action Scheduler dialog box opens.
ForeScout® Amazon® Web Services (AWS) Plugin  Configuration Guide

4. In the Specify Enable EC2 Termination Protection 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 a access key ID and secret access key that is required when configuring the AWS plugin.

2. **Level of Access** – If you would like to be able to control EC2 instances from CounterACT using AWS actions, then you will need *AmazonEC2FullAccess* for the user account. For gaining visibility only, *AmazonEC2ReadOnlyAccess* is sufficient.

3. **AWS Regions** – If you want complete visibility across all regions then while performing sync during configuration choose all the regions available. For a restrictive view you can pick specific regions only.

4. **Set Communications with AWS (Polling)** – When configuring the AWS plugin, it is recommended to use the default settings for *Query Interval* and *Flow Log Query Interval*. Depending upon the amount of data, the polling of EC2 instances can take anywhere between 1-4 hours per 1,000 instances.

5. **CounterACT Active Discovery** – If you do not want CounterACT to perform Active Discovery such as nmap, HPS Inspection, WMI, etc., 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.

**Additional CounterACT Documentation**

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

**Documentation Portal**

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.
To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online 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.

Console User Manual
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 Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-10-18 10:19