



October 2018

Version Information

Amazon® Web Services (AWS) Plugin version 2.0.0.

This section describes requirements for this version.

CounterACT Software Requirements

This 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)

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

Amazon Web Services 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 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

Use Cases

This plugin addresses the following use cases:

- *Consolidated Visibility* – Extended's CounterACT's see and control capability to AWS public cloud.
- *Encryption*– Verify that EC2 Elastic Block Storage (EBS) is encrypted.



Amazon® Web Services Plugin 2.0.0

CounterACT® Plugin Update

Release Notes

- *Dynamic Segmentation of Instances* – Segment EC2 instances based on their classification and/or compliance posture.
- *Security Management of EC2 Instances* – Manage security settings of instances using security groups.
- *AWS Account* – Verify that Multi-Factor Authentication (MFA) is enabled for the root user.
- *IAM Roles and Users* – Monitor if any IAM role or IAM user is created or modified.
- *Network* – Verify that no EC2 instance has a public IP address that is an Internet-facing address.

New Features in 2.0

The new features in 2.0 are as follows:

- Added support for multiple AWS accounts from common managing appliance.
 - Managing large deployments by dedicating AWS account and/or regions to specific managing appliances.
 - Added visibility into and control of IAM users and VPCs, and visibility into other AWS properties, such as IAM user roles.
 - Enhanced scalability support to handle up to 20K AWS endpoints per managing appliance.
 - Added near real-time context with Delta Polling support.
 - Added overlapping CIDR checks to identify if subnets have the same IP ranges.
 - Enhanced test output and manual polling capability.
 - Deprecated support for CloudWatch Flow Logs.
- 📄 *If you are currently using Flow Logs in policies (for example, sessions as a property, EC2 traffic as client or server, or client ports), these policies will be flagged during the AWS plugin upgrade. To proceed with the upgrade, remove any policies that reference AWS Flow Logs.*

Fixed Issues

AWS 2.0 is a re-architected plugin, so this section is not applicable for this release.



Known Issues

None.

Limitations

The following are AWS limitations:

- IPv6 properties of EC2 instances do not get populated in CounterACT.
- If two accounts/regions/VPCs have EC2 instances with duplicate IP addresses, they will be overwritten in CounterACT.
- AWS Config is not automatically configured using **Deploy**. Manual configuration is required.
- If/when AWS adds support for a new region, the new region does not automatically display in the plugin.
- When enabled, delta polling will read from CloudWatch logs, even if Lambda functions/AWS Config is not configured or enabled.

How to Install

Perform the following steps to download the plugin from the Web site and install it on the Console.

To install the plugin:

1. Navigate to the [Product Updates Portal, 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.
4. Select **Plugins**. The Plugins pane opens.
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.



More Release Information

This section provides information about the following topics:

- [More Plugin Information](#)
- [Rollback Support](#)

More Plugin Information

Refer to the plugin configuration guide for more information about the plugin.

To access the plugin configuration guide:

1. After the plugin is installed, select **Options** from the Console **Tools** menu.
2. Navigate to and select the **Plugins** folder. The Plugins pane opens.
3. Select the plugin from the Plugins pane and then select **Help**.

Rollback Support

Under certain circumstances you may want to roll back the plugin to a previously installed version. This may happen, for example, if your system does not operate as expected after the plugin upgrade.

You can roll back this plugin to a previous version.

Plugins on Appliances connected to the Enterprise Manager are rolled back to the selected version. Plugins on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances.

To view rollback versions and perform the roll back:

1. Select **Options** from the Console **Tools** menu.
2. Navigate to and select the **Plugins** folder.
3. In the Plugins pane, select the plugin you want to roll back.
4. Select **Rollback**. A dialog box opens listing the versions to which you can roll back.
5. Select a version and then select **OK**. A dialog box opens showing you the rollback progress.



Amazon[®] Web Services Plugin 2.0.0

CounterACT[®] Plugin Update

Release Notes

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-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-10-05 08:42