Amazon Inspector

User Guide

Version Latest

Amazon Inspector: User Guide

Table of Contents

What is Amazon Inspector?

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you to identify potential security issues. Using Amazon Inspector, you can define a collection of AWS resources that you want to include in an assessment target. You can then create an *assessment template* and launch a security *assessment run* of this target. During the assessment run, the network, file system, and process activity within the specified target are monitored, and a wide set of activity and configuration data is collected. This data includes details of communication with AWS services, use of secure channels, details of the running processes, network traffic among the running processes, and more. The collected data is correlated, analyzed, and compared to a set of security *rules* specified in the assessment template. A completed assessment run produces a list of *findings* - potential security problems of various severity.

Important
AWS does not guarantee that following the provided recommendations will resolve every potential security issue. The findings generated by Amazon Inspector depend on your choice of rule packages included in each assessment template, the presence of non-AWS components in your system, and other factors. You are responsible for the security of applications, processes, and tools that run on AWS services. For more information, see the AWS Shared Responsibility Model for security.

Note
AWS is responsible for protecting the global infrastructure that runs all the services offered in the AWS cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. AWS provides several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations. For more information, see AWS Cloud Compliance.

For more information, see Amazon Inspector Terminology and Concepts (p. 3).

Benefits of Amazon Inspector

- Amazon Inspector enables you to quickly and easily assess the security of your AWS resources for forensics, troubleshooting, or active auditing purposes at your own pace, either as you progress through the development of your infrastructures or on a regular basis in a stable production environment.
- Amazon Inspector enables you to focus on more complex security problems by offloading the overall security assessment of your infrastructure to this automated service.
- By using Amazon Inspector, you can gain deeper understanding of your AWS resources because Amazon Inspector findings are produced through the analysis of the real activity and configuration data of your AWS resources.

Features of Amazon Inspector

- **Configuration Scanning and Activity Monitoring Engine** - Amazon Inspector provides an engine that analyzes system and resource configuration and monitors activity to determine what an assessment target looks like, how it behaves, and its dependent components. The combination of this telemetry provides a complete picture of the assessment target and its potential security or compliance issues.
- **Built-in Content Library** - Amazon Inspector incorporates a built-in library of rules and reports. These include checks against best practices, common compliance standards and vulnerabilities. These checks include detailed recommended steps for resolving potential security issues.
- **Automatable via API** - Amazon Inspector is fully automatable via an API. This allows organizations to incorporate security testing into the development and design process, including selecting, executing, and reporting the results of those tests.

Amazon Inspector Pricing

Amazon Inspector is priced per agent per assessment (agent-assessment) per month. For detailed information about Amazon Inspector pricing, see Amazon Inspector Pricing.

Accessing Amazon Inspector

You can work with the Amazon Inspector service in any of the following ways.

Amazon Inspector Console
: Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.

  The console is a browser-based interface to access and use the Amazon Inspector service.

AWS SDKs
: AWS provides software development kits (SDKs) that consist of libraries and sample code for various programming languages and platforms (Java, Python, Ruby, .NET, iOS, Android, and more). The SDKs provide a convenient way to create programmatic access to the Amazon Inspector service. For information about the AWS SDKs, including how to download and install them, see Tools for Amazon Web Services.

Amazon Inspector HTTPS API
: You can access Amazon Inspector and AWS programmatically by using the Amazon Inspector HTTPS API, which lets you issue HTTPS requests directly to the service. For more information, see the Amazon Inspector API Reference.

AWS Command Line Tools
: You can use the AWS command line tools to issue commands at your system's command line to perform Amazon Inspector tasks; this can be faster and more convenient than using the console. The command line tools are also useful if you want to build scripts that perform AWS tasks. For more information, see the Amazon Inspector's AWS Command Line Interface.

Amazon Inspector Terminology and Concepts

As you get started with Amazon Inspector, you can benefit from learning about its key concepts.

AWS agent
A software agent that you must install on all Amazon Elastic Compute Cloud instances (EC2 instances) that are included in the assessment target, the security of which you want to evaluate with Amazon Inspector. The AWS agent monitors the behavior of the EC2 instance on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service. For more information, see AWS Agents (p. 12).

Assessment target
In the context of Amazon Inspector, a collection of AWS resources that work together as a unit to help you accomplish your business goals. Amazon Inspector evaluates the security state of the resources that constitute the assessment target.

> **Note**
> At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions:
>
> - US West (Oregon)
> - US East (N. Virginia)
> - EU (Ireland)
> - Asia Pacific (Incheon)
> - Asia Pacific (Mumbai)
> - Asia Pacific (Tokyo)
> - Asia Pacific (Sydney)
>
> Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations.

To create an Amazon Inspector assessment target, you must first tag your EC2 instances with key-value pairs of your choice, and then create a view of these tagged EC2 instances that have common keys or common values. For more information, see Amazon Inspector Assessment Targets (p. 22).

Assessment template
A configuration that is used during your assessment run, including rules packages against which you want Amazon Inspector to evaluate your assessment target, the duration of the assessment run, Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings, and Amazon Inspector-specific attributes (key-value pairs) that you can assign to findings generated by the assessment run that uses this assessment template.

Assessment run
The process of discovering potential security issues through the analysis of your assessment target's configuration and behavior against specified rule packages. During an assessment run, the agent monitors, collects, and analyzes behavioral data (telemetry) within the specified target, such as the use of secure channels, network traffic among running processes, and details of communication with AWS services. Next, the agent analyzes the data and compares it against a set of security rule packages specified in the assessment template used during the assessment run. A completed assessment run produces a list of findings - potential security issues of various severity. For more information, see Amazon Inspector Assessment Templates and Assessment Runs (p. 24).

Finding
A potential security issue discovered during the Amazon Inspector assessment run of the specified target. Findings are displayed in the Amazon Inspector console or retrieved through the API, and contain both a detailed description of the security issue and a recommendation on how to fix it. For more information, see Amazon Inspector Findings (p. 28).

Rule
In the context of Amazon Inspector, a security check that the agent performs during an assessment run. When a rule detects a potential security issue, Amazon Inspector generates a finding that describes the issue.

Rules package
In the context of Amazon Inspector, a collection of rules. A rules package corresponds to a security goal that you might have. You can specify your security goal by selecting the appropriate rules package when you create an Amazon Inspector assessment template. For more information, see Amazon Inspector Rules Packages and Rules (p. 30).

Telemetry
Behavioral data such as records of network connections and process creations, collected by the Amazon Inspector agent on your EC2 instances during an assessment run and passed to the Amazon Inspector service for analysis.

Setting up Amazon Inspector

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon Inspector. If you don't have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Open http://aws.amazon.com/, and then choose **Create an AWS Account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

When you launch the Amazon Inspector console for the first time, choose **Get Started** and complete the following prerequisite tasks. You must complete these tasks before you can create, start, and complete an Amazon Inspector assessment run:

- Create a role to allow Amazon Inspector to access your AWS account (p. 5)
- Tag all EC2 instances that you want to include in your assessment target (p. 6)
- Install the Amazon Inspector agent on all EC2 instances that you want to include in your assessment target (p. 6)

Create a Role

In order for Amazon Inspector to access the EC2 instances in your AWS account and collect the behavior data during the assessment run, you must create an Identity Access Management (IAM) role. To create an IAM role, do the following:

- On the **Inspector prerequisites** page, choose **Select/Create Role**.

  This launches the IAM console where you see the following message: "Amazon Inspector is requesting permissions to use resources in your account. Choose **Allow** to give Amazon Inspector read-only access to resources in your account."

  Choose **Allow**. You are redirected back to the Amazon Inspector console where you can complete the rest of the Getting Started wizard.

Create Assessment Targets with EC2 instance Tags

Amazon Inspector evaluates whether your assessment targets (collections of AWS resources) have potential security issues. Amazon Inspector uses the tags applied to your EC2 instances to target those resources as part of your defined assessment template. When configuring your assessment templates and specifying tags to target, you can utilize the tags you already have defined on your EC2 instances, or create entirely new tags specifically for your assessments. If you do not have tags already or want to create new tags, you must apply these new tags to all EC2 instances that you want as part of your assessment target. For more information about tagging, see Working with Tag Editor and Tagging Your Amazon EC2 Resources.

Important
At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions:

- US West (Oregon)
- US East (N. Virginia)
- EU (Ireland)
- Asia Pacific (Incheon)
- Asia Pacific (Mumbai)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)

Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations. In this release of Amazon Inspector, your assessment targets can consist only of EC2 instances that run the 64-bit version of the following operating systems:

- Amazon Linux (2015.03 or later)
- Ubuntu (14.04 LTS)
- Red Hat Enterprise Linux (7.2)
- CentOS (7.2)
- Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

  Important
  Support for Windows-based operating systems for the AWS agent is in preview and subject to change.

For detailed information about tagging EC2 instances to be included in Amazon Inspector assessment targets, see Amazon Inspector Assessment Targets (p. 22).

Install the AWS Agent

You must install the AWS agent on each EC2 instance in your assessment target. The agent monitors the behavior of the EC2 instances on which it is installed, including network, file system, and process activity, and collects a wide set of behavior and configuration data (telemetry), which it then passes to the Amazon Inspector service. For more information about AWS agent privileges, security, updates, telemetry data, and access control, see AWS Agents (p. 12).

For more information about how to install, uninstall, and reinstall the AWS agent, and how to verify whether the installed agent is running, see Working with AWS Agents (p. 14).

Amazon Inspector Quickstart Walkthrough

Before you follow the instructions in this walkthrough, we recommend that you get familiar with the Amazon Inspector Terminology and Concepts (p. 3).

This walkthrough is designed for a first-time user and includes all the tasks, including prerequisite tasks, for creating an assessment target, assessment template, and assessment run.

> **Note**
> This walkthrough is designed to demonstrate how to use Amazon Inspector to analyze the behavior of the EC2 instances that run the Ubuntu Server 14.04 LTS operating system.

By completing the steps in this walkthrough, you will accomplish the following:

- Set Up Amazon Inspector (p. 8). This is the first-run experience, including completing all the pre-requisite tasks via the Amazon Inspector console.
- Prepare Your Assessment Target for the Assessment Run (p. 9)
- Create an Assessment Template and Start an Assessment Run (p. 9)
- Locate and Analyze Generated Findings (p. 10)
- Apply the Recommended Fix to Your Assessment Target (p. 10)

Set Up Amazon Inspector

1. Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. Choose **Get started** to launch the **Get started** wizard, and on the **Step 1: Prerequisites** page, do the following:

   a. Choose **Select/Create Role** to create a role that allows Amazon Inspector to access your AWS account. For detailed information, see Create a Role (p. 5).

   b. Tag the EC2 instances that you want to include in your Amazon Inspector assessment target.

      For this walkthrough, create one EC2 instance running Ubuntu Server 14.04 LTS and tag it using the **Name** key and a value of **`InspectorEC2Instance`**.

Note
You can add tags to EC2 instances when you create them or add, change, or remove those tags one EC2 instance at a time on each EC2 instance's console page. To add tags to multiple EC2 instances at once, you can use Tag Editor. For more information, see Tag Editor. For more information about tagging EC2 instances, see Resources and Tags.

c. Install the Amazon Inspector agent on your tagged EC2 instance. For detailed information, see Install the AWS Agent (p. 6).

Prepare Your Assessment Target for the Assessment Run

For this walkthrough, you modify your assessment target to expose it to potential security issue CVE-2014-1424. For more information, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1424. Also, for more information, see Common Vulnerabilities and Exposures (p. 31).

Connect to your instance **`InspectorEC2Instance`** that you created in the preceding section, and run the following command:

```
sudo apt-get install apparmor=2.8.95~2430-0ubuntu5
```

Create an Assessment Template and Start an Assessment Run

1. On the **Define an assessment target** page, do the following:

   a. For **Name**, type the name for your assessment target.

      For this walkthrough, type **`MyTarget`**.

   b. Use the **Tags' Key** and **Value** fields to type the tag key name and key-value pairs in order to select the EC2 instances that you want to include in this assessment target.

      For this walkthrough, to use the EC2 instance that you created in the preceding step, type **`Name`** in the **Key** field and **`InspectorEC2Instance`** in the **Value** field, and then choose **Next**.

2. On the **Define assessment template** page, do the following:

   a. For **Name**, type the name for your assessment template. For this walkthrough, type **`MyFirstTemplate`**.

   b. For **Rule packages**, use the pull-down menu to select the rule packages that you want to use in this assessment template.

      For this walkthrough, choose **Common Vulnerabilities and Exposures**.

   c. For **Duration**, specify the duration for your assessment template.

      For this walkthrough, select 1 hour.

   d. Choose **Next**.

3. On the **Review** page, review your selections, and then choose **Create and run**.

Locate and Analyze Generated Findings

A completed assessment run produces a set of findings, or potential security issues that Amazon Inspector discovered in your assessment target. You can review the findings and follow the recommended steps to resolve the potential security issues.

In this walkthrough, if you complete the preceding steps, your assessment run produces a finding against the common vulnerability CVE-2014-1424.

1. Navigate to the **Assessment Runs** page in the Amazon Inspector console and verify that the status of **MyFirstAssessment** that you created in the preceding step is set to **Collecting_Data**. This indicates that the assessment run is currently in progress, and the telemetry data for your target is being collected and analyzed against the selected rules packages.
2. You cannot view the findings generated by the assessment run while it is still in progress. In a production environment, we recommend that you let the assessment run complete its entire duration. However, for this walkthrough, you can stop **MyFirstAssessment** after several minutes. To stop the assessment run, select it, and then choose **Stop**.

   Note that the status of **MyAssessment** changes to **Data_Collected**.
3. In the Amazon Inspector console, navigate to the **Findings** page.

   You can see a new finding of High severity that reads "Instance InspectorEC2Instance is vulnerable to CVE CVE-2014-1424".

   Note
   If you do not see the new finding, choose the **Refresh** icon.

   To expand the view and see the details of this finding, choose the arrow to the left of the finding. The details of the finding include the following:

   - The name of the assessment target that includes the EC2 instance where this finding was registered
   - The name of the assessment template that produced this finding
   - The assessment run start time
   - The assessment run end time
   - The assessment run status
   - The name of the rules package that includes the rule that triggered this finding
   - The name of the finding
   - The description of the finding
   - The recommended remediation steps that you can complete to fix the potential security issue described by the finding

Apply the Recommended Fix to Your Assessment Target

For this walkthrough, you modified your assessment target to expose it for a potential security issue CVE-2014-1424. In this procedure, you can apply the recommended fix for this issue.

1. Connect to your instance **`InspectorEC2Instance`** that you created in the preceding section, and run the following command: `sudo apt-get install apparmor=2.8.95~2430-0ubuntu5.1`
2. On the **Assessment Templates** page, select **MyFirstTemplate**, and then choose **Run** to start a new assessment run using this template.
3. Follow the steps in Locate and Analyze Generated Findings (p. 10) to see the findings resulting from this subsequent run of the **MyFirstTemplate** template.

   Because you resolved the found security issue, you can now see a finding that reads **No potential security issues found**, informing you that Amazon Inspector found no potential security issues during this assessment run.

AWS Agents

To assess the security of the EC2 instances that make up your Amazon Inspector assessment targets, you must install the AWS agent on each instance. The agent monitors the behavior (including network, file system, and process activity) of the EC2 instance on which it is installed, collects behavior and configuration data (telemetry), and then passes the data to the Amazon Inspector service.

Important
For more information about how to install, uninstall, and reinstall the AWS agent, and how to verify whether the installed agent is running, see Working with AWS Agents (p. 14).

Important
If your EC2 instances require a proxy server to connect to the internet, the Amazon Inspector agent running on these instances will not be able to connect to the Amazon Inspector service endpoint because proxy support for the Amazon Inspector agents is currently not available.

AWS Agent Privileges

Administrative or root permissions are required to install the AWS agent. On supported Linux-based operating systems, the AWS agent consists of a user mode executable that runs with root access and a kernel module that is required for the agent to function. On supported Windows-based operating systems, the agent consists of an updater service and an agent service, each running in user mode with LocalSystem privileges, and a kernel mode driver that is required for the agent to function.

Network and AWS Agent Security

All communication between the AWS agent and Amazon Inspector is initiated by the AWS agent. As such, the agent must have an outbound network path to the public endpoint for Amazon Inspector and Amazon S3 services. For more information, see AWS IP Address Ranges. Additionally, as all connections from the agent are established outbound, it is not necessary to open ports in your security groups to allow inbound communications to the agent from Amazon Inspector.

The AWS agent periodically communicates with Amazon Inspector over a TLS-protected channel which is authenticated using either the AWS identity associated with the role of the EC2 instance, if present, or with the instance metadata document if no role is assigned to the instance. Once authenticated, the agent sends heartbeat messages to the service and receives instructions from the service as responses to the heartbeat messages. If an assessment has been scheduled, the agent receives the instructions for that assessment. These instructions are structured JSON files and tell the agent to enable or disable specific

pre-configured sensors in the agent. Each instruction action is pre-defined within the agent and arbitrary instructions cannot be executed.

During an assessment, the agent gathers telemetry data from the system to send back to Amazon Inspector over a TLS-protected channel. The agent does not make changes to or inspect the data it collects; it only sends the telemetry data back to the Amazon Inspector for processing. Beyond the telemetry data that it generates, the agent is not capable of collecting or transmitting any other data about the system or assessment targets that it is assessing. At present, there is no method exposed for intercepting and examining telemetry data at the agent.

AWS Agent Updates

As updates for the AWS agent become available, they are automatically downloaded from Amazon S3 and applied. This eliminates the need for you to track and manually maintain the versioning of the agents that you have installed on your EC2 instances. All updates are subject to audited Amazon change control processes to ensure compliance with applicable security standards. To further ensure the security of the agent, all communication between the agent and the auto-update release site (S3) are performed over a TLS connection, and the server is authenticated. All binaries involved in the auto-update process are digitally signed and the signatures are verified by the updater prior to installation. The auto-update process is executed only during non-assessment periods, and the update process has the ability to rollback and retry the update if any errors are detected. Finally, the agent update process serves to only upgrade the agent capabilities, and none of your specific information is ever sent from the agent to Amazon Inspector as part of the update workflow. The only information communicated as part of the update process is the basic installation success/fail telemetry and, if applicable, any update failure diagnostic information.

Telemetry Data Lifecycle

The telemetry data generated by the AWS agent during assessment runs is formatted in JSON files and delivered in near-real-time over TLS to Amazon Inspector, where it is encrypted with a per-assessment-run, ephemeral KMS-derived key and securely stored in an S3 bucket dedicated for Amazon Inspector. The rules engine of Amazon Inspector' accesses the encrypted telemetry data in the S3 bucket, decrypts it in memory, and processes the data against the configured assessment rules to generate findings. The telemetry data stored in S3 is retained only to allow for assistance with support requests and is not used or aggregated by Amazon for any other purpose. After 30 days, telemetry data is permanently deleted per a standard Amazon Inspector-dedicated S3 bucket lifecycle policy. At present, Amazon Inspector does not provide an API or an S3 bucket access mechanism to collected telemetry.

Access Control from Amazon Inspector into AWS Accounts

As a security service, the Amazon Inspector control plane is restricted from direct access to your AWS accounts and resources. All communications with your environment are initiated by the AWS agent that is installed on EC2 instances. The objects that you create, such as assessment targets, assessment templates, and findings generated by Amazon Inspector, are stored in a database managed by and accessible only to Amazon Inspector.

Working with AWS Agents

This topic describes how to install, uninstall, and reinstall the AWS agent on supported operating systems and how to verify whether the installed agent is running.

Once the AWS agent is installed and running on your EC2 instance, you can modify the settings in the **agent.cfg file** to alter the agent's behavior. The **agent.cfg file** is located in the **/opt/aws/awsagent/etc** directory on Linux-based operating systems and in the **C:\ProgramData\Amazon Web Services\AWS Agent** directory on Windows-based operating systems. After you modify and save the **agent.cfg file**, you must stop and start the agent in order for the changes to take effect.

> **Important**
> We highly recommend that you modify the **agent.cfg** file only with the guidance of AWS Support.

Topics

Supported Operating Systems for the AWS Agent

In this release of Amazon Inspector, your assessment targets can consist only of EC2 instances that run the 64-bit version of the following operating systems:

- Amazon Linux (2015.03 or later)
- Ubuntu (14.04 LTS)
- Red Hat Enterprise Linux (7.2)
- CentOS (7.2)
- Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

> **Important**
> Support for Windows-based operating systems for the AWS agent is in preview and subject to change.

> **Note**
> Follow this link to view a list of kernel versions that are compatible with the AWS agent running on Amazon Linux, Ubuntu, Red Hat Enterprise Linux, and CentOS: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json. This list does not apply to the AWS agent running on Windows Server 2012 or Windows Server 2012 R2.

At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions:

- US West (Oregon)
- US East (N. Virginia)
- EU (Ireland)
- Asia Pacific (Incheon)
- Asia Pacific (Mumbai)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)

Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations.

Working with AWS Agents on Linux-based Operating Systems

Note
The following commands are functional in all regions that are supported by Amazon Inspector.

Sign in to your EC2 instance running a Linux-based operating system, and run any of the following procedures.

To install the AWS agent on Linux-based operating systems

1. Download the agent installation script by running either of the following commands:
   - **wget https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install**
   - **curl -O https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install**
2. (Optional) Verify that the AWS agent installation script is not altered or corrupted. For more information, see (Optional) Verify the Signature of the AWS Agent Download (p. 18)
3. To install the agent, run **sudo bash install**.

   Note
   As updates for the AWS agent become available, they are automatically downloaded from Amazon S3 and applied. For more information, see AWS Agent Updates (p. 13).
   If you want to skip this auto-update process, make sure to run the following command when you install the agent:
   sudo bash install -u false

   Note
   (Optional) To remove the agent installation script, run **rm install** .

To uninstall the AWS agent on Linux-based operating systems

- To uninstall the agent, use one of the following commands:
  - On Amazon Linux, CentOS, and Red Hat, run **yum remove AwsAgent**
  - On Ubuntu Server, run **apt-get remove awsagent**

To stop the AWS agent on Linux-based operating systems

- To stop the agent, run **sudo /etc/init.d/awsagent stop**

To start the AWS agent on Linux-based operating systems

- To start the agent, run **sudo /etc/init.d/awsagent start**

To verify AWS agent dependencies on Linux-based operating systems

- Make sure that the following files required for the agent to be successfully installed and functioning properly are installed:
  - libgcc1
  - libc6
  - libstdc++6
  - libssl1.0.0
  - libpcap0.8

To verify that the AWS Agent is running on Linux-based operating systems

- To verify that the AWS agent is installed and running, sign in to your EC2 instance, and run the following command:

  sudo /opt/aws/awsagent/bin/awsagent status

  This command returns the status of the currently running agent, or an error stating that the agent cannot be contacted.

To uninstall the Amazon Inspector Preview version of the agent

1. **Important**
   If you installed the agent on your EC2 instances from the Preview release of Amazon Inspector, you must uninstall it.

   Use the following command to download the removal script:

   curl -O https://d1wk0tztpsntt1.cloudfront.net/linux/latest/remove_preview_agent
2. To remove the Amazon Inspector's Preview agent, run **sudo ./remove_preview_agent**
3. You can then use the procedure above to install the latest AWS agent for Amazon Inspector.

Working with AWS agents on Windows-based operating systems

Sign in to your EC2 instance running a Windows-based operating system and run any of the following procedures.

Important
Support for Microsoft Windows-based operating systems for the AWS agent is in preview and subject to change.

To install the AWS agent on Windows-based operating systems

1. Download the following .exe file:
   https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe
2. Open a command prompt window (with Administrative permissions), navigate to the location where you saved the downloaded AWSAgentInstall.exe, and run **AWSAgentInstall.exe** to install the AWS agent.

   Note
   As updates for the AWS agent become available, they are automatically downloaded from Amazon S3 and applied. For more information, see AWS Agent Updates (p. 13).
   If you want to skip this auto-update process, make sure to run this command to install the AWS agent.
   AWSAgentInstall.exe AUTOUPDATE=No

To uninstall the AWS agent on Windows-based operating systems

1. On your EC2 instance, navigate to **Control Panel**, **Add/Remove Programs.**
2. In the list of installed programs, choose **AWS Agent**, and then choose **Uninstall**.

To stop or start the AWS Agent or verify that the AWS agent is running on Windows-based operating systems

1. On your EC2 instance, choose **Start**, then **Run**, and then type **services.msc**.
2. If the agent is successfully running, two services are listed with their status set to **Started** or **Running** in the Services Window: **AWS Agent Service** and **AWS Agent Updater Service**.
3. To start the agent, right-click **AWS Agent Service** and then choose **Start**. If the service is successfully started, the status is updated to **Started** or **Running**.
4. To stop the agent, right-click **AWS Agent Service** and choose **Stop**. If the service is successfully stopped, the status is cleared (appears as blank). We do not recommend stopping the **AWS Agent Updater Service** as it will disable the installation of all future enhancements and fixes to the AWS Agent.

To verify that the AWS Agent is running on Windows-based operating systems

- To verify that the AWS agent is installed and running, sign in to your EC2 instance, open a command prompt with Administrative permissions, navigate to C:/Program Files/Amazon Web Services/Aws Agent, and then run the following command:

  AWSAgentStatus.exe

  This command returns the status of the currently running agent, or an error stating that the agent cannot be contacted.

(Optional) Verify the Signature of the AWS Agent Download

Whenever you download an application from the Internet, we recommend that you authenticate the identity of the software publisher and check that the application is not altered or corrupted since it was published. This protects you from installing a version of the application that contains a virus or other malicious code.

If after running the steps in this topic, you determine that the software for the AWS agent is altered, do not run the installation file. Instead, contact Amazon Web Services.

Overview

The first step is to establish trust with the software publisher: Download the public key of the software publisher, check that the owner of the public key is who they claim to be, and then add the public key to your *keyring*. Your keyring is a collection of known public keys. After you establish the authenticity of the public key, you can use it to verify the signature of the application.

AWS agent files are signed using GnuPG, an open source implementation of the Pretty Good Privacy (OpenPGP) standard for secure digital signatures. GnuPG (also known as GPG) provides authentication and integrity checking through a digital signature. Amazon EC2 publishes a public key and signatures that you can use to verify the downloaded Amazon EC2 CLI tools. For more information about PGP and GnuPG (GPG), see http://www.gnupg.org.

Install the GPG Tools

If your operating system is Linux or Unix, the GPG tools are likely already installed. To test whether the tools are installed on your system, type **gpg** at a command prompt. If the GPG tools are installed, you see a GPG command prompt. If the GPG tools are not installed, you see an error stating that the command cannot be found. You can install the GnuPG package from a repository.

To install GPG tools on Debian-based Linux

- From a terminal, run the following command: **apt-get install gnupg**.

To install GPG tools on Red Hat–based Linux

- From a terminal, run the following command: **yum install gnupg**.

Authenticate and Import the Public Key

The next step in the process is to authenticate the Amazon Inspector public key and add it as a trusted key in your GPG keyring.

To authenticate and import the Amazon Inspector public key

1. Obtain a copy of our public GPG build key by doing one of the following:
   - Download from https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg.
   - Copy the key from the following text and paste it into a file called `inspector.key`. Be sure to include everything that follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. At a command prompt in the directory where you saved **inspector.key**, use the following command to import the Amazon Inspector public key into your keyring:

```
gpg --import inspector.key
```

The command returns results similar to the following:

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" im
ported
                    gpg: Total number processed: 1
                    gpg:               imported: 1  (RSA: 1)
```

Make a note of the key value; you need it in the next step. In the preceding example, the key value is `58360418`.

3. Verify the fingerprint by running the following command, replacing *key-value* with the value from the preceding step:

```
gpg --fingerprint key-value
```

This command returns results similar to the following:

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960
 5836 0418
               uid                  Amazon Inspector <inspector@amazon.com>
```

Additionally, the fingerprint string should be identical to `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418` as shown above. Compare the key fingerprint returned to that published on this page. They should match. If they do not match, do not install the AWS agent installation script, and contact Amazon Web Services.

Verify the Signature of the Package

After you've installed the GPG tools, authenticated and imported the Amazon Inspector public key, and verified that the Amazon Inspector public key is trusted, you are ready to verify the signature of the Amazon Inspector installation script.

To verify the Amazon Inspector installation script signature

1. At a command prompt, run the following command to download the signature file for the installation script:

   ```
   curl -O https://d1wk0tztpsntt1.cloudfront.net/linux/latest/install.sig
   ```

2. Verify the signature by running the following command at a command prompt in the directory where you saved `install.sig` and the Amazon Inspector installation file. Both files must be present.

   ```
   gpg --verify ./install.sig
   ```

   The output should look something like the following:

   ```
   gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
   gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:         There is no indication that the signature belongs to the owner.
   Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
   ```

   If the output contains the phrase `Good signature from "Amazon Inspector <inspector@amazon.com>"`, it means that the signature has successfully been verified, and you can proceed to run the Amazon Inspector installation script.

   If the output includes the phrase `BAD signature`, check whether you performed the procedure correctly. If you continue to get this response, contact Amazon Web Services and do not run the installation file that you downloaded previously.

The following are details about the warnings you might see:

- **WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.** This refers to your personal level of trust in your belief that you possess an authentic public key for Amazon Inspector. In an ideal world, you would visit an Amazon Web Services office and receive the key in person. However, more often you download it from a website. In this case, the website is an Amazon Web Services web site.

- **gpg: no ultimately trusted keys found.** This means that the specific key is not "ultimately trusted" by you (or by other people whom you trust).

For more information, see http://www.gnupg.org.

Amazon Inspector Assessment Targets

You can use Amazon Inspector to evaluate whether your AWS assessment targets (your collections of AWS resources) have potential security issues that you need to address.

Note
At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions:

- US West (Oregon)
- US East (N. Virginia)
- EU (Ireland)
- Asia Pacific (Incheon)
- Asia Pacific (Mumbai)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)

Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations.

Tagging Resources to Create an Assessment Target

To create an assessment target for Amazon Inspector to assess, you start by tagging the EC2 instances that you want to include in your target. Tags are words or phrases that act as metadata for identifying and organizing your instances and other AWS resources. Amazon Inspector uses the tags that you create to identify the instances that belong to your target.

Every AWS tag consists of a key and value pair of your choice. For example, you might choose to name your key "Name" and your value "MyFirstInstance". After you tag your instances, you use the Amazon Inspector console to add the instances to your assessment target. It is not necessary that any instance match more than one tag key-value pair.

When you tag your EC2 instances to build assessment targets for Amazon Inspector to assess, you can create your own custom tag keys or use tag keys created by others in the same AWS account. You also can use the tag keys that AWS automatically creates, for example, the **Name** tag key that is automatically created for the EC2 instances that you launch.

You can add tags to EC2 instances when you create them or add, change, or remove those tags one at a time within each EC2 instance's console page. You can also add tags to multiple EC2 instances at once using the Tag Editor.

For more information, see Tag Editor. For more information about tagging EC2 instances, see Resources and Tags.

Amazon Inspector Assessment Targets Limits

You can create up to 50 assessment targets per AWS account.

Creating an Assessment Target (Console)

You can use the Amazon Inspector console to create assessment targets.

To create an assessment target

1. Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. In the navigation pane, choose **Assessment Targets**, and then choose **Create**.
3. For **Name**, type a name for your assessment target.
4. Use the **Tags**' **Key** and **Value** fields to type the tag key name and key-value pairs in order to select the EC2 instances that you want to include in this assessment target.
5. Choose **Save**.

Amazon Inspector Assessment Templates and Assessment Runs

Amazon Inspector can help you discover potential security issues through the analysis of your assessment target's behavior against selected rule packages. Amazon Inspector monitors and collects behavioral data (telemetry) within the specified assessment target, such as the use of secure channels, network traffic among running processes, and details of communication with AWS services. Next, Amazon Inspector analyzes and compares the data against a set of selected security rules packages. Finally, Amazon Inspector produces a list of findings - potential security issues of various severity.

Amazon Inspector Assessment Templates

Once you've created your assessment target - a collection of AWS resources that you want analyzed, you can then create an assessment template where you specify the configuration for your analysis. And finally, you can use the assessment template that you've created to start an assessment run - the data collection and telemetry analysis process.

An assessment template allows you to specify a configuration for your assessment runs, including the following:

- Rules packages that Amazon Inspector uses to evaluate your assessment target
- Duration of the assessment run

  Note

  You can set your duration to any of the following available values:

  - 15 minutes
  - 1 hour (recommended)
  - 8 hours
  - 12 hours
  - 24 hours

  The longer your running assessment template's duration is, the more thorough and complete is the set of telemetry that Amazon Inspector can collect and analyze. In other words, longer analysis allows Amazon Inspector to observe the behavior of your assessment target in greater detail and to produce fuller sets of findings. Similarly, the more thoroughly you use your AWS resources that are included in your target during the assessment run, the more thorough and complete is the telemetry set that Amazon Inspector can collect and analyze.

- Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings.
- Amazon Inspector-specific attributes (key-value pairs) that you can assign to findings that are generated by the assessment run that uses this assessment template

Once Amazon Inspector creates the assessment template, you can tag it like any other AWS resource. For more information, see Tag Editor. Tagging assessment templates enables you to organize them and get better oversight of your security strategy. For example, Amazon Inspector offers a large number of rules that you can assess your assessment targets against, but you might want to include various subsets of the available rules in your assessment templates in order to target specific areas of concern or to uncover specific security problems. Tagging assessment templates allows you to locate and run them quickly at any time in accordance with your security strategy and goals.

Important
Once the assessment template is created, it cannot be modified.

Amazon Inspector Assessment Templates Limits

You can create up to 500 assessment templates per AWS account.

Creating an Assessment Template (Console)

1. Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. Navigate to the **Assessment Templates** page, and then choose **Create**.
3. For **Name**, type a name for your assessment template.
4. For **Target name**, choose an assessment target to analyze.
5. For **Rule packages**, choose one or more rule packages to include in your assessment template.
6. For **Duration**, specify the duration for your assessment template.
7. For **SNS topics**, specify an SNS topic to which you want Amazon Inspector to send notifications about assessment run states and findings. Amazon Inspector can send SNS notifications about the following events:

   - An assessment run has started
   - An assessment run has ended
   - An assessment run's status has changed
   - A finding was generated

   For more information about setting up an SNS topic to which Amazon Inspector can send notifications, see Setting Up an SNS Topic for Amazon Inspector Notifications (Console) (p. 26).
8. To tag this assessment template, you can use **Tag**'s **Key** and **Value** fields.
9. To automatically assign attributes to all findings generated by this assessment template, you can use the **Key** and **Value** fields from **Attributes added to findings**. For more information about findings and tagging findings, see Amazon Inspector Findings (p. 28).
10. Choose **Create and run** or **Create**.

Assessment Runs

Once you create an assessment template, you can use it to initiate assessment runs. You can initiate multiple assessment runs using the same template as long as you stay within the assessment runs limit per AWS account. For more information, see Amazon Inspector Assessment Runs Limits (p. 26). If you're using the Amazon Inspector console, you must start the first run using the newly created assessment template via the **Assessment templates** page.

Once you start an assessment run, you can use the **Assessment runs** page to monitor the run's progress and details. You can use the **Stop** and **Delete** buttons on the **Assessment runs** page to either stop or delete a run. You can use the XYZ widget next to the run's **Start time** on the **Assessment runs** page to view the run's details, including the ARN of the run, the run start time, the name of the assessment target used during the run, the name of the assessment template used during the run, rules packages selected for the run, duration of the run, Amazon Inspector-specific attributes that you configured to be assigned to all findings generated from this run, tags specified for the assessment template used for the run, status of the run, and the number of findings generated during the run.

You can use the **Run**, **Stop**, and **Delete** buttons on either the **Assessment templates** page or the **Assessment runs** page to start, stop, or delete subsequent assessment runs using the previously used assessment template.

Amazon Inspector Assessment Runs Limits

You can create up to 50,000 assessment runs per AWS account.

You can have multiple assessment runs happening at the same time as long as the assessment targets used for these runs do not contain overlapping EC2 instances.

Setting Up an SNS Topic for Amazon Inspector Notifications (Console)

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. For more information, see What is Amazon Simple Notification Service?.

To set up an SNS topic for notifications

1. Create an SNS topic. For more information, see Create a Topic.
2. Subscribe to the SNS topic that you created. For more information, see Subscribe to a Topic.
3. Publish to the SNS topic. For more information, see Publish to a Topic.
4. Enable Amazon Inspector to subscribe and publish messages to the topic:

    a. Open the Amazon SNS console at https://console.aws.amazon.com/sns/.
    b. Select your SNS topic, and for **Actions**, choose **Edit topic policy**.
    c. For **Allow these users to publish messages to this topic** and **Allow these users to subscribe to this topic**, choose **Only these AWS users**, and then type in one of the following ARNs, depending on your region:

    - for US West (Oregon) - *arn:aws:iam::758058086616:root*
    - for EU (Ireland) - *arn:aws:iam::357557129151:root*

- for US East (N. Virginia) - *arn:aws:iam::316112463485:root*
- for Asia Pacific (Incheon) - *arn:aws:iam::526946625049:root*
- for Asia Pacific (Mumbai) - *arn:aws:iam::162588757376:root*
- for Asia Pacific (Tokyo) - *arn:aws:iam::406045910587:root*
- for Asia Pacific (Sydney) - *arn:aws:iam::454640832652:root*

Amazon Inspector Findings

Findings are potential security issues discovered during the Amazon Inspector's assessment of the selected assessment target. Findings are displayed in the Amazon Inspector console or via the API, and contain both a detailed description of the security issues and recommendations for resolving them.

Once Amazon Inspector generates the findings, you can track them by assigning Amazon Inspector-specific attributes to them. These attributes consist of key-value pairs.

Tracking findings with attributes can be quite useful for driving the workflow of your security strategy. For example, once you create and run an assessment, it generates a list of findings of various severity, urgency, and interest to you, based on your security goals and approach. You might want to follow one finding's recommendation steps right away to resolve a potentially urgent security issue. And you might want to postpone resolving another finding until your next upcoming service update. For example, to track a finding to resolve right away, you can create and assign to a finding an attribute with a key-value pair of **`Status`** / **`Urgent`**. You could also use attributes to distribute the workload of resolving potential security issues. For example, to give Bob (who is a security engineer on your team) the task of resolving a finding, you can assign to a finding an attribute with a key-value pair of **`Assigned Engineer`** / **`Bob`**.

Locating, Analyzing, and Assigning Attributes to Findings

Complete the following procedure on any of the generated Amazon Inspector findings:

To locate, analyze, and assign attributes to findings

1. Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. After you run an assessment, navigate to the **Findings** page in the Amazon Inspector console to view your findings.

   You can also see your findings in the **Notable Findings** section on the **Dashboard** page of the Amazon Inspector console.

   Note
   You cannot view the findings generated by an assessment run while it is still in progress. However, you can view a subset of findings if you stop the assessment before it completes

its duration. In a production environment, we recommend that you let every assessment run through its entire duration so that it can produce a full set of findings.

3. To view the details of a specific finding, choose the **Expand** widget next to that finding. The details of the finding include the following:

   - Name of the assessment target that includes the EC2 instance where this finding was registered
   - Name of the assessment template that was used to produce this finding
   - Assessment run start time
   - Assessment run end time
   - Assessment run status
   - Name of the rules package that includes the rule that triggered this finding
   - Name of the finding
   - Severity of the finding
   - Description of the finding
   - Recommended steps that you can complete to fix the potential security issue described by the finding

4. To assign attributes to a finding, choose a finding, and then choose **Add/Edit Attributes**.

   You can also assign attributes to findings as you create a new assessment template by configuring the new template to automatically assign attributes to all findings generated by the assessment run. To do this, you can use the **Key** and **Value** fields from the **Tags for findings from this assessment** field. For more information, see Amazon Inspector Assessment Templates and Assessment Runs (p. 24).

Amazon Inspector Rules Packages and Rules

You can use Amazon Inspector to assess your assessment targets (collections of AWS resources) for potential security issues and vulnerabilities. Amazon Inspector compares the behavior and the security configuration of the assessment targets to selected security *rules packages*. In the context of Amazon Inspector, a *rule* is a security check that Amazon Inspector performs during the assessment run.

In Amazon Inspector, rules are grouped together into distinct *rules packages* either by category, severity, or pricing. This gives you choices for the kinds of analysis that you can perform. For example, Amazon Inspector offers a large number of rules that you can use to assess your applications. But you might want to include a smaller subset of the available rules to target a specific area of concern or to uncover specific security problems. Companies with large IT departments might want to determine whether their application is exposed to any security threat, while others might want to concentrate only on issues with the severity level of **High**.

Severity Levels for Rules in Amazon Inspector

Each Amazon Inspector rule has an assigned severity level. This reduces the need to prioritize one rule over another in your analyses. It can also help you determine your response when a rule highlights a potential problem. **High**, **Medium**, and **Low** levels all indicate a security issue that can result in compromised information confidentiality, integrity, and availability within your assessment target. The **Informational** level simply highlights a security configuration detail of your assessment target. Following are recommended ways to respond to each:

- **High** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your assessment target. We recommend that you treat this security issue as an emergency and implement an immediate remediation.
- **Medium** – Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your assessment target. We recommend that you fix this issue at the next possible opportunity, for example, during your next service update.
- **Low** - Describes a security issue that can result in a compromise of the information confidentiality, integrity, and availability within your assessment target. We recommend that you fix this issue as part of one of your future service updates.

- **Informational** – Describes a particular security configuration detail of your assessment target. Based on your business and organization goals, you can either simply make note of this information or use it to improve the security of your assessment target.

Rules Packages in Amazon Inspector

The following are the rule packages available in Amazon Inspector:

Common Vulnerabilities and Exposures

The rules in this package help verify whether the EC2 instances in your assessment targets are exposed to common vulnerabilities and exposures (CVEs). Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference method for publicly known information security vulnerabilities and exposures. For more information, go to https://cve.mitre.org/.

If a particular CVE appears in a *finding* produced by an Amazon Inspector assessment, you can search https://cve.mitre.org/ for the CVE's ID (for example, **`CVE-2009-0021`**). The search results can provide detailed information about this CVE, its severity, and how to mitigate it.

The rules included in this package help you assess whether your EC2 instances are exposed to the CVEs in the following list: https://s3-us-west-2.amazonaws.com/rules-engine/CVEList.txt. The CVE rules package is updated regularly; this list includes the CVEs that are included in assessments runs that occur at the same time that this list is retrieved.

CIS Operating System Security Configuration Benchmarks

The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be viewed here.

Amazon Inspector currently provides the following CIS Certified rules packages to help establish secure configuration postures for the following operating systems:

- Amazon Linux 2015.03 (CIS Benchmark for Amazon Linux 2014.09-2015.03, v1.1.0, Level 1 Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Domain Controller Profile)

If a particular CIS benchmark appears in a finding produced by an Amazon Inspector assessment run, you can download a detailed PDF description of the benchmark from https://benchmarks.cisecurity.org/

(free registration required). The benchmark document provides detailed information about this CIS benchmark, its severity, and how to mitigate it.

Security Best Practices

The rules in this package help determine whether your systems are configured securely.

> **Important**
> In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
> During an assessment run, the rules in all the packages described in this topic generate findings **only** for the EC2 instances that are running Linux-based operating systems. The rules in these packages do NOT generate findings for EC2 instances that are running Windows-based operating systems.

Topics

Disable Root Login over SSH

This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root .

Severity: Medium (p. 30)

Finding

There is an instance in your assessment target that is configured to allow users to log in with root credentials over SSH. This increases the likelihood of a successful brute-force attack.

Resolution

We recommend that you configure your EC2 instance to prevent root account logins over SSH. Instead, log in as a non-root user and use **sudo** to escalate privileges when necessary. To disable SSH root account logins, set **PermitRootLogin** to **no** in **/etc/ssh/sshd_config** and restart sshd.

Support SSH Version 2 Only

This rule helps determine whether your EC2 instances are configured to support SSH protocol version 1.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target is configured to support SSH 1, which contains inherent design flaws that greatly reduce its security.

Resolution

We recommend that you configure EC2 instances in your assessment target to support only SSH 2 and higher. For OpenSSH, you can achieve this by setting **Protocol 2** in **/etc/ssh/sshd_config**. For more information, see **man sshd_config**.

Disable Password Authentication Over SSH

This rule helps determine whether your EC2 instances are configured to support password authentication over the SSH protocol.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target is configured to support password authentication over SSH. Password authentication is susceptible to brute-force attacks and should be disabled in favor of key-based authentication where possible.

Resolution

We recommend that you disable password authentication over SSH on your EC2 instances and enable support for key-based authentication instead. This significantly reduces the likelihood of a successful brute-force attack. For more information, see https://aws.amazon.com/articles/1233/. If password authentication is supported, it is important to restrict access to the SSH server to trusted IP addresses.

Configure Password Maximum Age

This rule helps determine whether the maximum age for passwords is configured on your EC2 instances.

Severity - Medium (p. 30)

Finding

An EC2 instance in your assessment target is not configured for a maximum age for passwords.

Resolution

If you are using passwords, we recommend that you configure a maximum age for passwords on all EC2 instances in your assessment target. This requires users to regularly change their passwords and reduces the chances of a successful password guessing attack. To fix this issue for existing users, use the **chage** command. To configure a maximum age for passwords for all future users, edit the **PASS_MAX_DAYS** field in the **/etc/login.defs** file.

Configure Password Minimum Length

This rule helps determine whether a minimum length for passwords is configured on your EC2 instances.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target is not configured for a minimum length for passwords.

Resolution

If you are using passwords, we recommend that you configure a minimum length for passwords on all EC2 instances in your assessment target. Enforcing a minimum password length reduces the risk of a successful password guessing attack. To enforce minimum password lengths, set the **minlen** parameter of **pam_cracklib.so** in your PAM configuration. For more information, see **man pam_cracklib**.

Configure Password Complexity

This rule helps determine whether a password complexity mechanism is configured on your EC2 instances.

Severity: Medium (p. 30)

Finding

No password complexity mechanism or restrictions are configured on EC2 instances in your assessment target. This allows users to set simple passwords, thereby increasing the chances of unauthorized users gaining access and misusing accounts.

Resolution

If you are using passwords, we recommend that you configure all EC2 instances in your assessment target to require a level of password complexity. You can do this by using **pam_cracklib.so** "lcredit", "ucredit", "dcredit", and "ocredit" settings. For more information, see **man pam_cracklib**.

Enable ASLR

This rule helps determine whether address space layout randomization (ASLR) is enabled on the operating systems of the EC2 instances in your assessment target.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target does not have ASLR enabled.

Resolution

To improve the security of your assessment target, we recommend that you enable ASLR on the operating systems of all EC2 instances in your assessment target by running **echo 2 | sudo tee /proc/sys/kernel/randomize_va_space**.

Enable DEP

This rule helps determine whether Data Execution Prevention (DEP) is enabled on the operating systems of the EC2 instances in your assessment target.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target does not have DEP enabled.

Resolution

We recommend that you enable DEP on the operating systems of all EC2 instances in your assessment target. Enabling DEP protects your instances from security compromises using buffer-overflow techniques.

Configure Permissions for System Directories

This rule checks permissions on system directories that contain binaries and system configuration information to make sure that only the root user (a user who logs in by using root account credentials) has write permissions for these directories.

Severity: High (p. 30)

Finding

An EC2 instance in your assessment target contains a system directory that is writable by non-root users.

Resolution

To improve the security of your assessment target and to prevent privilege escalation by malicious local users, configure all system directories on all EC2 instances in your assessment target to be writable only by users who log in by using root account credentials.

Runtime Behavior Analysis

These rules analyze the behavior of your instances during an assessment run, and provide guidance about how to make your EC2 instances more secure.

Topics

Insecure Client Protocols (Login)

This rule detects a client's use of insecure protocols to log in to remote machines.

> **Important**
> In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
> This rule generates findings for the EC2 instances that are running either Linux-based or Windows-based operating systems.

Severity: Medium (p. 30)

Finding

An EC2 instance in your assessment target uses insecure protocols to connect to a remote host for login. These protocols pass credentials in the clear, increasing the risk of credential theft.

Resolution

It is recommended that you replace these insecure protocols with secure protocols, such as SSH.

Insecure Client Protocols (General)

This rule detects a client's use of insecure protocols.

> **Important**
> In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
> This rule generates findings for the EC2 instances that are running either Linux-based or Windows-based operating systems.

Severity: Low (p. 30)

Finding

An EC2 instance in your assessment target uses insecure protocols to connect to a remote host. These protocols pass traffic in the clear, increasing the risk of a successful traffic interception attack.

Resolution

It is recommended that you replace these insecure protocols with encrypted versions.

Unused Listening TCP Ports

This rule detects listening TCP ports that may not be required by the assessment target.

> **Important**
> In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
> This rule generates findings for the EC2 instances that are running either Linux-based or Windows-based operating systems.

Severity: Informational (p. 30)

Finding

An EC2 instance in your assessment target is listening on TCP ports but no traffic to these ports was seen during the assessment run.

Resolution

To reduce the attack surface area of your deployments, we recommend that you disable network services that you do not use. Where network services are required, we recommend that you employ network control mechanisms such as VPC ACLs, EC2 security groups, and firewalls to limit exposure of that service.

Insecure Server Protocols

This rule helps determine whether your EC2 instances allow support for insecure and unencrypted ports/services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

> **Important**
> In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
> This rule generates findings for the EC2 instances that are running either Linux-based or Windows-based operating systems.

Severity: Informational (p. 30)

Finding

An EC2 instance in your assessment target is configured to support insecure protocols.

Resolution

We recommend that you disable insecure protocols that are supported on an EC2 instance in your assessment target and replace them with secure alternatives as listed below:

- Disable Telnet, rsh, and rlogin and replace them with SSH. Where this is not possible, you should ensure that the insecure service is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups.
- Replace FTP with SCP or SFTP where possible. Where this is not possible, you should ensure that the FTP server is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups.
- Replace HTTP with HTTPS where possible. For more information specific to the web server in question, see http://nginx.org/en/docs/http/configuring_https_servers.html and http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html.
- Disable IMAP, POP3, and SMTP services if not required. If required, we recommend that these email protocols are used with encrypted protocols such as TLS.
- Disable SNMP service if not required. If required, replace SNMP v1and v2 with the more secure SNMP v3, which uses encrypted communication.

Software Without DEP

This rule detects the presence of third-party software that is compiled without support for Data Execution Prevention (DEP). DEP increases system security by defending against stack-based buffer overflow and other memory corruption attacks.

Important
In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
During an assessment run, this rule generates findings **only** for the EC2 instances that are running Linux-based operating systems. This rule does NOT generate findings for EC2 instances that are running Windows-based operating systems.

Severity: Medium (p. 30)

Finding

There are executable files on an EC2 instance in your assessment target that do not support DEP.

Resolution

It is recommended that you uninstall this software from your assessment target if you are not using it, or contact the vendor to get an updated version of this software with DEP enabled.

Software Without Stack Cookies

This rule detects the presence of third-party software that is compiled without support for stack cookies. Stack cookies increase system security by defending against stack-based buffer overflow and other memory corruption attacks.

Important
In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.
During an assessment run, this rule generates findings **only** for the EC2 instances that are running Linux-based operating systems. This rule does NOT generate findings for EC2 instances that are running Windows-based operating systems.

Severity: Medium (p. 30)

Finding

There are executable files running on your EC2 instance that do not support stack cookies.

Resolution

It is recommended that you uninstall this software from your assessment target if you are not using it, or contact the vendor to get an updated version of this software with stack cookies enabled.

Root Process with Insecure Permissions

This rule helps detect root processes that load modules that can be modified by unauthorized users.

Important
In this release of Amazon Inspector, you can include in your assessment targets EC2 instances that are running either Linux-based or Windows-based operating systems.

During an assessment run, this rule generates findings **only** for the EC2 instances that are running Linux-based operating systems. This rule does NOT generate findings for EC2 instances that are running Windows-based operating systems.

Severity: High (p. 30)

Finding

There is an instance in your assessment target with one or more root-owned processes that make use of shared objects that are vulnerable to unauthorized modification. These shared objects have inappropriate permissions/ownership and are therefore vulnerable to tampering.

Resolution

To improve the security of your assessment target, it is recommended that you correct the permissions on the relevant modules to ensure that they are writable only by root.

Logging Amazon Inspector API Calls with AWS CloudTrail

Amazon Inspector is integrated with CloudTrail, a service that captures all the Amazon InspectorAPI calls and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the Amazon Inspector console or from your code to the Amazon Inspector APIs. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Inspector, the source IP address from which the request was made, who made the request, when it was made, and so on.

To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

Amazon Inspector Information in CloudTrail

When CloudTrail logging is enabled in your AWS account, API calls made to Amazon Inspector actions are tracked in CloudTrail log files, where they are written with other AWS service records. CloudTrail determines when to create and write to a new file based on a time period and file size.

All Amazon Inspector actions are logged by CloudTrail and are documented in the Amazon Inspector API Reference.

For example, calls to the **CreateAssessmentTarget**, **CreateAssessmentTemplate** and **StartAssessmentRun** sections generate entries in the CloudTrail log files.

> **Note**
> For the Amazon Inspector integration with CloudTrail, for the List* and Describe* APIs, for example, ListAssessmentTargets or `DescribeAssessmentTargets`, only the request information is logged; for the Create*, Start*, Stop*, and all other APIs, for example, `CreateResourceGroup`, both the request and response information is logged.

Every log entry contains information about who generated the request. The user identity information in the log entry helps you determine the following:

- Whether the request was made with root or IAM user credentials
- Whether the request was made with temporary security credentials for a role or federated user
- Whether the request was made by another AWS service

For more information, see the CloudTrail userIdentity Element.

You can store your log files in your Amazon S3 bucket for as long as you want, but you can also define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted with Amazon S3 server-side encryption (SSE).

If you want to be notified upon log file delivery, you can configure CloudTrail to publish Amazon SNS notifications when new log files are delivered. For more information, see Configuring Amazon SNS Notifications for CloudTrail.

You can also aggregate Amazon Inspector log files from multiple AWS regions and multiple AWS accounts into a single Amazon S3 bucket.

For more information, see Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts.

Understanding Amazon Inspector Log File Entries

CloudTrail log files can contain one or more log entries. Each entry lists multiple JSON-formatted events. A log entry represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. Log entries are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the Amazon Inspector `CreateResourceGroup` action:


```
{
"eventVersion": "1.03",
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2016-04-14T17:05:54Z"
        },
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::444455556666:user/Alice",
            "accountId": "444455556666",
            "userName": "Alice"
        }
    }
},
"eventTime": "2016-04-14T17:12:34Z",
"eventSource": "inspector.amazonaws.com",
"eventName": "CreateResourceGroup",
"awsRegion": "us-west-2",
"sourceIPAddress": "205.251.233.179",
```

```
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
       "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resource
group/0-oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

From this event information, you can determine that the request was made to create a new resource group (using the Amazon Inspector `CreateResourceGroup` API) with the tag key-value pair of `Name` and `ExampleEC2Instance` to identify the EC2 instance to be included in the new resource group. You can also see that the request was made by an IAM user named `Alice` on April 14, 2016.

The following example shows a CloudTrail log entry that demonstrates the Amazon Inspector `DescribeAssessmentTargets` action:

```
    {
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
      "eventTime": "2016-04-14T17:30:49Z",
      "eventSource": "inspector.amazonaws.com",
      "eventName": "DescribeAssessmentTargets",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "205.251.233.179",
      "userAgent": "console.amazonaws.com",
```

```
    "requestParameters": {
      "assessmentTargetArns": [
        "arn:aws:inspector:us-west-2:444455556666:target/0-ABcQzlXc",
        "arn:aws:inspector:us-west-2:444455556666:target/0-nvgVhaxX"
      ]
    },
    "responseElements": null,
    "requestID": "a103f654-0266-11e6-93e6-890abdd45f56",
    "eventID": "bd7de684-2b2f-4d45-8cef-d22bf17bcb13",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
  },
```

From this event information, you can determine that the request was made to describe two assessment targets with corresponding ARNs of arn:aws:inspector:us-west-2:444455556666:target/0-ABcQzlXc and arn:aws:inspector:us-west-2:444455556666:target/0-nvgVhaxX (using the Amazon Inspector `DescribeAssessmentTargets` API). You can also see that the request was made by an IAM user named `Alice` on April 14, 2016. Note that per the Amazon Inspector implementation of the integration with CloudTrail, because this is a List* API, only the request information is logged (the ARNs to specify the assessment targets to be described). The list of response elements is not logged and left null.