Amazon Inspector

User Guide

Version Latest

Amazon Inspector: User Guide

Table of Contents

What Is Amazon Inspector?

Amazon Inspector tests the network accessibility of your Amazon EC2 instances and the security state of your applications that run on those instances. Amazon Inspector assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings that is organized by level of severity.

With Amazon Inspector, you can automate security vulnerability assessments throughout your development and deployment pipelines or for static production systems. This allows you to make security testing a regular part of development and IT operations.

Amazon Inspector also offers predefined software called an *agent* that you can optionally install in the operating system of the EC2 instances that you want to assess. The agent monitors the behavior of the EC2 instances, including network, file system, and process activity. It also collects a wide set of behavior and configuration data (telemetry).

Important
AWS doesn't guarantee that following the provided recommendations will resolve every potential security issue. The findings generated by Amazon Inspector depend on your choice of rules 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 the services offered in the AWS Cloud. This infrastructure consists of 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 information about Amazon Inspector terminology, see Amazon Inspector Terminology and Concepts (p. 2).

Benefits of Amazon Inspector

Here are some of the main benefits of Amazon Inspector:

- **Integrate automated security checks into your regular deployment and production processes** – Assess the security of your AWS resources for forensics, troubleshooting, or active auditing purposes. Run the assessments during the development process, or run them in a stable production environment.
- **Find application security issues** – Automate the security assessment of your applications and proactively identify vulnerabilities. This allows you to develop and iterate on new applications quickly, and assess compliance with best practices and policies.
- **Gain a deeper understanding of your AWS resources** – Stay informed about the activity and configuration data of your AWS resources by reviewing the findings that Amazon Inspector produces.

Features of Amazon Inspector

Here are some of the main features of Amazon Inspector:

- **Configuration scanning and activity monitoring engine** – Amazon Inspector provides an agent that analyzes system and resource configuration. It also 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 target and its potential security or compliance issues.

- **Built-in content library** – Amazon Inspector includes a built-in library of rules and reports. These include checks against best practices, common compliance standards, and vulnerabilities. The checks include detailed recommended steps for resolving potential security issues.
- **Automation through an API** – Amazon Inspector can be fully automated through an API. This allows you 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 pricing is based on the number of EC2 instances included in each assessment and the rules packages used in those assessments. For more 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 that lets you 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. These include 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 run commands at your system's command line to perform Amazon Inspector tasks. The command line tools are also useful if you want to build scripts that perform AWS tasks. For more information, see the Amazon Inspector 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.

Amazon Inspector agent

A software agent that you can install on the Amazon EC2 instances that are included in the assessment target. The agent monitors the behavior of the EC2 instances, including network,

file system, and process activity. It also collects a wide set of behavior and configuration data (telemetry). For more information, see Amazon Inspector Agents (p. 20).

Assessment run

The process of discovering potential security issues through the analysis of your assessment target's configuration and behavior against specified rules packages. During an assessment run, Amazon Inspector monitors, collects, and analyzes behavioral data (telemetry) within the specified target. This includes the use of secure channels, network traffic among running processes, and details of communication with AWS services. Next, Amazon Inspector analyzes the data and compares it against a set of security rules packages that are specified in the assessment template used during the assessment run. A completed assessment run produces a list of findings, which are potential security issues of various levels of severity. For more information, see Amazon Inspector Assessment Templates and Assessment Runs (p. 50).

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.

> **Important**
> Currently, your Amazon Inspector assessment targets can consist only of EC2 instances. For more information, see Amazon Inspector Service Limits (p. 4)

To create an Amazon Inspector assessment target, you must first tag your EC2 instances with key-value pairs of your choice. Next, you can create a view of these tagged EC2 instances that have common keys or common values. For more information, see Amazon Inspector Assessment Targets (p. 34).

Assessment template

A configuration that is used during your assessment run. The template includes the following:

- Rules packages that Amazon Inspector uses to evaluate your assessment target
- Amazon SNS topics that you want Amazon Inspector to send notifications to about assessment run states and findings
- Tags (key-value pairs) that you can assign to findings that are generated by the assessment run
- The duration of the assessment run

Finding

A potential security issue that Amazon Inspector discovers during an assessment run of the specified target. Findings are displayed in the Amazon Inspector console or retrieved through the API. They 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. 56).

Rule

In the context of Amazon Inspector, a security check performed 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. 37).

Telemetry

EC2 instance data (behavioral, configuration, and so on), such as records of network connections and process creations. Amazon Inspector collects the data during an assessment run.

Amazon Inspector Service Limits

The following table shows the Amazon Inspector limits for an AWS account.

Important
Currently, your assessment targets can consist only of EC2 instances.

The following are Amazon Inspector limits per AWS account per region:

Resource	Default Limit	Comments
Instances in running assessments	500	The maximum number of EC2 instances that can be included across all running assessments per account per region.
Assessment runs	50000	The maximum number of assessment runs that you can create per account per region. 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.
Assessment Templates	500	The maximum number of assessment templates that you can have at any given time per account per region.
Assessment Targets	50	The maximum number of assessment targets that you can have at any given time per account per region.

Unless otherwise noted, these limits can be increased upon request by contacting the AWS Support Center.

Amazon Inspector Supported Operating Systems and Regions

This chapter provides information about the operating systems and AWS Regions that Amazon Inspector supports.

Important
Currently, Amazon Inspector assessment targets can consist only of EC2 instances. You can run an agentless assessment with the Network Reachability (p. 38) rules package on any EC2 instances regardless of operating system.

For information about the Amazon Inspector rules packages that are available across supported operating systems, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

Topics

Supported Linux-based Operating Systems for the Amazon Inspector Agent

You can use the Amazon Inspector agent only on EC2 instances that run the 64-bit x86 version of the following Linux-based operating systems:

- Amazon Linux 2 (LTS, 2017.12)
- Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
- Ubuntu (18.04 LTS, 16.04 LTS, 14.04 LTS)
- Debian (9.0 - 9.5, 8.0 - 8.7)
- Red Hat Enterprise Linux (7.2 - 7.6, 6.2 - 6.9)
- CentOS (7.2 - 7.6, 6.2 - 6.9)

Amazon Inspector does not yet support Amazon EC2 A1 (Arm) instances.

Important
The following list contains all kernel versions that are compatible with an Amazon Inspector agent running on Linux, Ubuntu, Red Hat Enterprise Linux, and CentOS: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json.
You can run a successful assessment of an EC2 instance with a Linux-based OS using either the CVE (p. 41), CIS (p. 41), or Security Best Practices (p. 46) rules packages. The assessment is successful even if your instance doesn't have a kernel version that is included in this list.
To run a successful assessment of an EC2 instance with a Linux-based OS using the Runtime Behavior Analysis (p. 43) rules package, your instance must have a kernel version that is included in this list. If your instance has a kernel version that is not compatible with the agent, the Runtime Behavior Analysis rules package that assesses the EC2 instance results in only one finding. The finding informs you that the kernel version of your EC2 instance is not supported.

Supported Windows-based Operating Systems for the Amazon Inspector Agent

You can use the Amazon Inspector agent only on EC2 instances that run the 64-bit version of the following Windows-based operating systems:

- Windows Server 2008 R2
- Windows Server 2012

- Windows Server 2012 R2
- Windows Server 2016 Base

Supported AWS Regions

Amazon Inspector is supported in the following AWS Regions:

- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- EU (Frankfurt)
- EU (Ireland)
- US East (Northern Virginia)
- US East (Ohio)
- US West (Northern California)
- US West (Oregon)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Note
The Network Reachability (p. 38) rules package is not available in the AWS GovCloud (US) Regions.

Getting Started with Amazon Inspector

This tutorial shows you how to set up Amazon Inspector and get started by creating and running your first assessment.

Important
To use Amazon Inspector, you must have an AWS account. When you sign up for AWS, your 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 https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   If you previously signed in to the AWS Management Console using AWS account root user credentials, choose **Sign in to a different account**. If you previously signed in to the console using IAM credentials, choose **Sign-in using root account credentials**. Then choose **Create a new AWS account**.

2. Follow the online instructions.

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

Topics

Prerequisites for Using Amazon Inspector

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 perform an Amazon Inspector assessment run:

- You must have at least one Amazon EC2 instance running in your AWS environment to run an Amazon Inspector assessment. For information about launching EC2 instances, see the Amazon Elastic Compute Cloud Documentation.
- In most cases, the Amazon Inspector agent must be running on each EC2 instance in your assessment target. For information about installing an agent, see Installing Amazon Inspector Agents (p. 22). Alternatively, you can use Systems Manager Run Command to install the agent on your Amazon EC2 instances. For more information about Amazon Inspector agents, see Amazon Inspector Agents (p. 20).

One-Click Setup

The following procedure shows you how to create and run an automatic assessment using a pre-built template and pre-defined scheduling parameters (once a week or one time only) on all available EC2 instances in the current AWS account and Region.

1. Sign in to the AWS Management Console and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. On the **Welcome** page, choose the type of assessment that you would like to run. **Network Assessments** analyze the network configurations of your AWS environment for vulnerabilities, and do not require an Amazon Inspector agent. **Host Assessments** analyze the on-host software and configurations of your EC2 instances for vulnerabilities, and requires an agent to be installed on the EC2 instances.

   Choose either **Run weekly (recommended)** or **Run once**. As soon as you make your choice, the service automatically creates the assessment for you. Specifically, the service does the following:

   a. Creates a service-linked role (p. 17).

      Note
      To identify the EC2 instances that are specified in the assessment targets, Amazon Inspector needs to enumerate your EC2 instances and tags. Amazon Inspector gets access to these resources in your AWS account through a service-linked role called `AWSServiceRoleForAmazonInspector`. For more information about service-linked roles, see Using Service-Linked Roles for Amazon Inspector (p. 17) and Using Service-Linked Roles.

   b. If applicable, installs an Amazon Inspector agent (p. 20) on all available Amazon EC2 instances in your AWS account and AWS Region.

      Note
      The service installs an Amazon Inspector agent only on those EC2 instances that allow AWS Systems Manager Run Command. To use this option, make sure that all of your EC2 instances in the current AWS account and AWS Region have the SSM Agent installed and have an IAM role that allows Run Command. For more information, see Installing the Agent on Multiple EC2 Instances Using the Systems Manager Run Command (p. 23).

   c. Adds those instances to an assessment target (p. 34).

   d. Includes that target in an assessment template (p. 50) with a standardized set of rules packages.

   e. Runs the assessment weekly or only once, depending on whether you chose **Run weekly (recommended)** or **Run once**.
3. In the **Confirmation** dialog box, choose **OK**. Amazon Inspector automatically runs your assessment.

Advanced Setup

The following procedure shows you how to choose specific Amazon EC2 instances, rules packages, and scheduling parameters to include in an assessment target and template.

1. On the **Welcome** page, choose **Advanced setup**.
2. On the **Define an assessment target** page, enter the name of your assessment target.
3. For **All Instances**, you can keep the check box selected to include all EC2 instances in your AWS account and Region in the assessment target. If you want to choose which EC2 instances to include, clear the **All Instances** check box, and enter the **Key** and **Value** tags that are associated with the target EC2 instances. For more information about tagging your EC2 instances, see Tagging Your Amazon EC2 Resources.
4. For **Install Agents**, you can keep the check box selected by default if your instances allows System Manager Run Command. The service installs an Amazon Inspector agent on all EC2 instances in the assessment target that allow System Manager Run Command. To use this option, make sure that all of your EC2 instances in the current AWS account and AWS region have the SSM Agent installed and have an IAM role that allows Run Command. For more information, see Installing the Agent

on Multiple EC2 Instances Using the Systems Manager Run Command (p. 23). If you want to manually install the agent, see Installing Amazon Inspector Agents (p. 22).

5. Choose **Next**.
6. On the **Define an assessment template** page, enter the name of your assessment template.
7. For **Rules packages**, choose the rules packages to include in the assessment template. For more information about rules packages, see Amazon Inspector Rules Packages and Rules (p. 37).
8. For **Duration**, choose the duration of your assessment run.
9. For **Assessment Schedule**, you can set a schedule for recurring assessment runs.
10. Choose **Next**.
11. On the **Review** page, review your choices for the assessment target and template. If you are satisfied with the configuration, choose **Create**. If you set an assessment schedule for your assessment template, the assessment automatically runs after you choose **Create**.

    Note
    To identify the EC2 instances that are specified in the assessment targets, Amazon Inspector needs to enumerate your EC2 instances and tags. Amazon Inspector gets access to these resources in your AWS account through a service-linked role called `AWSServiceRoleForAmazonInspector`. For more information about service-linked roles, see Using Service-Linked Roles for Amazon Inspector (p. 17) and Using Service-Linked Roles.
12. If you didn't set up an assessment schedule, navigate to your assessment template through the console, and then choose **Run**.
13. To track the progress of the assessment run, in the navigation pane of the console, choose **Assessment runs**, and then choose **Findings**. For more information about findings, see *Amazon Inspector Findings* (p. 56).

Tutorials for Amazon Inspector

The following tutorials show you how to perform Amazon Inspector assessment runs on the Red Hat Enterprise Linux and Ubuntu operating systems.

Tutorials

Amazon Inspector Tutorial - Red Hat Enterprise Linux

Before you follow the instructions in this tutorial, we recommend that you get familiar with the Amazon Inspector Terminology and Concepts (p. 2).

This tutorial shows how to use Amazon Inspector to analyze the behavior of an EC2 instance that runs the Red Hat Enterprise Linux 7.5 operating system. It provides step-by-step instructions on how to navigate the Amazon Inspector workflow. The workflow includes preparing Amazon EC2 instances, running an assessment template, and performing the recommended security fixes generated in the assessment's findings. If you are a first-time user and would like to set up and run an Amazon Inspector assessment with one click, see Creating a Basic Assessment (p. 7).

Topics

Step 1: Set Up an Amazon EC2 Instance to Use With Amazon Inspector

For this tutorial, create one EC2 instance that runs Red Hat Enterprise Linux 7.5, and tag it using the **Name** key and a value of **`InspectorEC2InstanceLinux`**.

> **Note**
> For more information about tagging EC2 instances, see Resources and Tags.

Step 2: Modify Your Amazon EC2 Instance

For this tutorial, you modify your target EC2 instance to expose it to the potential security issue CVE-2018-1111. For more information, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 and Common Vulnerabilities and Exposures (p. 41).

Connect to your instance, **`InspectorEC2InstanceLinux`**, and run the following command:

```
sudo yum install dhclient-12:4.2.5-68.el7
```

For instructions on how to connect to an EC2 instance, see Connect to Your Instance in the *Amazon EC2 User Guide*.

Step 3: Create an Assessment Target and Install an Agent on the EC2 Instance

Amazon Inspector uses assessment targets to designate the AWS resources that you want to evaluate.

To create an assessment target and install an agent on an EC2 instance

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**.

   Do the following:

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

      For this tutorial, enter **`MyTargetLinux`**.

   b. For **Use Tags**, choose the EC2 instances that you want to include in this assessment target by entering values for the **Key** and **Value** fields.

      For this tutorial, choose the EC2 instance that you created in the preceding step by entering **`Name`** in the **Key** field and **`InspectorEC2InstanceLinux`** in the **Value** field.

      To include all EC2 instances in your AWS account and Region in the assessment target, select the **All Instances** check box.

   c. Choose **Save**.

   d. Install an Amazon Inspector agent on your tagged EC2 instance. To install an agent on all EC2 instances included in an assessment target, select the **Install Agents** check box.

      Note
      You can also install the Amazon Inspector agent using the AWS Systems Manager Run Command (p. 23). To install the agent on all instances in the assessment target, you can specify the same tags that you used when creating the assessment target. Or you can install the Amazon Inspector agent on your EC2 instance manually. For more information, see Installing Amazon Inspector Agents (p. 22).

   e. Choose **Save**.

   Note
   At this point, Amazon Inspector creates a service-linked role called `AWSServiceRoleForAmazonInspector`. The role grants Amazon Inspector the necessary access to your resources. For more information, see Creating a Service-Linked Role for Amazon Inspector (p. 17).

Step 4: Create and Run Your Assessment Template

To create and run your template

1. In the navigation pane, choose **Assessment templates**, and then choose **Create**.
2. For **Name**, enter the name for your assessment template. For this tutorial, enter **`MyFirstTemplateLinux`**.

3. For **Target name**, choose the assessment target that you created above, **`MyTargetLinux`**.
4. For **Rules packages**, choose the rules packages that you want to use in this assessment template.

   For this tutorial, choose **Common Vulnerabilities and Exposures-1.1**.
5. For **Duration**, specify the duration for your assessment template.

   For this tutorial, select **15 minutes**.
6. Choose **Create and run**.

Step 5: Locate and Analyze Your Finding

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

In this tutorial, if you complete the preceding steps, your assessment run produces a finding against the common vulnerability CVE-2018-1111.

To locate and analyze your finding

1. In the navigation pane, choose **Assessment runs**. Verify that the status of the run for the assessment template called **MyFirstTemplateLinux** 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 can't view the findings generated by the assessment run while it is still in progress. Let the assessment run complete its entire duration. However, for this tutorial, you can stop the run after several minutes.

   The status of **MyFirstTemplateLinux** changes first to **Stopping**, then in a few minutes to **Analyzing**, and then finally to **Analysis complete**. To see this change in status, choose the **Refresh** icon.
3. In the navigation pane, choose **Findings**.

   You can see a new finding of **High** severity called **Instance InspectorEC2InstanceLinux is vulnerable to CVE-2018-1111**.

   > **Note**
   > If you don't 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:

   - ARN of the finding
   - Name of the assessment run that produced this finding
   - Name of the assessment target that produced this finding
   - Name of the assessment template that produced 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
   - Amazon Inspector agent ID
   - Name of the finding
   - Severity of the finding
   - Description of the finding

- Recommended remediation steps that you can complete to fix the potential security issue described by the finding

Step 6: Apply the Recommended Fix to Your Assessment Target

For this tutorial, you modified your assessment target to expose it to the potential security issue CVE-2018-1111. In this procedure, you apply the recommended fix for the issue.

To apply the fix to your target

1. Connect to your instance **`InspectorEC2InstanceLinux`** that you created in the preceding section, and run the following command:

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```
2. On the **Assessment templates** page, choose **MyFirstTemplateLinux**, and then choose **Run** to start a new assessment run using this template.
3. Follow the steps in Step 5: Locate and Analyze Your Finding (p. 12) to see the findings that result from this subsequent run of the **MyFirstTemplateLinux** template.

   Because you resolved the CVE-2018-1111 security issue, you should no longer see a finding for it.

Amazon Inspector Tutorial - Ubuntu Server

Before you follow the instructions in this tutorial, we recommend that you get familiar with the Amazon Inspector Terminology and Concepts (p. 2).

This tutorial shows how to use Amazon Inspector to analyze the behavior of an EC2 instance that runs the Ubuntu Server 16.04 LTS operating system. It provides step-by-step instructions on how to navigate the Amazon Inspector workflow. This includes preparing an Amazon EC2 instance, to running an assessment template, to performing a recommended security fix generated in the assessment's findings.

If you are a first-time user and would like to set up and run an Amazon Inspector assessment with one click, see Creating a Basic Assessment (p. 7).

Topics

Step 1: Set Up an Amazon EC2 Instance to Use With Amazon Inspector

To set up an EC2 instance

- For this tutorial, create one EC2 instance running Ubuntu Server 16.04 LTS and tag it using the **Name** key and a value of **`InspectorEC2InstanceUbuntu`**.

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

Step 2: Modify Your Amazon EC2 Instance

For this tutorial, you modify your target EC2 instance to expose it to the potential security issue CVE-2017-6507. For more information, see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6507 and Common Vulnerabilities and Exposures (p. 41).

To modify your EC2 instance

- Connect to your instance **`InspectorEC2InstanceUbuntu`** that you created in the preceding section, and run the following command:

  ```
  sudo apt-get install apparmor=2.10.95-0ubuntu2.5
  ```

Step 3: Create an Assessment Target and Install an Agent on the EC2 Instance

Amazon Inspector uses assessment targets to designate the AWS resources to evaluate.

To create an assessment target and install an agent on the EC2 instance

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**, enter the name for your assessment target.

   For this tutorial, type **`MyTargetUbuntu`**.
4. For **Use Tags**, choose the EC2 instances that you want to include in this assessment target by entering values for the **Key** and **Value** fields.

   For this tutorial, choose the EC2 instance that you created in the preceding step by entering **`Name`** in the **Key** field and **`InspectorEC2InstanceUbuntu`** in the **Value** field.

   To include all EC2 instances in your AWS account and Region in the assessment target, select the **All Instances** box.
5. Install an Amazon Inspector Agent on your tagged EC2 instance. To install an agent on all EC2 instances included in an assessment target, select the **Install Agents** box.

   Note
   You can also install the Amazon Inspector Agent using the Systems Manager Run Command (p. 23). To install the agent on all instances in the assessment target, you can specify the same tags used for creating the assessment target. Or you can install the Amazon Inspector Agent on your EC2 instance manually. For more information, see Installing Amazon Inspector Agents (p. 22).
6. Choose **Save**.

   Note
   At this point, a service-linked role called `AWSServiceRoleForAmazonInspector` is created to grant Amazon Inspector access to your resources. For more information, see Creating a Service-Linked Role for Amazon Inspector (p. 17).

Step 4: Create and Run Your Assessment Template

To create and run your template

1. If you are using **Advanced setup**, you are directed to the **Define an assessment template** page. Otherwise, navigate to the **Assessment templates** page, and then choose **Create**.
2. For **Name**, enter the name for your assessment template. For this tutorial, enter **`MyFirstTemplateUbuntu`**.
3. For **Target name**, choose the assessment target that you created above, **`MyTargetUbuntu`**.
4. For **Rules packages**, use the dropdown menu to choose the rules packages that you want to use in this assessment template.

   For this tutorial, choose **Common Vulnerabilities and Exposures-1.1**.
5. For **Duration**, specify the duration for your assessment template.

   For this tutorial, choose **15 minutes**.
6. If you are using **Advanced setup**, choose **Next**. On the following **Review** page, choose **Create**. Otherwise, choose **Create and run**.

Step 5: Locate and Analyze Generated Findings

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

In this tutorial, if you completed the preceding steps, your assessment run produces a finding against the common vulnerability **CVE-2017-6507**.

1. Navigate to the **Assessment Runs** page. Verify that the status of the run for the assessment template called **MyFirstTemplateUbuntu** 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 can't view the findings generated by the assessment run while it is still in progress. Let the assessment run complete its entire duration.

   The status of **MyFirstTemplateUbuntu** changes first to **Stopping**, then in a few minutes to **Analyzing**, and then finally to **Analysis complete**. To see this change in status, choose the **Refresh** icon.
3. Navigate to the **Findings** page.

   You can see a new finding of **High** severity called **Instance InspectorEC2InstanceUbuntu is vulnerable to CVE-2017-6507**.

   > **Note**
   > If you don't 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:

   - ARN of the finding
   - Name of the assessment run that produced this finding
   - Name of the assessment target that produced this finding
   - Name of the assessment template that produced 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
- Amazon Inspector agent ID
- Name of the finding
- Severity of the finding
- Description of the finding
- Recommended remediation steps that you can complete to fix the potential security issue described by the finding

Step 6: Apply the Recommended Fix to Your Assessment Target

For this tutorial, you modified your assessment target to expose it to a potential security issue **CVE-2017-6507**. In this procedure, you apply the recommended fix for the issue.

1. Connect to your instance **`InspectorEC2InstanceUbuntu`**, and run the following command:

   ```
   sudo apt-get install apparmor=2.10.95-0ubuntu2.6
   ```
2. On the **Assessment templates** page, choose **MyFirstTemplateUbuntu**, and then choose **Run** to start a new run using this template.
3. Follow the steps in Step 5: Locate and Analyze Generated Findings (p. 15) to see the findings that result from this subsequent run of the **MyFirstTemplateUbuntu** template.

   Because you resolved the **CVE-2017-6507** security issue, you should no longer see a finding for it.

Using Service-Linked Roles for Amazon Inspector

Amazon Inspector uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Inspector. Service-linked roles are predefined by Amazon Inspector and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon Inspector easier because you don't have to manually add the necessary permissions. Amazon Inspector defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Inspector can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy can't be attached to any other IAM entity.

You can delete a service-linked role only after first deleting your assessment targets for an AWS account in all the Regions where you have Amazon Inspector running.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-Linked Role Permissions for Amazon Inspector

Amazon Inspector uses the service-linked role named `AWSServiceRoleForAmazonInspector`. The`AWSServiceRoleForAmazonInspector` service-linked role trusts Amazon Inspector to assume the role.

The permissions policy of the role allows Amazon Inspector to complete the following action on the specified resources:

- Action: `iam:CreateServiceLinkedRole` on `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

For the `AWSServiceRoleForAmazonInspector` role to be successfully created, the IAM identity (user, role, or group) that you use when you work with Amazon Inspector must have the required permissions. To grant the required permissions, attach the `AmazonInspectorFullAccess` managed policy to the IAM user, group, or role. For more information about the managed policy, see AWS Managed (Predefined) Policies for Amazon Inspector (p. 81).

For more information about service-linked roles, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a Service-Linked Role for Amazon Inspector

You don't need to manually create the `AWSServiceRoleForAmazonInspector` service-linked role.

The `AWSServiceRoleForAmazonInspector` service-linked role is created automatically, but you might need to do some minimal setup first. The following sections describe the details of setting up and using the `AWSServiceRoleForAmazonInspector` service-linked role.

If You Are Getting Started with Amazon Inspector for the First Time

- The `AWSServiceRoleForAmazonInspector` service-linked role is created automatically when you go through the **Get Started with Amazon Inspector** wizard on the console or when you run the CreateAssessmentTarget API operation.
- The `AWSServiceRoleForAmazonInspector` service-linked role is created for your AWS account only in the Region that you are currently signed in to. It grants Amazon Inspector access to the resources in your AWS account only in that Region. If you then use the same AWS account to go through the **Get Started with Amazon Inspector** console wizard or run the CreateAssessmentTarget API operation in other Regions, the same service-linked role that is already created in your AWS account is applied in these other Regions and grants Amazon Inspector access to the resources in your AWS account in those Regions.

If You Already Have Amazon Inspector Running in Your AWS Account

- If you already have Amazon Inspector running in your AWS account, the IAM role that grants Amazon Inspector access to your resources already exists in your AWS account. In this case, the `AWSServiceRoleForAmazonInspector` service-linked role is autogenerated when you create an assessment target or an assessment template (either through the Amazon Inspector console or the API operations). This newly created service-linked role replaces the previously created IAM role that up until now granted Amazon Inspector access to your resources.

  You can also create the `AWSServiceRoleForAmazonInspector` service-linked role manually by choosing the **Manage Amazon Inspector service-linked role** link in the **Accounts Setting** section on the Amazon Inspector **Dashboard** page. This newly created service-linked role replaces the previously created IAM role that up until now granted Amazon Inspector access to your resources.

  Note
  This previously created IAM role is not deleted. It remains intact, but it is no longer used to grant Amazon Inspector access to your resources. You can use the IAM console to further manage or delete this IAM role.
- The `AWSServiceRoleForAmazonInspector` service-linked role is created for your AWS account only in the Region that you are currently signed in to. It grants Amazon Inspector access to the resources in your AWS account only in this Region. If you then use the same AWS account to create an assessment target or an assessment template for your Amazon Inspector service running in other Regions, the same service-linked role that is already created in your AWS account is applied. It grants Amazon Inspector access to the resources in your AWS account in those regions.

You can also use the IAM console to create an Inspector service-linked role. In the IAM CLI or the IAM API, create a service-linked role with the `Amazon Inspector` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you Get started with Amazon Inspector again, the service-linked role is automatically created for you again.

Editing a Service-Linked Role for Amazon Inspector

Amazon Inspector does not allow you to edit the `AWSServiceRoleForAmazonInspector` service-linked role. After you create a service-linked role, you can't change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a Service-Linked Role for Amazon Inspector

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note
If the Amazon Inspector service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Amazon Inspector resources used by `AWSServiceRoleForAmazonInspector`

- Delete your assessment targets for this AWS account in all the Regions where you have Amazon Inspector running. For more information, see Amazon Inspector Assessment Targets (p. 34).

To manually delete the service-linked role using IAM

Use the IAM console, the IAM CLI, or the IAM API to delete the `AWSServiceRoleForAmazonInspector` service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Amazon Inspector Agents

To fully assess the security of the EC2 instances that make up your Amazon Inspector assessment targets, you can install the Amazon Inspector agent on each instance. The agent monitors the behavior (including network, file system, and process activity) of the instance. It also collects behavior and configuration data (telemetry).

For more information about how to install, uninstall, and reinstall the agent, how to verify whether the installed agent is running, and how to configure proxy support for the agent, see Working with Amazon Inspector Agents on Linux-based Operating Systems (p. 25) and Working with Amazon Inspector Agents on Windows-based Operating Systems (p. 27).

Note
An Amazon Inspector agent is not required to run the Network Reachability (p. 38) rules package.

Amazon Inspector Agent Privileges

You must have administrative or root permissions to install the Amazon Inspector agent. On supported Linux-based operating systems, the 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. The agent also includes a kernel mode driver that is required for the agent to function.

Important
The following list contains all kernel versions that are compatible with the Amazon Inspector agent running on Linux, Ubuntu, Red Hat Enterprise Linux, and CentOS: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json.
You can run an Amazon Inspector assessment of an EC2 instance with a Linux-based OS using either the CVE (p. 41), CIS (p. 41), or Security Best Practices (p. 46) rules packages. The assessment is successful even if your instance doesn't have a kernel version that is included in the list.
To run a successful assessment of an EC2 instance with a Linux-based OS using the Runtime Behavior Analysis (p. 43) rules package, your instance must have a kernel version that is included in the list. If your instance has a kernel version that is not compatible with the agent, the Runtime Behavior Analysis (p. 43) rules package that assesses the EC2 instance results in only one finding. The finding informs you that the kernel version of your EC2 instance is not supported.

Network and Amazon Inspector Agent Security

The Amazon Inspector agent initiates all communication with the Amazon Inspector service. This means that the agent must have an outbound network path to a public endpoint so that it can send telemetry data to the endpoint. For example, the agent might be `arsenal.<region>.amazonaws.com`, and the endpoint might be an Amazon S3 bucket at `s3.dualstack.aws-region.amazonaws.com`. (Make sure to replace `<region>` with the actual AWS Region where you are running Amazon Inspector.) For more information, see AWS IP Address Ranges. Because 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 agent periodically communicates with Amazon Inspector over a TLS-protected channel that 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. When 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 they tell the agent to enable or disable specific preconfigured sensors in the agent. Each instruction action is predefined within the agent. Arbitrary instructions can't 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 doesn't make changes to the system that it collects data from. After the agent collects the telemetry data, it sends the data back to 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. Currently, there is no method exposed for intercepting and examining telemetry data at the agent.

Amazon Inspector Agent Updates

As updates for the Amazon Inspector agent become available, they are automatically downloaded from Amazon S3 and applied. This also updates any required dependencies. The auto-update feature 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) is 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 before installation. The auto-update process is executed only during non-assessment periods. If any errors are detected, the update process can rollback and retry the update. Finally, the agent update process serves to upgrade only the agent capabilities. None of your specific information is ever sent from the agent to Amazon Inspector as part of the update workflow. The only information that is communicated as part of the update process is the basic installation success or fail telemetry and, if applicable, any update failure diagnostic information.

Telemetry Data Lifecycle

The telemetry data that is generated by the Amazon Inspector agent during assessment runs is formatted in JSON files. The files are delivered in near-real-time over TLS to Amazon Inspector, where they are encrypted with a per-assessment-run, ephemeral KMS-derived key. The files are securely stored in an Amazon S3 bucket this is 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 that is stored in S3 is retained only to allow for assistance with support requests. It isn't used or aggregated by Amazon for any other purpose. After 30 days, telemetry data is permanently deleted according to a standard S3 bucket lifecycle policy for Amazon Inspector data. Currently, 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, Amazon Inspector accesses your AWS accounts and resources only when it needs to find EC2 instances to assess by querying for tags. It does this through standard IAM access through

the role created during the initial setup of the Amazon Inspector service. During an assessment, all communications with your environment are initiated by the Amazon Inspector agent that is installed locally on EC2 instances. The Amazon Inspector service objects that are created, such as assessment targets, assessment templates, and findings generated by the service, are stored in a database managed by and accessible only to Amazon Inspector.

Amazon Inspector Agent Limits

For information about Amazon Inspector agent limits, see Amazon Inspector Service Limits (p. 4).

Amazon Inspector Agent Public Licensing

The Amazon Inspector agent uses a kernel module (`amznmon64`) as a component of the overall agent. This kernel module uses a general public license (GPLv2). The module source code and licensing information are publicly available and can be accessed here:

- Source code: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz
- Signature file: https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz.sig

Installing Amazon Inspector Agents

You can install the Amazon Inspector agent using the Systems Manager Run Command on multiple instances (including both Linux-based and Windows-based instances). Alternatively, you can install the agent individually by signing in to each EC2 instance. The procedures in this chapter provide instructions for both methods.

As another option, you can quickly install the agent on all Amazon EC2 instances included in an assessment target by selecting the **Install Agents** check box on the **Define an Assessment target** page on the console.

Topics

> **Note**
> The procedures in this chapter apply to all AWS Regions that are supported by Amazon Inspector.

Amazon Linux AMI with the Amazon Inspector Agent

To skip the manual Amazon Inspector agent installation on the Amazon Linux EC2 instances that you want to include in your assessment targets, you can use the **Amazon Linux AMI with Amazon Inspector Agent**. This AMI has the agent preinstalled and requires no additional steps to install or set up the agent. To start using Amazon Inspector with these EC2 instances, tag them to match the assessment target that

you want. The configuration of **Amazon Linux AMI with Amazon Inspector Agent** enhances security by focusing on two main security goals: limiting access and reducing software vulnerabilities.

This is the only currently available EC2 instance AMI with the preinstalled Amazon Inspector agent. For the EC2 instances that run Ubuntu Server or Windows Server, you must complete the manual agent installation steps.

The **Amazon Linux AMI with Amazon Inspector Agent** is available on the EC2 console and also at the AWS Marketplace.

Installing the Agent on Multiple EC2 Instances Using the Systems Manager Run Command

You can install the Amazon Inspector agent on your EC2 instances using the Systems Manager Run Command. This enables you to install the agent remotely and on multiple instances (both Linux-based and Windows-based instances with the same command) at once.

Important
Agent installation using the Systems Manager Run Command is not currently supported for the Debian operating system.

Important
To use this option, make sure that your EC2 instance has the SSM Agent installed and has an IAM role that allows Run Command. The SSM Agent is installed, by default, on Amazon EC2 Windows instances and Amazon Linux instances. Amazon EC2 Systems Manager requires an IAM role for EC2 instances that processes commands and a separate role for users executing commands. For more information, see Installing and Configuring SSM Agent and Configuring Security Roles for System Manager.

To install the agent on multiple EC2 instances using the Systems Manager Run Command

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane under **Systems Manager Services**, choose **Run Command**.
3. Choose **Run a command**.
4. For **Command document**, choose the document named **AmazonInspector-ManageAWSAgent** that is owned by **Amazon**. This document contains the script for installing the Amazon Inspector agent on EC2 instances.
5. For **Select targets by**, specify your EC2 instances either by choosing the **Specifying a Tag** option or by choosing **Manually Selecting Instances**. Then choose **Select instances**. To install the agent on all the instances in the assessment target, you can specify the same tags that are used for creating the assessment target.
6. Provide your choices for the rest of the available options using the instructions in Executing Commands from the EC2 Console, and then choose **Run**.

Note
You can also install the agent on multiple EC2 instances (both Linux-based and Windows-based) when you create an assessment target, or you can use the **Install Agents with Run Command** button for an existing target. For more information, see Creating an Assessment Target (p. 35).

Installing the Agent on a Linux-based EC2 Instance

Perform the following procedure to install the Amazon Inspector agent on a Linux-based EC2 instance.

To install the agent on a Linux-based EC2 instance

1. Sign in to your EC2 instance running a Linux-based operating system where you want to install the Amazon Inspector agent.

   Note
   For information about the operating systems that Amazon Inspector supports, see Amazon Inspector Supported Operating Systems and Regions (p. 4).
2. Download the agent installation script by running one of the following commands:

   - **wget https://inspector-agent.amazonaws.com/linux/latest/install**
   - **curl -O https://inspector-agent.amazonaws.com/linux/latest/install**
3. (Optional) Verify that the agent installation script is not altered or corrupted. For more information, see (Optional) Verify the Signature of the Amazon Inspector Agent Installation Script on Linux-based Operating Systems (p. 29).
4. To install the agent, run **sudo bash install**.

   Note
   As updates for the agent become available, they are automatically downloaded from Amazon S3 and applied. For more information, see Amazon Inspector Agent Updates (p. 21).
   If you want to skip this auto-update process, 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**.
5. Verify that the following files required for the agent to be successfully installed and functioning properly are installed:

   - `libcurl4` (required to install the agent on Ubuntu 18.04)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (required to install the agent on Debian 9)
   - `libpcap0.8`

Installing the Agent on a Windows-based EC2 Instance

Perform the following procedure to install the Amazon Inspector agent on a Windows-based EC2 instance.

To install the agent on a Windows-based EC2 instance

1. Sign in to your EC2 instance running a Windows-based operating system where you want to install the agent.

   Note
   For more information about the operating systems that Amazon Inspector supports, see Amazon Inspector Supported Operating Systems and Regions (p. 4).
2. Download the following .exe file:

```
https://inspector-agent.amazonaws.com/windows/installer/latest/
AWSAgentInstall.exe
```

3. Open a command prompt window (with administrative permissions), navigate to the location where you saved the downloaded `AWSAgentInstall.exe`, and run the .exe file to install the agent.

   Note
   As updates for the agent become available, they are automatically downloaded from Amazon S3 and applied. For more information, see Amazon Inspector Agent Updates (p. 21).
   If you want to skip this auto-update process, run the following command when you install the agent:
   AWSAgentInstall.exe AUTOUPDATE=No

Working with Amazon Inspector Agents on Linux-based Operating Systems

You can install, remove, verify, and modify the behavior of Amazon Inspector agents. Sign in to your Amazon EC2 instance running a Linux-based operating system, and run any of the following procedures. For more information about the operating systems that are supported for Amazon Inspector, see Amazon Inspector Supported Operating Systems and Regions (p. 4).

Note
The commands in this section function in all AWS Regions that are supported by Amazon Inspector.

Topics

Verifying That the Amazon Inspector Agent is Running

- To verify that the 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.

Stopping the Amazon Inspector Agent

- To stop the agent, run the following command:

  sudo /etc/init.d/awsagent stop

Starting the Amazon Inspector Agent

- To start the agent, run the following command:

  sudo /etc/init.d/awsagent start

Modifying Amazon Inspector Agent Settings

After the Amazon Inspector 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. On Linux-based operating systems, the `agent.cfg` file is located in the `/opt/aws/awsagent/etc` directory. After you modify and save the `agent.cfg` file, you must stop and start the agent for the changes to take effect.

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

Configuring Proxy Support for an Amazon Inspector Agent

To get proxy support for an agent on a Linux-based operating system, use an agent-specific configuration file with specific environment variables. For more information, see https://wiki.archlinux.org/index.php/proxy_settings.

Complete one of the following procedures:

To install an agent on an EC2 instance that uses a proxy server

1. Create a file called `awsagent.env` and save it in the `/etc/init.d/` directory.
2. Edit `awsagent.env` to include these environment variables in the following format:

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   > Substitute values in the preceding examples with valid hostname and port number combinations only. Specify the IP address of the instance metadata endpoint (169.254.169.254) for the `no_proxy` variable.
3. Install the Amazon Inspector agent by completing the steps in the Installing the Agent on a Linux-based EC2 Instance (p. 23) procedure.

To configure proxy support on an EC2 instance with a running agent

1. To configure proxy support, the version of the agent that is running on your EC2 instance must be 1.0.800.1 or later. If you enabled the auto-update process for the agent, you can verify that your agent's version is 1.0.800.1 or later by using the Verifying That the Amazon Inspector Agent is Running (p. 25) procedure. If you didn't enable the auto-update process for the agent, you must install the agent on this EC2 instance again by following the Installing the Agent on a Linux-based EC2 Instance (p. 23) procedure.
2. Create a file called `awsagent.env`, and save it in the `/etc/init.d/` directory.
3. Edit `awsagent.env` to include these environment variables in the following format:

- `export https_proxy=hostname:port`
- `export http_proxy=hostname:port`
- `export no_proxy=169.254.169.254`

Note
Substitute values in the preceding examples with valid hostname and port number combinations only. Specify the IP address of the instance metadata endpoint (169.254.169.254) for the `no_proxy` variable.

4. Restart the agent by first stopping it using the following command:

   ```
   sudo /etc/init.d/awsagent restart
   ```

   Proxy settings are picked up and used by both the agent and the auto-update process.

Uninstalling the Amazon Inspector Agent

To uninstall the agent

1. Sign in to your EC2 instance running a Linux-based operating system where you want to uninstall the agent.

   Note
   For more information about the operating systems that are supported for Amazon Inspector, see Amazon Inspector Supported Operating Systems and Regions (p. 4).

2. To uninstall the agent, use one of the following commands:

   - On Amazon Linux, CentOS, and Red Hat, run the following command:

     sudo yum remove 'AwsAgent*'

   - On Ubuntu Server, run the following command:

     sudo apt-get purge 'awsagent*'

Working with Amazon Inspector Agents on Windows-based Operating Systems

You can start, stop, and modify the behavior of Amazon Inspector agents. Sign in to your EC2 instance running a Windows-based operating system and perform any of the procedures in this chapter. For more information about the operating systems that are supported for Amazon Inspector, see Amazon Inspector Supported Operating Systems and Regions (p. 4).

Note
The commands in this chapter function in all AWS Regions that are supported by Amazon Inspector.

Topics

Starting or Stopping an Amazon Inspector Agent or Verifying That the Agent is Running

To start, stop, or verify an agent

1. On your EC2 instance, choose **Start**, **Run**, and then enter **`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 successfully starts, the status is updated to **Started** or **Running**.
4. To stop the agent, right-click **AWS Agent Service**, and then choose **Stop**. If the service successfully stops, the status is cleared (appears as blank). We don't recommend stopping the **AWS Agent Updater Service** because it disables the installation of all future enhancements and fixes to the agent.
5. To verify that the agent is installed and running, sign in to your EC2 instance, and open a command prompt using 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 can't be contacted.

Modifying Amazon Inspector Agent Settings

After the Amazon Inspector 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. On Windows-based operating systems, the file is located in the `C:\ProgramData\Amazon Web Services\AWS Agent` directory. After you modify and save the `agent.cfg` file, you must stop and start the agent for the changes to take effect.

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

Configuring Proxy Support for an Amazon Inspector Agent

To get proxy support for an agent on a Windows-based operating system, use the `WinHTTP` proxy. To set up the `WinHTTP` proxy using the `netsh` utility, see https://technet.microsoft.com/en-us/library/cc731131%28v=ws.10%29.aspx.

Complete one of the following procedures:

To install an agent on an EC2 instance that uses a proxy server

1. Download the following .exe file: `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`.
2. Open a command prompt window or PowerShell window (using administrative permissions). Navigate to the location where you saved the downloaded `AWSAgentInstall.exe`, and then run the following command:

   ```
   ./AWSAgentInstall.exe \install USEPROXY=1
   ```

To configure proxy support on an EC2 instance with a running agent

1. To configure proxy support, the version of the Amazon Inspector agent that is running on your EC2 instance must be 1.0.0.59 or later. If you enabled the auto-update process for the agent, you can verify that your agent's version is 1.0.0.59 or later by using theStarting or Stopping an Amazon Inspector Agent or Verifying That the Agent is Running (p. 28) procedure. If you didn't enable the auto-update process for the agent, you must install the agent on this EC2 instance again by following the Installing the Agent on a Windows-based EC2 Instance (p. 24) procedure.
2. Open the registry editor (`regedit.exe`).
3. Navigate to the following registry key: `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`.
4. Inside this registry key, create a registry `DWORD(32bit)` value called `"UseProxy"`.
5. Double-click on the value, and set the value to 1.
6. Enter **`services.msc`**, locate the **AWS Agent Service** and the **AWS Agent Updater Service** in the **Services** window, and restart each process. After both processes have successfully restarted, run the `AWSAgentStatus.exe` file (see step 5 in Starting or Stopping an Amazon Inspector Agent or Verifying That the Agent is Running (p. 28)). View the status of your agent and verify that it is using the configured proxy.

Uninstalling the Amazon Inspector Agent

To uninstall the agent

1. Sign in to your EC2 instance running a Windows-based operating system where you want to uninstall the Amazon Inspector agent.

   Note
   For more information about the operating systems that are supported for Amazon Inspector, see Amazon Inspector Supported Operating Systems and Regions (p. 4).
2. On your EC2 instance, navigate to **Control Panel**, **Add/Remove Programs**.
3. In the list of installed programs, choose **AWS Agent**, and then choose **Uninstall**.

(Optional) Verify the Signature of the Amazon Inspector Agent Installation Script on Linux-based Operating Systems

This topic describes the recommended process of verifying the validity of the Amazon Inspector agent's installations script for Linux-based operating systems.

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 Amazon Inspector agent is altered or corrupted, do NOT run the installation file. Instead, contact AWS Support.

Amazon Inspector agent files for Linux-based operating systems 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.

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.

Topics

Installing 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**.

Authenticating and Importing 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`. Make 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 that are similar to the following:

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   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 in the preceding example. Compare the key fingerprint that is returned to the one published on this page. They should match. If they don't match, don't install the Amazon Inspector agent installation script, and contact AWS Support.

Verify the Signature of the Package

After you install the `GPG` tools, authenticate and import the Amazon Inspector public key, and verify that the public key is trusted, you are ready to verify the signature of the installation script.

To verify the 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, don't run the installation file that you downloaded previously, and contact AWS Support.

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 AWS office and receive the key in person. However, more often you download it from a website. In this case, the website is an AWS website.
- **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.

(Optional) Verify the Signature of the Amazon Inspector Agent Installation Script on Windows-based Operating Systems

This topic describes the recommended process of verifying the validity of the Amazon Inspector agent's installations script for Windows-based operating systems.

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 Amazon Inspector agent is altered or corrupted, do NOT run the installation file. Instead, contact AWS Support.

To verify the validity of the downloaded agent installation script on Windows-based operating systems, make sure that the thumbprint of its Amazon Services LLC signer certificate is equal to this value:

5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

To verify this value, perform the following procedure:

1. Right-click the downloaded `AWSAgentInstall.exe`, and open the **Properties** window.
2. Choose the **Digital Signatures** tab.
3. From the **Signature List**, choose **Amazon Services LLC**, and then choose **Details**.
4. Choose the **General** tab, if not already selected, and then choose **View Certificate**.
5. Choose the **Details** tab, and then choose **All** in the **Show** dropdown list, if not already selected.
6. Scroll down until you see the **Thumbprint** field and then choose **Thumbprint**. This displays the entire thumbprint value in the lower window.

   - If the thumbprint value in the lower window is identical to the following value:

     5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

     then your downloaded agent installation script is authentic and can be safely installed.
   - If the thumbprint value in the lower details window is not identical to the value above, do not run `AWSAgentInstall.exe`.

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 should address.

Important
Currently, your assessment targets can consist only of EC2 instances that run on supported operating systems. For information about supported operating systems and supported AWS Regions, see Amazon Inspector Service Limits (p. 4).

Note
For information about launching EC2 instances, see Amazon Elastic Compute Cloud Documentation.

Topics

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, you can create your own custom tag keys or use tag keys created by others in the same AWS account. You can also use the tag keys that AWS automatically creates. For example, AWS automatically creates a **Name** tag key for the EC2 instances that you launch.

You can add tags to EC2 instances when you create them, or you can add, change, or remove those tags one at a time on the console page for each EC2 instance. 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 Target Limits

You can create up to 50 assessment targets per AWS account. For more information, see Amazon Inspector Service Limits (p. 4).

Creating an Assessment Target

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**, enter a name for your assessment target.
4. Do one of the following:

   - To include all EC2 instances in this AWS account and Region in this assessment target, select the **All instances** check box.

     Note
     The limit on the maximum number of agents that you can include in an assessment run applies when you use this option. For more information, see Amazon Inspector Service Limits (p. 4).

   - To choose the EC2 instances that you want to include in this assessment target, for **Use Tags**, enter the tag key names and key-value pairs.
5. (Optional) While creating a target, you can select the **Install Agents** check box to install the agent on all EC2 instances in this target. To use this option, your EC2 instances must have the SSM Agent installed and an IAM role that allows Run Command. The SSM Agent is installed, by default, on Amazon EC2 Windows instances and Amazon Linux instances. Amazon EC2 Systems Manager requires an IAM role for EC2 instances that process commands and a separate role for users that execute commands. For more information, see Installing and Configuring SSM Agent and Configuring Security Roles for System Manager.

   Important
   If an EC2 instance already has an agent running on it, using this option replaces the agent currently running on the instance with the latest agent version.

   Note
   For your existing assessment targets, you can choose the **Install Agents with Run Command button** to install the agent on all EC2 instances in this target.

   Note
   You can also install the agent on multiple EC2 instances (both Linux-based and Windows-based instances with the same command) remotely by using the Systems Manager Run Command. For more information, see Installing the Amazon Inspector Agent on Multiple EC2 Instances Using the Systems Manager Run Command (p. 23).
6. Choose **Save**.

Note
You can use the **Preview Target** button on the **Assessment Targets** page to review all EC2 instances included in the assessment target. For each EC2 instance, you can review the hostname, instance ID, IP address, and, if applicable, the status of the agent. The agent status can have the following values: **HEALTHY**, **UNHEALTHY**, and **UNKNOWN**. Amazon Inspector displays an **UNKNOWN** status when it can't determine whether there is an agent running on the EC2 instance.

Deleting an Assessment Target

To delete an assessment target, perform the following procedure.

To delete an assessment target

- On the **Assessment targets** page, choose the target that you want to delete, and then choose **Delete**. When prompted for confirmation, choose **Yes**.

  Important
  When you delete an assessment target, all assessment templates, assessment runs, findings, and versions of the reports that are associated with the target are also deleted.

You can also delete an assessment target by using the `DeleteAssessmentTarget` API.

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 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. Others might want to focus 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

An Amazon Inspector assessment can use any combination of the following rules packages:

Network assessments:

Host assessments:

- Common Vulnerabilities and Exposures (p. 41)
- Center for Internet Security (CIS) Benchmarks (p. 41)
- Security Best Practices for Amazon Inspector (p. 46)
- Runtime Behavior Analysis (p. 43)

Network Reachability

The rules in the Network Reachability package analyze your network configurations to find security vulnerabilities of your EC2 instances. The findings that Amazon Inspector generates also provide guidance about restricting access that is not secure.

The Network Reachability rules package uses the latest technology from the AWS Provable Security initiative.

The findings generated by these rules show whether your ports are reachable from the internet through an internet gateway (including instances behind Application Load Balancers or Classic Load Balancers), a VPC peering connection, or a VPN through a virtual gateway. These findings also highlight network configurations that allow for potentially malicious access, such as mismanaged security groups, ACLs, IGWs, and so on.

These rules help automate the monitoring of your AWS networks and identify where network access to your EC2 instances might be misconfigured. By including this package in your assessment run, you can implement detailed network security checks without having to install scanners and send packets, which are complex and expensive to maintain, especially across VPC peering connections and VPNs.

Important
An Amazon Inspector agent is not required to assess your EC2 instances with this rules package. However, an installed agent can provide information about the presence of any processes listening on the ports.

Important
This rules package does not support Amazon EC2 Classic networks.

For more information, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

Configurations Analyzed

Network Reachability rules analyze the configuration of the following entities for vulnerabilities:

- Amazon EC2 instances
- Application Load Balancers
- Direct Connect
- Elastic Load Balancers
- Elastic Network Interfaces
- Internet Gateways (IGWs)
- Network Access Control Lists (ACLs)
- Route Tables
- Security Groups (SGs)
- Subnets
- Virtual Private Clouds (VPCs)
- Virtual Private Gateways (VGWs)
- VPC peering connections

Important
The Network Reachability rules package does not account for any other constructs that allow or restrict inbound access.

Reachability Routes

Network Reachability rules check for the following reachability routes, which correspond to the ways in which your ports can be accessed from outside of your VPC:

- **`Internet`** - Internet gateways (including Application Load Balancers and Classic Load Balancers)
- **`PeeredVPC`** - VPC peering connections
- **`VGW`** - Virtual private gateways

Findings Types

An assessment that includes the Network Reachability rules package can return the following types of findings for each reachability route:

- `RecognizedPort` (p. 39)
- `UnrecognizedPortWithListener` (p. 40)
- `NetworkExposure` (p. 40)

`RecognizedPort`

A port that is typically used for a well-known service is reachable. If an agent is present on the target EC2 instance, the generated finding will also indicate whether there is an active listening process on the port. Findings of this type are given a severity based on the security impact of the well-known service:

- **`RecognizedPortWithListener`** – A recognized port is externally reachable from the public internet through a specific networking component, and a process is listening on the port.
- **`RecognizedPortNoListener`** – A port is externally reachable from the public internet through a specific networking component, and there are no processes listening on the port.
- **`RecognizedPortNoAgent`** – A port is externally reachable from the public internet through a specific networking component. The presence of a process listening on the port can't be determined without installing an agent on the target instance.

The following table shows a list of recognized ports:

Service	TCP Ports	UDP Ports
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP over TLS	636	
Global catalog LDAP	3268	
Global catalog LDAP over TLS	3269	

Service	TCP Ports	UDP Ports
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514
Print services	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80
HTTPS	443	443

UnrecogizedPortWithListener

A port that is not listed in the preceding table is reachable and has an active listening process on it. Because findings of this type show information about listening processes, they can be generated only when an Amazon Inspector agent is installed on the target EC2 instance. Findings of this type are given **Low** severity.

NetworkExposure

Findings of this type show aggregate information on the ports that are reachable on your EC2 instance. For each combination of elastic network interfaces and security groups on an EC2 instance, these findings show the reachable set of TCP and UDP port ranges. Findings of this type have the severity of **Informational**.

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, see https://cve.mitre.org/.

If a particular CVE appears in a *finding* that is produced by an Amazon Inspector assessment, you can search https://cve.mitre.org/ for the ID of the CVE (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 regional lists:

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- EU (Ireland)
- EU (Frankfurt)
- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- Asia Pacific (Sydney)
- AWS GovCloud West (US)
- AWS GovCloud East (US)

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.

For more information, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

Center for Internet Security (CIS) Benchmarks

The CIS Security Benchmarks program provides well-defined, unbiased, consensus-based industry best practices to help organizations assess and improve their security. AWS is a CIS Security Benchmarks Member company. For a list of Amazon Inspector certifications, see the Amazon Web Services page on the CIS website.

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

Amazon Linux

- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1`
- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2`
- `CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1`

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)

If a specific CIS benchmark appears in a finding that is 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.

For more information, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

Runtime Behavior Analysis

The rules in the Runtime Behavior Analysis rules package analyze the behavior of your instances during an assessment run. They also provide guidance about how to make your EC2 instances more secure.

For more information, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

Topics

Non-Secure Client Protocols (Login)

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

> **Important**
> Currently, 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. 37)

Finding

An EC2 instance in your assessment target uses insecure protocols to connect to a remote host for login. These protocols do not secure 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.

Non-Secure Client Protocols (General)

This rule detects a client's use of non-secure protocols.

> **Important**
> Currently, 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. 37)

Finding

An EC2 instance in your assessment target uses non-secure protocols to connect to a remote host. These protocols do not secure traffic, increasing the risk of a successful traffic interception attack.

Resolution

It is recommended that you replace these non-secure protocols with encrypted versions.

Unused Listening TCP Ports

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

Important
Currently, 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. 37)

Finding

An EC2 instance in your assessment target is listening on TCP ports, but Amazon Inspector didn't discover any traffic to these ports 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.

Non-Secure Server Protocols

This rule helps determine whether your EC2 instances allow support for non-secure and unencrypted ports or services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, RSH, and `rlogin`.

Important
Currently, 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. 37)

Finding

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

Resolution

We recommend that you disable non-secure protocols that are supported on an EC2 instance in your assessment target, and replace them with more 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 non-secure 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 Data Execution Prevention (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**
> Currently, 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. 37)

Finding

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

Resolution

We recommend 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.

Root Process with Non-Secure Permissions

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

> **Important**
> Currently, 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. 37)

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, we recommend that you correct the permissions on the relevant modules to ensure that they are writable only by the root user.

Security Best Practices for Amazon Inspector

Use Amazon Inspector rules to help determine whether your systems are configured securely.

> **Important**
> Currently, 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 described in this section generate findings **only** for the EC2 instances that are running Linux-based operating systems. The rules do not generate findings for EC2 instances that are running Windows-based operating systems.
> For more information, see Amazon Inspector Rules Packages for Supported Operating Systems (p. 67).

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. 37)

Finding

There is an EC2 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 the `/etc/ssh/sshd_config` file, and then 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. 37)

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 later. For OpenSSH, you can achieve this by setting `Protocol 2` in the `/etc/ssh/sshd_config` file. 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. 37)

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. 37)

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. 37)

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. 37)

Finding

No password complexity mechanism or restrictions are configured on EC2 instances in your assessment target. This allows users to set simple passwords, which increases 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 the following options in the `pwquality.conf` file: `lcredit`, `ucredit`, `dcredit`, and `ocredit`. For more information, see https://linux.die.net/man/5/pwquality.conf . If `pwquality.conf` is not available on your instance, you can set the `lcredit`, `ucredit`, `dcredit`, and `ocredit` options using the `pam_cracklib.so` module. 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. 37)

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 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. 37)

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. It checks that only the root user (a user who logs in by using root account credentials) has write permissions for these directories.

Severity: High (p. 37)

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 target to be writable only by users who log in by using root account credentials.

Amazon Inspector Assessment Templates and Assessment Runs

Amazon Inspector helps you discover potential security issues by using security rules to analyze your AWS resources. Amazon Inspector monitors and collects behavioral data (telemetry) about your resources. The data includes information about 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 security rules packages. Finally, Amazon Inspector produces a list of *findings* that identify potential security issues of various levels of severity.

To get started, you create an *assessment target* (a collection of the AWS resources that you want Amazon Inspector to analyze). Next, you create an *assessment template* (a blueprint that you use to configure your assessment). You use the template to start an *assessment run*, which is the monitoring and analysis process that results in a set of findings.

Topics

Amazon Inspector Assessment Templates

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

- Amazon SNS topics that Amazon Inspector sends notifications to about your assessment run states and findings
- Amazon Inspector attributes (key-value pairs) that you can assign to findings that are generated by the assessment run that uses this assessment template

After 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. You might want to include various subsets of the available rules in your assessment templates to target specific areas of concern or to uncover specific security issues. Tagging assessment templates allows you to locate and run them quickly at any time in accordance with your security strategy and goals.

Important
After you create an assessment template, you can't modify it.

Amazon Inspector Assessment Templates Limits

You can create up to 500 assessment templates for each AWS account.

For more information, see Amazon Inspector Service Limits (p. 4).

Creating an Assessment Template

To create an assessment template

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 Templates**, and then choose **Create**.
3. For **Name**, enter a name for your assessment template.
4. For **Target name**, choose an assessment target to analyze.

   Note
   When you create an assessment template, you can use the **Preview Target** button on the **Assessment Templates** page to review all EC2 instances included in the assessment target. For each EC2 instance, you can review the hostname, instance ID, IP address, and, if applicable, the status of the agent. The agent status can have the following values: **HEALTHY**, **UNHEALTHY**, and **UNKNOWN**. Amazon Inspector displays an **UNKNOWN** status when it can't determine whether there is an agent running on the EC2 instance.
   You can also use the **Preview Target** button on the **Assessment Templates** page to review EC2 instances that make up assessment targets included in your previously created templates.
5. For **Rules packages**, choose one or more rules 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 that you want Amazon Inspector to send notifications to 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, see Setting Up an SNS Topic for Amazon Inspector Notifications (p. 54).

8. (Optional) For **Tag**, enter values for **Key** and **Value**. You can add multiple tags to the assessment template.
9. (Optional) For **Attributes added to findings**, enter values for **Key** and **Value**. Amazon Inspector applies the attributes to all findings that are generated by the assessment template. You can add multiple attributes to the assessment template. For more information about findings and tagging findings, see Amazon Inspector Findings (p. 56).
10. (Optional) To set up a schedule for your assessment runs using this template, select the **Set up recurring assessment runs once every <number_of_days>, starting now** check box and specify the recurrence pattern (number of days) using the up and down arrows.

    Note
    When you use this check box, Amazon Inspector automatically creates an Amazon CloudWatch Events rule for the assessment runs schedule that you are setting up. Amazon Inspector then also automatically creates an IAM role named `AWS_InspectorEvents_Invoke_Assessment_Template`. This role enables CloudWatch Events to make API calls against the Amazon Inspector resources. For more information, see What is Amazon CloudWatch Events? and Using Resource-Based Policies for CloudWatch Events.

    Note
    You can also set up automatic assessment runs through an AWS Lambda function. For more information, see Setting Up Automatic Assessment Runs Through a Lambda Function (p. 53).
11. Choose **Create and run** or **Create**.

Deleting an Assessment Template

To delete an assessment template, perform the following procedure.

To delete an assessment template

- On the **Assessment Templates** page, choose the template that you want to delete, and then choose **Delete**. When prompted for confirmation, choose **Yes**.

  Important
  When you delete an assessment template, all assessment runs, findings, and versions of the reports associated with this template are also deleted.

You can also delete an assessment template by using the `DeleteAssessmentTemplate` API.

Assessment Runs

After you create an assessment template, you can use it to start assessment runs. You can start multiple runs using the same template as long as you stay within the runs limit for each AWS account. For more information, see Amazon Inspector Assessment Runs Limits (p. 53).

If you use the Amazon Inspector console, you must start the first run of your new assessment template from the **Assessment templates** page. After you start the run, you can use the **Assessment runs** page to monitor the run's progress. Use the **Run**, **Cancel**, and **Delete** buttons to start, cancel, or delete a run. You

can also view the run's details, including the ARN of the run, the rules packages selected for the run, the tags and attributes that you applied to the run, and more.

For subsequent runs of the assessment template, you can use the **Run**, **Cancel**, and **Delete** buttons on either the **Assessment templates** page or the **Assessment runs** page.

Deleting an Assessment Run

To delete an assessment run, perform the following procedure.

To delete a run

- On the **Assessment runs** page, choose the run that you want to delete, and then choose **Delete**. When prompted for confirmation, choose **Yes**.

  Important
  When you delete an run, all findings and all versions of the report from that run are also deleted.

You can also delete a run by using the `DeleteAssessmentRun` API.

Amazon Inspector Assessment Runs Limits

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

You can have multiple runs occurring at the same time as long as the targets used for the runs don't contain overlapping EC2 instances.

For more information, see Amazon Inspector Service Limits (p. 4).

Setting Up Automatic Assessment Runs Through a Lambda Function

If you want to set up a recurring schedule for your assessment, you can configure your assessment template to run automatically by creating a Lambda function using the AWS Lambda console. For more information, see Lambda Functions.

To set up automatic assessment runs using the AWS Lambda console, perform the following procedure.

To set up automatic runs through a Lambda function

1. Sign in to the AWS Management Console, and open the AWS Lambda console.
2. In the navigation pane, choose either **Dashboard** or **Functions**, and then choose **Create a Lambda Function**.
3. On the **Select blueprint** page, choose the **inspector-scheduled-run** blueprint. You can find this blueprint by entering **`inspector`** in the **Filter** field.
4. On the **Configure triggers** page, set up a recurring schedule for automated runs by specifying a CloudWatch event that triggers your function. To do this, enter a rule name and description, and then choose a schedule expression. The schedule expression determines how often the run occurs, for example, every 15 minutes or once a day. For more information about CloudWatch events and concepts, see What is Amazon CloudWatch Events?

If you select the **Enable trigger** check box, the run begins immediately after you finish creating your function. Subsequent automated runs follow the recurrence pattern that you specify in the **Schedule expression** field. If you don't select the **Enable trigger** check box while creating the function, you can edit the function later to enable this trigger.

5. On the **Configure function** page, specify the following:

   - For **Name**, enter a name for your function.
   - (Optional) For **Description**, enter a description that will help you identify your function later.
   - For **runtime**, keep the default value of **`Node.js 8.10`**. AWS Lambda supports the **inspector-scheduled-run** blueprint only for the **`Node.js 8.10`** runtime.
   - The assessment template that you want to run automatically using this function. You do this by providing the value for the environment variable called **assessmentTemplateArn**.
   - Keep the handler set to the default value of **`index.handler`**.
   - The permissions for your function using the **Role** field. For more information, see AWS Lambda Permissions Model.

     To run this function, you need an IAM role that allows AWS Lambda to start the runs and write log messages about the runs, including any errors, to Amazon CloudWatch Logs. AWS Lambda assumes this role for every recurring automated run. For example, you can attach the following sample policy to this IAM role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

6. Review your selections, and then choose **Create function**.

Setting Up an SNS Topic for Amazon Inspector Notifications

Amazon Simple Notification Service (Amazon SNS) is a web service that sends messages to subscribing endpoints or clients. You can use Amazon SNS to set up notifications for Amazon Inspector. For more information, see What is Amazon Simple Notification Service 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 publish messages to the topic:

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

   - `Asia Pacific (Mumbai)` - *arn:aws:iam::162588757376:root*
   - `Asia Pacific (Seoul)` - *arn:aws:iam::526946625049:root*
   - `Asia Pacific (Sydney)` - *arn:aws:iam::454640832652:root*
   - `Asia Pacific (Tokyo)` - *arn:aws:iam::406045910587:root*
   - `EU (Frankfurt)` - *arn:aws:iam::537503971621:root*
   - `EU (Ireland)` - *arn:aws:iam::357557129151:root*
   - `US East (Northern Virginia)` - *arn:aws:iam::316112463485:root*
   - `US East (Ohio)` - *arn:aws:iam::646659390643:root*
   - `US West (Northern California)` - *arn:aws:iam::166987590008:root*
   - `US West (Oregon)` - *arn:aws:iam::758058086616:root*
   - `AWS GovCloud (US-East)` - *arn:aws-us-gov:iam::206278770380:root*
   - `AWS GovCloud (US-West)` - *arn:aws-us-gov:iam::850862329162:root*

Amazon Inspector Findings

Findings are potential security issues that Amazon Inspector discovers during an assessment of your assessment target. Findings are displayed on the Amazon Inspector console or through the API. Findings contain detailed descriptions of the security issues and recommendations for resolving them.

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

Tracking your findings with attributes can be useful for managing the workflow of your security strategy. For example, after you create and run an assessment, it generates a list of findings of various levels of 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. Or 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`**.

Working with 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 can't view the findings that are 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.

- Native severity details from the Common Vulnerability Scoring System (CVSS). These include CVSS vector and CVSS score metrics (including CVSS version 2.0 and 3.0) for the findings triggered by the rules in the Common Vulnerabilities and Exposures rules package. For details about the CVSS, see https://www.first.org/cvss/.
- Native severity details from the Center of Internet Security (CIS). These include the CIS weight metric for the findings triggered by the rules in the CIS Benchmarks package. For more information about CIS weight metric, see https://www.cisecurity.org/.
- 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 an assessment template. To do that, you configure the new template to automatically assign attributes to all findings that are generated by the assessment run. 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. 50).
5. To export findings to a spreadsheet, choose the down arrow in the upper-right corner of the **Findings** page. In the dialog box, choose **Export all columns** or **Export visible columns**.
6. To show or hide columns for the generated findings and to filter through the generated findings, choose the settings icon in the upper-right corner of the **Findings** page.
7. To delete findings, navigate to the **Assessment runs** page and choose the run that resulted in the findings that you want to delete. Then choose **Delete**. When prompted for confirmation, choose **Yes**.

   Important
   You can't delete individual findings in Amazon Inspector. When you delete an assessment run, all findings and all versions of the report from that run are also deleted.

   You can also delete an assessment run by using the DeleteAssessmentRun API.

Assessment Reports

An Amazon Inspector *assessment report* is a document that details what is tested in the assessment run and the results of the assessment. You can store the reports, share them with your team for remediation actions, or use them to augment your compliance audit data. You can generate a report for an assessment run after the run has successfully completed.

> **Note**
> You can generate reports only for assessment runs that occur after April 25, 2017, which is when assessment reports in Amazon Inspector became available.

You can view the following types of assessment reports:

- **Findings report** – this report contains the following information:
  - Summary of the assessment
  - EC2 instances evaluated during the assessment run
  - Rules packages included in the assessment run
  - Detailed information about each finding, including all EC2 instances that had the finding
- **Full report** – this report contains all the information that is included in a findings report, and additionally provides the list of rules that were checked against the instances in the assessment target.

To generate an assessment report

1. On the **Assessment runs** page, locate the assessment run that you want to generate a report for. Make sure that its status is set to **Analysis complete**.
2. Under the **Reports** column for this assessment run, choose the reports icon.

   > **Important**
   > The reports icon is present in the **Reports** column only for those assessment runs that took place or will take place after April 25, 2017. That is when assessment reports in Amazon Inspector became available.
3. In the **Assessment report** dialog box, choose the type of report that you want to view (either a **Findings** or a **Full** report) and the report format (HTML or PDF). Then choose **Generate report**.

You can also generate assessment reports through the GetAssessmentReport API.

To delete an assessment report, perform the following procedure.

To delete a report

- On the **Assessment runs** page, choose the run that the report that you want to delete is based on, and then choose **Delete**. When prompted for confirmation, choose **Yes**.

  > **Important**
  > In Amazon Inspector, you can't delete individual reports. When you delete an assessment run, all versions of the report from that run and all findings are also deleted.

  You can also delete an assessment run by using the DeleteAssessmentRun API.

Exclusions in Amazon Inspector

Exclusions are an output of Amazon Inspector assessment runs. Exclusions show which of your security checks can't be completed and how to resolve the issues. For example, issues can be caused by the absence of an agent on the specified target's EC2 instances, the use of an unsupported operating system, or unexpected errors.

You can view exclusions on the **Assessment runs** page on the console. For more information, see Viewing Post-Assessment Exclusions (p. 66).

To avoid incurring unnecessary AWS fees, Amazon Inspector allows you to preview exclusions before running an assessment. You can find the previews on the **Assessment templates** page on the console. For more information, see Previewing Exclusions (p. 65).

> **Note**
> You can generate post-assessment exclusions only for runs that occur after June 25, 2018. That's when exclusions in Amazon Inspector became available. However, exclusion previews are available for all assessment templates regardless of date.

Topics

Exclusion Types

Amazon Inspector can produce the following exclusion types.

Exclus Type	Description	Recommenda								
No instances in target	There are no EC2 instances with the tags specified in the assessment target.	Check that the tags in your assessment target match the tags of your target EC2 instance.								
Agent is already running	An assessment run is already in progress on the target EC2 instance.	Wait until the current assessment run on the target EC2 instance has completed.								
Agent not found	An Amazon Inspector agent was	Install or reinstall an Amazon								

Exclus Type	Description	Recommenda								
	not found on the target EC2 instance.	Inspector agent on the target EC2 instance. For more information, see Installing Amazon Inspector Agents (p. 22).								
Agent is unhealthy	The Amazon Inspector agent on the target EC2 instance is in an unhealthy state.	Check the status of the Amazon Inspector agent on this instance and take necessary action. For more information, see Inspector Agents.								
Kernel module unavailable	The kernel module is unavailable for the Amazon Inspector agent on the target EC2 instance.	For a list of supported kernel versions, see Amazon Inspector Supported Operating Systems and Regions.								

Exclus Type	Description	Recommenda								
Unsupported OS version	The operating system of the target EC2 instance is not supported for Amazon Inspector assessments.	Remove the target EC2 instance from the assessment target, or create a target that doesn't include this instance. For a list of supported operating systems, see Amazon Inspector Supported Operating Systems and Regions.								
Deprecated rules package	The assessment template includes a deprecated rules package.	Create an assessment template without the deprecated rules package, and use it for future assessment runs.								

Exclus Type	Description	Recommenda								
Rules package not supported by OS	The operating system of the target EC2 instance is not supported by a rules package included in the assessment template.	Create an assessment template without the conflicting rules packages or remove the target EC2 instance from the assessment template. For a list of rules package support by operating system, see Rules Package Availability Across Supported Operating Systems.								
Rules evaluation error for single instance	An internal error has caused the rules evaluation to fail for this instance.	Attempt to run your assessment again. Contact support if the exclusion persists when you rerun the assessment.								
Rules evaluation error	An internal error has caused the rules evaluation to fail for your assessment.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								

Exclus Type	Description	Recommenda								
Network Reachability error – internet	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable from the internet. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								
Network Reachability error – internet through an Application Load Balancer	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable from the internet through an Application Load Balancer. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								

Exclus Type	Description	Recommenda								
Network Reachability error – internet through an Elastic Load Balancing load balancer	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable from the internet though an Elastic Load Balancing load balancer. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								
Network Reachability error –VPN	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable from VPN. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								

Exclus Type	Description	Recommenda								
Network Reachability error – AWS Direct Connect	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable through AWS Direct Connect. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								
Network Reachability error – VPC peering	An internal error has caused a Network Reachability evaluation to fail on checks for ports reachable from a peered VPC. You might get findings for other Network Reachability types.	Attempt to run the assessment again. Contact support if the exclusion persists when you rerun the assessment.								

Previewing Exclusions

Amazon Inspector allows you to preview potential exclusions before running an assessment.

To preview assessment exclusions

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 templates**.
3. Expand a template, and in the **Assessment templates** section, choose **Preview exclusions**.
4. Review the descriptions of all detected exclusions and the recommendations for addressing them.

You can also list and describe exclusions by using the `ListExclusions` and `DescribeExclusions` operations.

Viewing Post-Assessment Exclusions

After an assessment run, you can view details about any exclusions.

To view details about exclusions

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 runs**.
3. In the **Exclusions** column, choose the active link that is associated with an assessment run.
4. Review the descriptions of all detected exclusions and the recommendations for addressing them.

   You can also list and describe exclusions by using the `ListExclusions` and `DescribeExclusions` operations.

Amazon Inspector Rules Packages for Supported Operating Systems

You can run Amazon Inspector rules packages on the EC2 instances that are included in your assessment targets. The following table shows the availability of rules packages for supported operating systems.

Important
You can run an agentless assessment with the Network Reachability (p. 38) rules package on any EC2 instance regardless of operating system.

Note
For more information about supported operating systems, see Amazon Inspector Supported Operating Systems and Regions (p. 4).

Suppo Opera Syste	Common Vulnerabiliti and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Amazon Linux 2 LTS, 2017.12	Supported		Supported	Supported	Supported
Amazon Linux 2018.03	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2017.09	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2017.03	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2016.09	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2016.03	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2015.09	Supported	Supported	Supported	Supported	Supported
Amazon Linux 2015.03	Supported	Supported	Supported	Supported	Supported

Suppo Opera System	Common Vulnerabiliti and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Amazon Linux 2014.09	Supported		Supported	Supported	
Amazon Linux 2014.03	Supported		Supported	Supported	
Amazon Linux 2013.09	Supported		Supported	Supported	
Amazon Linux 2013.03	Supported		Supported	Supported	
Amazon Linux 2012.09	Supported		Supported	Supported	
Amazon Linux 2012.03	Supported		Supported	Supported	
Ubuntu 18.04 LTS	Supported		Supported	Supported	Supported
Ubuntu 16.04 LTS	Supported	Supported	Supported	Supported	Supported
Ubuntu 14.04 LTS	Supported	Supported	Supported	Supported	Supported
Debian 9.0 - 9.5, 8.0 - 8.7	Supported		Supported	Supported	
RHEL 7.6	Supported	Supported	Supported	Supported	
RHEL 6.2 - 6.9, 7.2 - 7.5	Supported	Supported	Supported	Supported	Supported
CentOS 7.6	Supported	Supported	Supported	Supported	

Suppo Opera System	Common Vulnerabiliti and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
CentOS 6.2 - 6.9, 7.2 - 7.5	Supported	Supported	Supported	Supported	Supported
Windows Server 2012 R2	Supported	Supported	Supported		Supported
Windows Server 2012	Supported	Supported	Supported		Supported
Windows Server 2008 R2	Supported	Supported	Supported		Supported
Windows Server 2016 Base	Supported		Supported		Supported

Logging Amazon Inspector API Calls with AWS CloudTrail

Amazon Inspector is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Inspector. CloudTrail captures all API calls for Amazon Inspector as events, including calls from the Amazon Inspector console and code calls to the Amazon Inspector API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Inspector. If you don't configure a trail, you can still view the most recent events on the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Inspector, the IP address the request was made from, who made the request, when it was made, and more.

To learn more about CloudTrail, see the AWS CloudTrail User Guide. For a full list of Amazon Inspector API operations, see Actions in the *Amazon Inspector API Reference*.

Amazon Inspector Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon Inspector, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Amazon Inspector, create a *trail*. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail on the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

CloudTrail logs all Amazon Inspector operations, including read-only operations, such as `ListAssessmentRuns` and `DescribeAssessmentTargets`, and management operations, such as `AddAttributesToFindings` and `CreateAssessmentTemplate`.

> **Note**
> CloudTrail logs only the request information of Amazon Inspector read-only operations. Both request and response information is logged for all other Amazon Inspector operations.

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

- Whether the request was made with root or AWS Identity and Access Management (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 CloudTrail userIdentity Element.

Understanding Amazon Inspector Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, and other request parameters. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

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


```
{
    "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:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
```

```
    "recipientAccountId": "444455556666"
}
```

Monitoring Amazon Inspector Using Amazon CloudWatch

You can monitor Amazon Inspector using Amazon CloudWatch, which collects and processes raw data into readable, near real-time metrics. By default, Amazon Inspector sends metric data to CloudWatch in 5-minute periods. You can use the AWS Management Console, the AWS CLI, or an API to view the metrics that Amazon Inspector sends to CloudWatch.

For more information about Amazon CloudWatch, see the Amazon CloudWatch User Guide.

Amazon Inspector CloudWatch Metrics

The Amazon Inspector namespace includes the following metrics.

`AssessmentTargetARN` metrics:

Metric	Description			
`TotalMatchingAgents`	Number of agents that match this target			
`TotalHealthyAgents`	Number of agents that match this target that are healthy			
`TotalAssessmentRuns`	Number of assessment runs for this target			
`TotalAssessmentRunFindings`	Number of findings for this target			

`AssessmentTemplateARN` metrics:

Metric	Description			
`TotalMatchingAgents`	Number of agents that match this template			
`TotalHealthyAgents`	Number of agents that match this template that are healthy			
`TotalAssessmentRuns`	Number of assessment runs for this template			
`TotalAssessmentRunFindings`	Number of findings for this template			

Aggregate metrics

Metric	Description			
TotalAssessmentRuns	Number of assessment runs in this AWS account			

Configuring Amazon Inspector Using AWS CloudFormation

For reference information about Amazon Inspector resources that are supported by AWS CloudFormation, see the following topics:

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

Important
For lists of the ARNs of Amazon Inspector rules packages in supported AWS Regions, see Amazon Inspector ARNS for Rules Packages (p. 84).

Authentication and Access Control for Amazon Inspector

Access to Amazon Inspector requires credentials that AWS can use to authenticate your requests. Those credentials must have permissions to access AWS resources such as Amazon Inspector assessment targets, assessment templates, or findings. The following sections provide details on how you can use AWS Identity and Access Management (IAM) and Amazon Inspector to help secure your resources by controlling who can access them:

Authentication

You can access AWS as any of the following types of identities:

- **AWS account root user** – When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.
- **IAM user** – An IAM user is an identity within your AWS account that has specific custom permissions (for example, permissions to create a directory in AWS Directory Service). You can use an IAM user name and password to sign in to secure AWS webpages like the AWS Management Console, AWS Discussion Forums, or the AWS Support Center.

  In addition to a user name and password, you can also generate access keys for each user. You can use these keys when you access AWS services programmatically, either through one of the several SDKs or by using the AWS Command Line Interface (CLI). The SDK and CLI tools use the access keys to cryptographically sign your request. If you don't use AWS tools, you must sign the request yourself. AWS Directory Service supports *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the *AWS General Reference*.

- **IAM role** – An IAM role is an IAM identity that you can create in your account that has specific permissions. It is similar to an *IAM user*, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources. IAM roles with temporary credentials are useful in the following situations:

  - **Federated user access** – Instead of creating an IAM user, you can use existing user identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the *IAM User Guide*.

- **AWS service access** – You can use an IAM role in your account to grant an AWS service permissions to access your account's resources. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the *IAM User Guide*.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances in the *IAM User Guide*.

Access Control

You can have valid credentials to authenticate your requests, but unless you have permissions you cannot create or access Amazon Inspector resources. For example, you must have permissions to create an Amazon Inspector assessment target and an assessment template to start an assessment run.

The following sections describe how to manage permissions for Amazon Inspector. We recommend that you read the overview first.

Overview of Managing Access Permissions to Your Amazon Inspector Resources

Every AWS resource is owned by an AWS account, and permissions to create or access a resource are governed by AWS Identity and Access Management (IAM) permissions policies. An account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles). Some services (such as AWS Lambda) also support attaching permissions policies to resources.

> **Note**
> An *account administrator* (or administrator user) is an IAM user with administrator privileges. For more information, see IAM Best Practices in the *IAM User Guide*.

When you grant permissions, you decide who gets the permissions, the resources they get permissions for, and the specific actions that you want to allow on those resources.

Topics

Amazon Inspector Resources and Operations

In Amazon Inspector, the primary resources are resource groups, assessment targets, assessment templates, assessment runs, and findings. These resources have unique Amazon Resource Names (ARNs) associated with them, as shown in the following table.

Resource Type	ARN Format
Resource Group	`arn:aws:inspector:region:account-id:resourcegroup/ID`
Assessment Target	`arn:aws:inspector:region:account-id:target/ID`
Assessment Template	`arn:aws:inspector:region:account-id:target/ID:template:ID`
Assessment Run	`arn:aws:inspector:region:account-id:target/ID/template/ID/run/ID`
Finding	`arn:aws:inspector:region:account-id:target/ID/template/ID/run/ID/finding/ID`

Amazon Inspector provides a set of operations to work with the Amazon Inspector resources. For a list of available operations, see Actions.

Understanding Resource Ownership

A *resource owner* is the AWS account that creates the resource. That is, the resource owner is the AWS account of the *principal entity* (the root account, an IAM user, or an IAM role) that authenticates the request that creates the resource. The following examples illustrate how this works:

- If you use the root account credentials of your AWS account to create an Amazon Inspector assessment target, your AWS account is the owner of this resource.
- If you create an IAM user in your AWS account and grant permissions to create an assessment target to that user, the user can create the target. However, your AWS account, to which the user belongs, owns the assessment target resource.
- If you create an IAM role in your AWS account with permissions to create an assessment target, anyone who can assume the role can create a target. However, your AWS account, to which the role belongs, owns the Amazon Inspector assessment target resource.

Managing Access to Resources

A *permissions policy* describes who has access to what. The following section explains the available options for creating permissions policies.

> **Note**
> This section discusses using IAM in the context of Amazon Inspector. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see What Is IAM? in the *IAM User Guide*. For information about IAM policy syntax and descriptions, see the AWS IAM Policy Reference in the *IAM User Guide*.

Policies that are attached to an IAM identity are called *identity-based* policies (IAM policies). Policies attached to a resource are called *resource-based* policies. Amazon Inspector supports only identity-based policies.

Topics

Identity-based Policies (IAM Policies)

You can attach policies to IAM identities. For example, you can do the following:

- **Attach a permissions policy to a user or a group in your account** – An account administrator can use a permissions policy that is associated with an IAM user to grant permissions for that user to create an assessment target.
- **Attach a permissions policy to a role (grant cross-account permissions)** – You can attach an identity-based permissions policy to an IAM role to grant cross-account permissions. For example, the administrator in Account A can create a role to grant cross-account permissions to another AWS account (for example, Account B) or an AWS service as follows:
  - Account A administrator creates an IAM role and attaches a permissions policy to the role that grants permissions for resources in Account A.
  - Account A administrator attaches a trust policy to the role that identifies Account B as the principal that can assume the role.
  - Account B administrator can then delegate permissions to assume the role to any users in Account B. Doing this allows users in Account B to create or access resources in Account A. If you want to grant AWS service permissions to assume the role, the principal in the trust policy can also be an AWS service principal.

  For more information about using IAM to delegate permissions, see Access Management in the *IAM User Guide*.

The following is an example policy that grants permissions for the `inspector:ListFindings` operation on all resources:

```
                {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information about using identity-based policies with Amazon Inspector, see Using Identity-based Policies (IAM Policies) for Amazon Inspector (p. 80). For more information about users, groups, roles, and permissions, see Identities (Users, Groups, and Roles) in the *IAM User Guide*.

Resource-based Policies

Other services, such as Amazon S3, also support resource-based permissions policies. For example, you can attach a policy to an S3 bucket to manage access permissions to that bucket. Amazon Inspector doesn't support resource-based policies.

Specifying Policy Elements: Actions, Effects, Resources, and Principals

For each Amazon Inspector resource (see Amazon Inspector Resources and Operations (p. 78)), the service defines a set of API operations (see Actions). To grant permissions for these API operations, Amazon Inspector defines a set of actions that you can specify in a policy. Performing an API operation can require permissions for more than one action. When granting permissions for specific actions, you also identify the resource on which the actions are allowed or denied.

The following are the most basic policy elements:

- **Resource** – In a policy, you use an Amazon Resource Name (ARN) to identify the resource to which the policy applies. For more information, see Amazon Inspector Resources and Operations (p. 78).
- **Action** – You use action keywords to identify resource operations that you want to allow or deny. For example, the `inspector:ListFindings` permission allows the user permissions to perform the Amazon Inspector `ListFindings` operation.
- **Effect** – You specify the effect when the user requests the specific action. The effect can be either allow or deny. If you don't explicitly grant access to allow a resource, access is implicitly denied. You can also explicitly deny access to a resource. You might want to do that to make sure that a user can't access it, even if a different policy grants access.
- **Principal** – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal.

To learn more about IAM policy syntax and descriptions, see the AWS IAM Policy Reference in the *IAM User Guide*.

For a table that shows all the Amazon Inspector API actions and the resources that they apply to, see Amazon Inspector API Permissions: Actions, Resources, and Conditions Reference (p. 83).

Specifying Conditions in a Policy

When you grant permissions, you can use the IAM policy language to specify the conditions that must be met for a policy to take effect. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy's language, see Condition in the *IAM User Guide*.

To express conditions, you use predefined condition keys. There are no condition keys that are specific to Amazon Inspector. However, there are AWS condition keys that you can use as appropriate. For a complete list of AWS keys, see Available Keys for Conditions in the *IAM User Guide*.

Using Identity-based Policies (IAM Policies) for Amazon Inspector

This chapter provides examples of identity-based permissions policies, also known as IAM policies. An account administrator can attach these permissions policies to IAM identities (that is, users, groups, and roles).

> **Important**
> We recommend that you first review the introductory topics that explain the basic concepts and options available for you to manage access to your Amazon Inspector resources. For more information, see Overview of Managing Access Permissions to Your Amazon Inspector Resources (p. 77).

The sections in this chapter cover the following:

The following is an example of a permissions policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

This example policy includes a statement that grants permission to list Amazon Inspector findings. Amazon Inspector doesn't support permissions for this particular action at the resource level. Therefore, the policy specifies a wildcard character (*) as the `Resource` value.

Permissions Required to Use the Amazon Inspector Console

To use the Amazon Inspector console, a user must have permissions granted by the `AmazonInspectorFullAccess` or `AmazonInspectorReadOnlyAccess` policies described in AWS Managed (Predefined) Policies for Amazon Inspector (p. 81). If you create an IAM policy that is more restrictive than the minimum required permissions described in either of these policies (such as the preceding example policy), the console won't function as intended for users with that policy.

> **Note**
> An IAM user that has the preceding example policy attached can successfully list Amazon Inspector findings by calling the `ListFindings` API operation or the `list-findings` CLI command.

AWS Managed (Predefined) Policies for Amazon Inspector

AWS addresses many common use cases by providing standalone IAM policies that are created and administered by AWS. These *managed policies* grant necessary permissions for common use cases so that you can avoid having to investigate which permissions are needed. For more information, see AWS Managed Policies in the *IAM User Guide*.

The following AWS managed policies, which you can attach to IAM users in your account, are specific to Amazon Inspector:

- `AmazonInspectorFullAccess` – Provides full access to Amazon Inspector.
- `AmazonInspectorReadOnlyAccess` – Provides read-only access to Amazon Inspector.

You can also create custom IAM policies that allow users to access the required API operations and resources. You can attach these custom policies to the IAM users or groups that require those permissions.

Customer Managed Policy Examples

This section provides example user policies that grant permissions for various Amazon Inspector operations.

Note
All examples use the US West (Oregon) Region (`us-west-2`) and contain fictitious account IDs.

Examples

Example 1: Allow a User to Perform Any Describe and List Operations on Any Amazon Inspector Resource

The following permissions policy grants a user permission to run all the operations that begin with `Describe` and `List`. These operations show information about an Amazon Inspector resource, such as an assessment target or finding. The wildcard character (*) in the `Resource` element indicates that the operations are allowed for all Amazon Inspector resources that are owned by the account:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

Example 2: Allow a User to Perform Describe and List Operations Only on Amazon Inspector Findings

The following permissions policy grants a user permission to run only `ListFindings` and `DescribeFindings` operations. These operations show information about Amazon Inspector findings. The wildcard character (*) in the `Resource` element indicates that the operations are allowed for all Amazon Inspector resources that are owned by the account.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
```

```
            ],
            "Resource":"*"
        }
    ]
}
```

Amazon Inspector API Permissions: Actions, Resources, and Conditions Reference

The following table lists each Amazon Inspector API operation. It also lists the corresponding action that you use to grant permissions to perform the action, and the AWS resource for which you can grant the permissions. Use it as a reference when setting up Access Control (p. 77) and writing permissions policies that you can attach to an IAM identity (identity-based policies). You specify the actions in the policy's `Action` field, and the resource value in the policy's `Resource` field.

You can use AWS condition keys in your Amazon Inspector policies to express conditions. For a complete list of AWS keys, see Available Keys for Conditions in the *IAM User Guide*.

Note
To specify an action, use the `inspector:` prefix followed by the API operation name, for example, `inspector:CreateResourceGroup`.

Amazon Inspector ARNS for Rules Packages

The following tables show the ARNs for Amazon Inspector rules packages in all supported Regions.

Topics

US West (Oregon)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p`	
CIS Operating System Security Configuration Benchmarks	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc`	
Network Reachability	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl`	
Security Best Practices	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ`	
Runtime Behavior Analysis	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-vg5GGHSD`	

US East (N. Virginia)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8	
Network Reachability	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd	
Security Best Practices	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q	
Runtime Behavior Analysis	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gBONHN9h	

US East (Ohio)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh	
Network Reachability	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30	
Security Best Practices	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX	
Runtime Behavior Analysis	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-UCYZFKPV	

US West (N. California)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX	
Network Reachability	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF	
Security Best Practices	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm	
Runtime Behavior Analysis	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-yeYxlt0x	

Asia Pacific (Mumbai)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m	
Network Reachability	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1	
Security Best Practices	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj	
Runtime Behavior Analysis	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-EhMQZy6C	

Asia Pacific (Sydney)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-D5TGAxiR	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-Vkd2Vxjq	
Network Reachability	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-FLcuV4Gz	
Security Best Practices	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-asL6HRgN	
Runtime Behavior Analysis	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-P8Tel2Xj	

Asia Pacific (Seoul)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-T9srhg1z	
Network Reachability	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-s3OmLzhL	
Security Best Practices	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-2WRpmi4n	
Runtime Behavior Analysis	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoYq7lI7	

Asia Pacific (Tokyo)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-gHP9oWNT	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-7WNjqgGu	
Network Reachability	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7	
Security Best Practices	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq	
Runtime Behavior Analysis	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-knGBhqEu	

EU (Ireland)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh	
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F	
Network Reachability	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SPzU33xe	
Security Best Practices	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6	
Runtime Behavior Analysis	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-lLmwe1zd	

EU (Frankfurt)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-wNqHa8M9
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
Network Reachability	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
Security Best Practices	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB
Runtime Behavior Analysis	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-0GMUM6fg

AWS GovCloud (US-East)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFuOb
CIS Operating System Security Configuration Benchmarks	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-pTLCdIww
Security Best Practices	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD
Runtime Behavior Analysis	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-850TmCFX

AWS GovCloud (US-West)

Rules Package Name	ARN	
Common Vulnerabilities and Exposures	`arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G`	
CIS Operating System Security Configuration Benchmarks	`arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc`	
Security Best Practices	`arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G`	
Runtime Behavior Analysis	`arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-JMyjuzoW`	

Document History

Latest documentation update: November 12, 2018

The following table describes the documentation release history of Amazon Inspector after May 2018.

update-history-change	update-history-description	update-history-date
Added OS Support (p. 91)	Added Amazon Inspector support for CentOS 7.6. For more information, see Amazon Inspector Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems.	December 3, 2018
New content (p. 91)	Added the Amazon Inspector Network Reachability rules package, which allows users to run agentless assessments that analyze network configuration for security vulnerabilities. For more information, see Network Reachability.	November 9, 2018
Added OS Support (p. 91)	Added Amazon Inspector support for RHEL 7.6. For more information, see Amazon Inspector Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems.	October 30, 2018
Added OS support (p. 91)	Added support for various operating systems to the CIS Benchmark rules package. For more information, see Center for Internet Security (CIS) Benchmarks and Rules Packages Availability Across Supported Operating Systems.	August 13, 2018
Added Region support (p. 91)	Added Region support for `AWS GovCloud (US)`.	June 13, 2018

The following table describes the documentation release history of Amazon Inspector before June 2018.

Change	Description	Date
New content	Added the ability to target all Amazon EC2 instances in an account. For more information, see Amazon Inspector Assessment Targets (p. 34).	May 24, 2018

Change	Description	Date
Added OS support	Added Amazon Inspector support for Amazon Linux 2018.03 and Ubuntu 18.04.	May 15, 2018
New content	Added ability to set up recurring Amazon Inspector assessments.	April 30, 2018
New content	Added ability to install an Amazon Inspector agent through the console.	April 30, 2018
Added OS support	Added Amazon Inspector support for Amazon Linux 2.	March 13, 2018
Added OS support	Added Amazon Inspector assessment support for Windows Server 2016 Base.	February 20, 2018
Added Region support	Added Amazon Inspector support for the `US East (Ohio)` Region.	February 7, 2018
New content	Amazon Inspector assessments can now run when the kernel module is unavailable.	January 11, 2018
Added Region support	Added Amazon Inspector support for the `EU (Frankfurt)` Region.	December 19, 2017
New content	Added ability to check Amazon Inspector agent health with the Amazon Inspector API and console.	December 15, 2017
New content	Added the following features: • Service-linked role usage • Amazon Inspector agent AMI available in the AWS Marketplace • Amazon Inspector AWS CloudFormation templates	December 5, 2017
Added OS support	Added Amazon Inspector assessment support for CentOS 7.4.	November 9, 2017
Added OS support	Added Amazon Inspector assessment support for Amazon Linux 2017.09.	October 11, 2017
Added OS support	Added Amazon Inspector assessment support for RHEL 7.4.	February 20, 2018

Change	Description	Date
Added HIPAA eligibility	Amazon Inspector is now HIPAA eligible.	July 31, 2017
New content	Added ability to automatically trigger Amazon Inspector security assessment with Amazon CloudWatch Events.	July 27, 2017
Added Region support	Added Amazon Inspector support for the `US West (N. California)` Region.	June 6, 2018
Added OS support	Added Amazon Inspector assessment support for RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9, and CentOS 7.2-7.3.	May 23, 2017
Added OS support	Added Amazon Inspector assessment support for Amazon Linux 2017.03.	April 25, 2017
New content and added OS support	Added: • Amazon Inspector support for Ubuntu 16.04. • Availability of Lambda blueprint for automating Amazon Inspector operations.	January 5, 2017
New OS support	Added Amazon Inspector support for Microsoft Windows.	August 26, 2016
Added Region support	Added Amazon Inspector support for the `Asia Pacific (Seoul)` Region.	August 26, 2016
Added Region support	Added Amazon Inspector support for the `Asia Pacific (Mumbai)` Region.	April 25, 2016
Added Region support	Added Amazon Inspector support for the `Asia Pacific (Sydney)` Region.	April 25, 2016
Service launch	Amazon Inspector serviced launched.	Oct 7, 2015

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the *AWS General Reference*.