aws

User Guide

Amazon Inspector Classic

Version Latest

Amazon Inspector Classic: User Guide

Table of Contents

End of support notice: On May 20, 2026, AWS will end support for Amazon Inspector Classic. After May 20, 2026, you will no longer be able to access the Amazon Inspector Classic console or Amazon Inspector Classic resources. Amazon Inspector Classic no longer available to new accounts and accounts that have not completed an assessment in the last 6 months. For all other accounts, access will remain valid until May 20, 2026, after which you will no longer be able to access the Amazon Inspector Classic console or Amazon Inspector Classic resources. For more information, see Amazon Inspector Classic end of support.

What is Amazon Inspector Classic?

Note

The new Amazon Inspector, a completely rearchitected and redesigned version of Amazon Inspector Classic, is now available across AWS Regions. The new Amazon Inspector has expanded coverage to add support for container images residing in Amazon Elastic Container Registry (Amazon ECR) in addition to EC2 instances. The new Amazon Inspector offers multi-account support through integration with AWS Organizations, and continual software vulnerability and network reachability scanning based on common vulnerabilities and exposures (CVEs). We encourage you to explore and use these and other new and improved features, and to benefit from the significantly enhanced security value. To learn about features and pricing for the new Amazon Inspector, see Amazon Inspector. To learn how to move to the new Amazon Inspector, see Amazon Inspector Classic end of support.

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

With Amazon Inspector Classic, 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 Classic 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 Classic 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 Classic terminology, see Amazon Inspector Classic terminology and concepts.

Benefits of Amazon Inspector Classic

Here are some of the main benefits of Amazon Inspector Classic:

- **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 Classic produces.

Features of Amazon Inspector Classic

Here are some of the main features of Amazon Inspector Classic:

- **Configuration scanning and activity monitoring engine** – Amazon Inspector Classic 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 Classic 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 Classic 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.

Accessing Amazon Inspector Classic

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

Amazon Inspector Classic Console

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

The console is a browser-based interface that lets you access and use the Amazon Inspector Classic 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 Classic service. For information about the AWS SDKs, including how to download and install them, see Tools for Amazon Web Services.

Amazon Inspector Classic HTTPS API

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

Amazon Inspector Classic terminology and concepts

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

Amazon Inspector Classic agent

A software agent that you can install on the EC2 instances that are included in the assessment target. The agent collects a wide set of configuration data (telemetry). For more information, see Amazon Inspector Classic agents.

Assessment run

The process of discovering potential security issues through the analysis of your assessment target's configuration against specified rules packages. During an assessment run, Amazon Inspector monitors, collects, and analyzes configuration data (telemetry) from resources within the specified target. 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 Classic assessment templates and assessment runs.

Assessment target

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

> **Important**
>
> Currently, your Amazon Inspector Classic assessment targets can consist only of EC2 instances. For more information, see Amazon Inspector Classic service limits

To create an Amazon Inspector Classic 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 Classic assessment targets.

Assessment template

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

- Rules packages that Amazon Inspector Classic uses to evaluate your assessment target
- Amazon SNS topics that you want Amazon Inspector Classic 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 Classic discovers during an assessment run of the specified target. Findings are displayed in the Amazon Inspector Classic 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 Classic findings.

Rule

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

Rules package

In the context of Amazon Inspector Classic, 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 Classic assessment template. For more information, see Amazon Inspector Classic rules packages and rules.

Telemetry

Installed package information and software configuration for an EC2 instance. Amazon Inspector Classic collects the data during an assessment run.

Amazon Inspector Classic service limits

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

Important

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

The following are Amazon Inspector Classic 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

Resource	Default Limit	Comments
		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 Classic pricing

Amazon Inspector Classic pricing is based on the number of EC2 instances included in each assessment and the rules packages used in those assessments.

Pricing for the network reachability rules package

Amazon Inspector Classic assessments with the network reachability rules packages are priced per instance per assessment (instance-assessment) per month. For example, if you run 1 assessment against 1 instance, that is 1 instance-assessment. If you run 1 assessment against 10 instances, that is 10 instance-assessments. The pricing starts at $0.15 per instance-assessment per month with volume discounting to achieve as low as $0.04 per instance-assessment per month.

Free trial details

First 90-days using Amazon Inspector Classic	Per instance-assessment price
First 250 instance-assessments	$0.00

Pricing details

In a given month	Per instance-assessment price
First 250 instance-assessments	$0.15
Next 750 instance-assessments	$0.13
Next 4,000 instance-assessments	$0.10
Next 45,000 instance-assessments	$0.07
All other instance-assessments	$0.04

Pricing for host assessment rules packages

For any combination of Common Vulnerabilities and Exposures (CVE), Center for Internet Security (CIS) benchmarks, Security Best Practices, and Runtime Behavior Analysis included in assessments

Amazon Inspector Classic's host assessment rules packages use an agent deployed on the Amazon EC2 Instances running the applications you want to assess. Assessments with the host rules packages are priced per agent per assessment (agent-assessment) per month. For example, if you run 1 assessment against 1 agent, that is 1 agent-assessment. If you run 1 assessment against 10 agents, that is 10 agent-assessments. The pricing starts at $0.30 per agent-assessment per month with volume discounting to achieve as low as $0.05 per agent-assessment per month.

Free trial details

First 90-days using Amazon Inspector Classic	Per agent-assessment price
First 250 agent-assessments	$0.00

Pricing details

In a given month	Per agent-assessment price
First 250 agent-assessments	$0.30
Next 750 agent-assessments	$0.25
Next 4,000 agent-assessments	$0.15
Next 45,000 agent-assessments	$0.10
All other agent-assessments	$0.05

Amazon Inspector Classic supported operating systems and Regions

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

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

For information about the Amazon Inspector Classic rules packages that are available across supported operating systems, see Amazon Inspector Classic rules packages for supported operating systems.

Topics

- Supported Linux-based operating systems for the Amazon Inspector Classic agent
- Supported Windows-based operating systems for the Amazon Inspector Classic agent
- Supported AWS Regions

Supported Linux-based operating systems for the Amazon Inspector Classic agent

You can use the Amazon Inspector Classic agent on 64-bit x86 and Arm EC2 instances. The agent is compatible with the following versions of Linux-based operating systems:

- **64-bit x86 instances**
  - Amazon Linux 2
  - 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 (20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)
  - Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
  - Red Hat Enterprise Linux (8.x, 7.2, 6.2 - 6.9)
  - CentOS (7.2 - 7.x, 6.2 - 6.9)
- **Arm instances**
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS, 16.04 LTS)

Supported Windows-based operating systems for the Amazon Inspector Classic agent

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

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Supported AWS Regions

Amazon Inspector Classic is supported in the following AWS Regions:

- US East (Ohio) us-east-2
- US East (N. Virginia) us-east-1
- US West (N. California) us-west-1
- US West (Oregon) us-west-2
- Asia Pacific (Mumbai) ap-south-1
- Asia Pacific (Seoul) ap-northeast-2
- Asia Pacific (Sydney) ap-southeast-2
- Asia Pacific (Tokyo) ap-northeast-1
- Europe (Frankfurt) eu-central-1
- Europe (Ireland) eu-west-1
- Europe (London) eu-west-2
- Europe (Stockholm) eu-north-1
- AWS GovCloud (US-East) gov-us-east-1
- AWS GovCloud (US-West) gov-us-west-1

Note

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

Amazon Inspector Classic end of support

After careful consideration, we decided to end support for Amazon Inspector Classic, effective May 20, 2026. Amazon Inspector Classic will no longer accept new customers beginning May 20, 2025. As an existing customer with an account signed up for the service before May 20, 2025, you can continue to use Amazon Inspector Classic features. After May 20, 2026, you will no longer be able to use Amazon Inspector Classic.

The new Amazon Inspector is now available globally in AWS Regions. The new Amazon Inspector is a completely rearchitected and redesigned version of the existing Amazon Inspector, now called Amazon Inspector Classic. The following capabilities are the key Amazon Inspector enhancements:

- **Built for scale** – The new Amazon Inspector is built for scale and the dynamic cloud environment. There is no limit to the number of instances or images that can be scanned in an account.
- **Support for container images** – The new Amazon Inspector also scans container images residing in Amazon Elastic Container Registry (Amazon ECR) for software vulnerabilities.
- **Support for multi-account management** – The new Amazon Inspector is integrated with Organizations. This allows you to delegate an administrator account for Amazon Inspector from your organization. The delegated administrator account is a centralized account that consolidates all findings and can configure all member accounts.
- **Uses AWS Systems Manager Agent (SSM Agent)** – With the new Amazon Inspector, you no longer need to install and maintain a stand-alone Amazon Inspector agent on all of your EC2 instances. The new Amazon Inspector leverages the widely-deployed SSM Agent.
- **Automated and continual scanning** – With Amazon Inspector Classic, you manually set up assessment targets, assessment templates, and configure the frequency of the assessments. However, the new version of Amazon Inspector automatically detects all newly launched EC2 instances and eligible container images pushed to Amazon ECR and immediately scans them for software vulnerabilities and unintended network exposure. The resources are automatically re-scanned based on several triggers, including a new EC2 instance being launched, a container image being pushed to Amazon ECR, installation of a new package in an EC2 instance, installation of a patch, or publication of a new Common Vulnerabilities and Exposure (CVE) that impacts the resource.
- **Amazon Inspector risk score** – The new Amazon Inspector calculates an Amazon Inspector risk score to help prioritize your findings. The risk score is calcuatled by correlating up-to-date CVE

information with temporal and environmental factors like network accessibility and exploitability information.

- **More integrations** – All findings are aggregated in a newly designed Amazon Inspector console and pushed to AWS Security Hub CSPM and Amazon EventBridge to automate workflows, such as ticketing. Container image related findings are also pushed to Amazon ECR.

To learn about all features and pricing for the new Amazon Inspector, see the Amazon Inspector User Guide.

While we will continue to support Amazon Inspector Classic for some time, and customers can use both the new Amazon Inspector and Amazon Inspector Classic in the same account, we highly encourage you to migrate to the new Amazon Inspector. The following sections walks you through the process of moving from Amazon Inspector Classic to the new Amazon Inspector.

Topics

Step 1: (Optional) Export assessment reports and findings

To save the assessment reports and findings in Amazon Inspector Classic, generate an assessment report.

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 **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's when assessment reports in Amazon Inspector Classic became available.

3. In the **Assessment report** dialog box, choose the type of report that you want to view (either a **Findings** report or a **Full** report) and the report format (HTML or PDF). Then choose **Generate report**.

Step 2: Delete all scheduled assessment runs in Amazon Inspector Classic

To disable Amazon Inspector Classic, delete all the assessment templates in your account in all active AWS Regions. Deleting assessment templates stops all your scheduled future assessment runs.

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.

Step 3: Enable the new Amazon Inspector

You can enable the new Amazon Inspector using the AWS Management Console or the new Amazon Inspector APIs. To get started with the new Amazon Inspector, see Getting Started in the *Amazon Inspector User Guide*.

Getting started with Amazon Inspector Classic

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

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 Amazon Elastic Compute Cloud (Amazon EC2) instances in the current AWS account and AWS Region.

1. Sign in to the AWS Management Console and open the Amazon Inspector Classic 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 Classic agent. **Host Assessments** analyze the on-host software and configurations of your EC2 instances for vulnerabilities, and require 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.

      > **Note**
      >
      > To identify the EC2 instances that are specified in the assessment targets, Amazon Inspector Classic needs to enumerate your EC2 instances and tags. Amazon Inspector Classic 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 Classic and Using Service-Linked Roles.

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

> **Note**
>
> The service installs an Amazon Inspector Classic 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.

c. Adds those instances to an assessment target.

d. Includes that target in an assessment template 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 Classic 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 allow System Manager Run Command. The service installs an Amazon Inspector Classic agent on all EC2 instances in the assessment target that allow AWS Systems Manager. 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. If you want to manually install the agent, see Installing Amazon Inspector Agents.

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.
8. For **Duration**, choose the duration of your assessment run.
9. (Optional) For **Assessment Schedule**, 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're 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 Classic needs to enumerate your EC2 instances and tags. Amazon Inspector Classic gets access to these resources in your AWS account through a service-linked role called `AWSServiceRoleForAmazonInspector`. For more information about using service-linked roles in Amazon Inspector Classic, see Using service-linked roles for Amazon Inspector Classic. For detailed information about using service-linked roles, see Using service-linked roles in the *AWS Identity and Access Management User Guide*.

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 Classic findings*.

Tutorials for Amazon Inspector Classic

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

Tutorials

- Tutorial: Using Amazon Inspector Classic with Red Hat Enterprise Linux
- Tutorial: Using Amazon Inspector Classic with Ubuntu Server

Amazon Inspector Classic tutorial - Red Hat Enterprise Linux

Before you follow the instructions in this tutorial, we recommend that you get familiar with the Amazon Inspector Classic terminology and concepts.

This tutorial shows how to use Amazon Inspector Classic 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 Classic 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 Classic assessment with one click, see Creating a Basic Assessment.

Topics

- Step 1: Set up an Amazon EC2 instance to use with Amazon Inspector Classic
- Step 2: Modify your Amazon EC2 instance
- Step 3: Create an assessment target and install an agent on the EC2 instance
- Step 4: Create and run your assessment template
- Step 5: Locate and analyze your finding
- Step 6: Apply the recommended fix to your assessment target

Step 1: Set up an Amazon EC2 instance to use with Amazon Inspector Classic

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.

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 Classic 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 Classic 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 Classic 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 Classic agent using the AWS Systems Manager Run Command. 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 Classic agent on your EC2 instance manually. For more information, see Installing Amazon Inspector Classic agents.

e. Choose **Save**.

> **Note**
>
> At this point, Amazon Inspector Classic creates a service-linked role called `AWSServiceRoleForAmazonInspector`. The role grants Amazon Inspector Classic the necessary access to your resources. For more information, see Creating a service-linked role for Amazon Inspector Classic.

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 Classic 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 Classic 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 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 Classic tutorial - Ubuntu Server

Before you follow the instructions in this tutorial, we recommend that you get familiar with the Amazon Inspector Classic terminology and concepts.

This tutorial shows how to use Amazon Inspector Classic 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 Classic workflow.

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

Topics

Step 1: Set up an Amazon EC2 instance to use with Amazon Inspector Classic

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: Create an assessment target and install an agent on the EC2 instance

Amazon Inspector Classic 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 Classic 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 Classic 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. 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 Classic agents.

6. Choose **Save**.

> **Note**
>
> At this point, a service-linked role called `AWSServiceRoleForAmazonInspector` is created to grant Amazon Inspector Classic access to your resources. For more information, see Creating a service-linked role for Amazon Inspector Classic.

Step 3: 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 4: Locate and analyze generated findings

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

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.

   To expand the view and see the details of a 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 the finding
   - Amazon Inspector Classic 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 5: Apply the recommended fix to your assessment target

In this procedure, you apply an update to fix the uncovered issues.

1. Connect to your instance **`InspectorEC2InstanceUbuntu`**, and perform a package update.

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 4: Locate and analyze generated findings to see the findings that result from this subsequent run of the **MyFirstTemplateUbuntu** template.

   The package update should have resolved the findings from the first run of the template.

Security in Amazon Inspector Classic

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon Inspector Classic, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Inspector Classic. The following topics show you how to configure Amazon Inspector Classic to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Inspector Classic resources.

Topics

Data protection in Amazon Inspector Classic

The AWS shared responsibility model applies to data protection in Amazon Inspector Classic. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Inspector Classic or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Topics

- Encryption of data at rest
- Encryption of data in transit

Encryption of data at rest

The telemetry data that an Amazon Inspector Classic agent generates during assessment runs is formatted in JSON files. These files are delivered in near-real-time over TLS to Amazon Inspector Classic, where they are encrypted with a per-assessment-run, ephemeral AWS KMS-derived key.

The files are securely stored in S3 buckets that are dedicated to Amazon Inspector Classic. The rules engine of Amazon Inspector Classic does the following:

- Accesses the encrypted telemetry data in the S3 bucket
- Decrypts it in memory
- Processes the data against the configured assessment rules to generate findings

Encryption of data in transit

As a managed service, Amazon Inspector Classic is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Inspector Classic through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Identity and Access Management for Amazon Inspector Classic

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in)

and *authorized* (have permissions) to use Amazon Inspector resources. IAM is an AWS service that you can use with no additional charge.

Topics

Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting Amazon Inspector Classic identity and access)
- **Service administrator** - determine user access and submit permission requests (see How Amazon Inspector Classic works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for Amazon Inspector Classic)

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-

based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon Inspector Classic works with IAM

Before you use IAM to manage access to Amazon Inspector, learn what IAM features are available to use with Amazon Inspector.

IAM features you can use with Amazon Inspector Classic

IAM feature	Amazon Inspector support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys (service-specific)	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Principal permissions	Yes
Service roles	No
Service-linked roles	Yes

To get a high-level view of how Amazon Inspector and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon Inspector

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Amazon Inspector

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector Classic.

Resource-based policies within Amazon Inspector

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon Inspector

Supports policy actions: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Inspector actions, see Actions defined by Amazon Inspector Classic in the *Service Authorization Reference*.

Policy actions in Amazon Inspector use the following prefix before the action:

```
inspector
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

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:

JSON

```
{
   "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.

JSON

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

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector Classic.

Policy resources for Amazon Inspector

Supports policy resources: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of Amazon Inspector resource types and their ARNs, see Resources defined by Amazon Inspector Classic in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions defined by Amazon Inspector Classic.

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector Classic.

Policy condition keys for Amazon Inspector

Supports service-specific policy condition keys: Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Amazon Inspector condition keys, see Condition keys for Amazon Inspector Classic in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions defined by Amazon Inspector Classic.

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector Classic.

ACLs in Amazon Inspector

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Inspector

Supports ABAC (tags in policies): Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using temporary credentials with Amazon Inspector

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Cross-service principal permissions for Amazon Inspector

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon Inspector

Supports service roles: No

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> ⚠ **Warning**
>
> Changing the permissions for a service role might break Amazon Inspector functionality. Edit service roles only when Amazon Inspector provides guidance to do so.

Service-linked roles for Amazon Inspector

Supports service-linked roles: Yes

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Amazon Inspector service-linked roles, see Using service-linked roles for Amazon Inspector Classic.

Identity-based policy examples for Amazon Inspector Classic

By default, users and roles don't have permission to create or modify Amazon Inspector resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon Inspector, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for Amazon Inspector Classic in the *Service Authorization Reference*.

Topics

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Inspector resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies*

that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Amazon Inspector console

To access the Amazon Inspector Classic console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Inspector resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon Inspector console, also attach the Amazon Inspector *ConsoleAccess* or *ReadOnly* AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

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.

JSON

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

Using service-linked roles for Amazon Inspector Classic

Amazon Inspector Classic 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 Classic. Service-linked roles are predefined by Amazon Inspector Classic 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 Classic easier because you don't have to manually add the necessary permissions. Amazon Inspector Classic defines the permissions of

its service-linked roles, and unless defined otherwise, only Amazon Inspector Classic can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting its related resources. This protects your Amazon Inspector Classic resources because you can't inadvertently remove permission to access the resources.

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 roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon Inspector Classic

Amazon Inspector Classic uses the service-linked role named **AWSServiceRoleForAmazonInspector** – ServiceLinkedRoleDescription.

The AWSServiceRoleForAmazonInspector service-linked role trusts the following services to assume the role:

- `inspector.amazonaws.com`

The role permissions policy named AmazonInspectorServiceRolePolicy allows Amazon Inspector Classic to complete the following actions on the specified resources:

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

You must configure permissions to allow an IAM entity (such as an IAM user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for Amazon Inspector Classic

You don't need to manually create a service-linked role. When you CompleteThisCreateActionInThisService in the AWS Management Console, the AWS CLI, or the AWS API, Amazon Inspector Classic creates the service-linked role for you.

Editing a service-linked role for Amazon Inspector Classic

Amazon Inspector Classic does not allow you to edit the AWSServiceRoleForAmazonInspector service-linked role. After you create a service-linked role, you cannot 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 Classic

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's 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 Classic 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 Classic resources used by `AWSServiceRoleForAmazonInspector`

- Delete your assessment targets for this AWS account in all the AWS Regions where you have Amazon Inspector Classic running. For more information, see Amazon Inspector Classic assessment targets.

To manually delete the service-linked role using IAM

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

Supported Regions for Amazon Inspector Classic service-linked roles

Amazon Inspector Classic supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS regions and endpoints.

Troubleshooting Amazon Inspector Classic identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Inspector and IAM.

Topics

I am not authorized to perform an action in Amazon Inspector

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `inspector:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector:GetWidget on resource: my-example-widget
```

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `inspector:`*`GetWidget`* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Inspector.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Inspector. However, the action requires the service to have

permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Amazon Inspector resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Inspector supports these features, see How Amazon Inspector Classic works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Logging and monitoring in Amazon Inspector Classic

Amazon Inspector Classic 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 Classic. CloudTrail captures all

API calls for Amazon Inspector Classic as events, including calls from the Amazon Inspector Classic console and code calls to the Amazon Inspector Classic API operations.

For information on using CloudTrail logging in Amazon Inspector Classic, see *Logging Amazon Inspector Classic API calls with AWS CloudTrail*.

You can monitor Amazon Inspector Classic using Amazon CloudWatch, which collects and processes raw data into readable, near-real time metrics. By default, Amazon Inspector Classic sends metric data to CloudWatch in 5-minute periods.

For information on using CloudWatch with Amazon Inspector Classic, see *Monitoring Amazon Inspector Classic using Amazon CloudWatch*.

Incident response in Amazon Inspector Classic

Incident response for Amazon Inspector Classic is an AWS responsibility. AWS has a formal, documented policy and program that governs incident response.

AWS operational issues with broad impact are posted on the AWS Service Health Dashboard.

Operational issues are also posted to individual accounts via the AWS Health Dashboard. For information on how to use the AWS Health Dashboard, see the AWS Health User Guide.

Compliance validation for Amazon Inspector Classic

Third-party auditors assess the security and compliance of Amazon Inspector Classic as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using Amazon Inspector Classic is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.

- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub CSPM – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon Inspector Classic

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Amazon Inspector Classic is highly available and executes queries using compute resources across multiple Availability Zones. It automatically routes queries appropriately if a particular Availability Zone is unreachable.

Amazon Inspector Classic uses Amazon S3 as its underlying data store, which makes your data highly available and durable. Amazon S3 provides durable infrastructure to store important data. It is designed for durability of 99.999999999% of objects. Your data is redundantly stored across multiple facilities and multiple devices in each facility.

Infrastructure security in Amazon Inspector Classic

As a managed service, Amazon Inspector Classic is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon Inspector Classic through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

For more information about Amazon Inspector Classic network and agent security, see the section called “Network and Amazon Inspector Classic agent security”.

Configuration and vulnerability analysis in Amazon Inspector Classic

Amazon Inspector Classic 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 collects a wide set of configuration data, known as telemetry. For more information about Amazon Inspector Classic agents, see *Amazon Inspector Classic agents*.

Security best practices for Amazon Inspector Classic

Amazon Inspector Classic provides a number of security features to consider as you develop and implement your own security policies. These best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

For the list of security best practices for Amazon Inspector Classic, see the section called “Security best practices for Amazon Inspector Classic”.

Amazon Inspector Classic agents

The Amazon Inspector Classic agent is an entity that collects installed package information and software configuration for an Amazon EC2 instance. Though not required in all cases, you should install the Amazon Inspector Classic agent on each of your target Amazon EC2 instances in order to fully assess their security.

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 Classic agents on Linux-based operating systems and Working with Amazon Inspector Classic agents on Windows-based operating systems.

Note

An Amazon Inspector Classic agent is not required to run the Network Reachability rules package.

Important

The Amazon Inspector Classic agent relies on Amazon EC2 instance metadata to function correctly. It accesses instance metadata using version 1 or version 2 of the Instance Metadata Service (IMDSv1 or IMDSv2). See Instance Metadata and User Data to learn more about EC2 instance metadata and access methods.

Topics

- Working with Amazon Inspector Classic agents on Windows-based operating systems
- (Optional) Verify the signature of the Amazon Inspector Classic agent installation script on Linux-based operating systems
- (Optional) Verify the signature of the Amazon Inspector Classic agent installation script on Windows-based operating systems

Amazon Inspector Classic agent privileges

You must have administrative or root permissions to install the Amazon Inspector Classic agent. On supported Linux-based operating systems, the agent consists of a user mode executable that runs with root access. 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.

Network and Amazon Inspector Classic agent security

The Amazon Inspector Classic agent initiates all communication with the Amazon Inspector Classic service. This means that the agent must have an outbound network path to public endpoints so that it can send telemetry data. For example, the agent might connect to `arsenal.<region>.amazonaws.com`, or the endpoint might be an Amazon S3 bucket at `s3.dualstack.<region>.amazonaws.com`. Make sure to replace `<region>` with the actual AWS Region where you are running Amazon Inspector Classic. 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 Classic.

The agent periodically communicates with Amazon Inspector Classic over a TLS-protected channel, which is authenticated using either the AWS identity associated with the role of the EC2 instance, or, if no role is assigned, with the instance's metadata document. When authenticated, the agent sends heartbeat messages to the service and receives instructions from the service in response. 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 Classic 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 Classic 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 Classic agent updates

As updates for the Amazon Inspector Classic 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 Classic 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 Classic agent during assessment runs is formatted in JSON files. The files are delivered in near-real-time over TLS to Amazon Inspector Classic, 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 Classic. The rules engine of Amazon Inspector Classic 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 Classic data. Currently, Amazon Inspector Classic does not provide an API or an S3 bucket access mechanism to collected telemetry.

Access control from Amazon Inspector Classic into AWS accounts

As a security service, Amazon Inspector Classic 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 Classic service. During an assessment, all communications with your environment are initiated by the Amazon Inspector Classic agent that is installed locally on EC2 instances. The Amazon Inspector Classic 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 Classic.

Amazon Inspector Classic agent limits

For information about Amazon Inspector Classic agent limits, see Amazon Inspector Classic service limits.

Installing Amazon Inspector Classic agents

You can install the Amazon Inspector Classic 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 Classic.

Installing the agent on multiple EC2 instances using the Systems Manager Run Command

You can install the Amazon Inspector Classic 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 SSM.

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

1. Open the AWS Systems Manager console at https://console.aws.amazon.com/systems-manager/.
2. In the navigation pane under **Node Tools**, 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 Classic agent on EC2 instances.
5. For **Targets**, you can select EC2 instances using different methods. To install the agent on all of the instances in the assessment target, you can specify the tags that were used to create the assessment target.
6. Provide your choices for the rest of the available options using the instructions in Running commands from the 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.

Installing the agent on a Linux-based EC2 instance

Perform the following procedure to install the Amazon Inspector Classic 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 Classic agent.

   > **Note**
   >
   > For information about the operating systems that Amazon Inspector Classic supports, see Amazon Inspector Classic supported operating systems and Regions.

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 Classic agent installation script on Linux-based operating systems.
4. To install the agent, run **sudo bash install**.

> **Note**
>
> If you are installing the agent in a SELinux environment the Amazon Inspector Classic may be detected as an unconfined daemon. You can avoid this by changing the domain of the agent process from the default `initrc_t` to `bin_t`. Use the following commands to assign the `bin_t` context to the Amazon Inspector Classic run scripts before installing the agent for SELinux:
> **sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent**
> **sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent**

> **Note**
>
> As updates for the agent become available, they are automatically downloaded from Amazon S3 and applied. For more information, see Amazon Inspector Classic agent updates.
> 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)
- `libssl1.1` (required to install the agent on Ubuntu 20.04 LTS)
- `libpcap0.8`

Installing the agent on a Windows-based EC2 instance

Perform the following procedure to install the Amazon Inspector Classic 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 Classic supports, see Amazon Inspector Classic supported operating systems and Regions.

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 Classic agent updates.
   >
   > 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 Classic agents on Linux-based operating systems

You can install, remove, verify, and modify the behavior of Amazon Inspector Classic 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 Classic, see Amazon Inspector Classic supported operating systems and Regions.

Important

The Amazon Inspector Classic agent relies on Amazon EC2 instance metadata to function correctly. It accesses instance metadata using version 1 or version 2 of the Instance Metadata Service (IMDSv1 or IMDSv2). See Instance Metadata and User Data to learn more about EC2 instance metadata and access methods.

Note

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

Topics

Verifying that the Amazon Inspector Classic 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 Classic agent

- To stop the agent, run the following command:

  sudo /etc/init.d/awsagent stop

Starting the Amazon Inspector Classic agent

- To start the agent, run the following command:

  sudo /etc/init.d/awsagent start

Modifying Amazon Inspector Classic agents settings

After the Amazon Inspector Classic 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 Classic 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 Classic agent by completing the steps in the Installing the agent on a Linux-based EC2 instance 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 Classic agent is running 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 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 Classic 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 Classic, see Amazon Inspector Classic supported operating systems and Regions.

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 Classic agents on Windows-based operating systems

You can start, stop, and modify the behavior of Amazon Inspector Classic 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 Classic, see Amazon Inspector Classic supported operating systems and Regions.

Important

The Amazon Inspector Classic agent relies on Amazon EC2 instance metadata to function correctly. It accesses instance metadata using version 1 or version 2 of the Instance Metadata Service (IMDSv1or IMDSv2). See Instance Metadata and User Data to learn more about EC2 instance metadata and access methods.

Note

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

Topics

Starting or stopping an Amazon Inspector Classic 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 Classic agent settings

After the Amazon Inspector Classic 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 Classic 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 Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

> **Important**
>
> Only HTTPS proxies are supported for Windows-based instances.

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 Classic 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 the Starting or stopping an Amazon Inspector Classic agent or verifying that the agent is running 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 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 Classic agent or verifying that the agent is running). View the status of your agent and verify that it is using the configured proxy.

Uninstalling the Amazon Inspector Classic 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 Classic agent.

   > **Note**
   >
   > For more information about the operating systems that are supported for Amazon Inspector Classic, see Amazon Inspector Classic supported operating systems and Regions.

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 Classic agent installation script on Linux-based operating systems

This topic describes the recommended process of verifying the validity of the Amazon Inspector Classic 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 Classic agent is altered or corrupted, do NOT run the installation file. Instead, contact AWS Support.

Amazon Inspector Classic 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 Classic public key and add it as a trusted key in your GPG keyring.

To authenticate and import the Amazon Inspector Classic 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.gpg`. 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.gpg**, use the following command to import the Amazon Inspector Classic public key into your keyring:

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

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 Classic 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 Classic 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://inspector-agent.amazonaws.com/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 Classic 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 Classic 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 Classic. 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 Classic agent installation script on Windows-based operating systems

This topic describes the recommended process of verifying the validity of the Amazon Inspector Classic 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 Classic 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:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

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 Web Services, Inc.**, 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:

     E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

     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 Classic assessment targets

You can use Amazon Inspector Classic 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 the section called "Supported operating systems and Regions".

Note

For information about launching EC2 instances, see the Amazon Elastic Compute Cloud documentation.

Topics

Tagging resources to create an assessment target

To create an assessment target for Amazon Inspector Classic 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 Classic 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 Classic 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 Classic assessment target limits

You can create up to 50 assessment targets per AWS account. For more information, see Amazon Inspector Classic service limits.

Creating an assessment target

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

To create an assessment target

1. Sign in to the AWS Management Console and open the Amazon Inspector Classic 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 Classic service limits.

- 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.

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 Classic 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 Classic rules packages and rules

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

In Amazon Inspector Classic, 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 Classic 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 Classic
- Rules packages in Amazon Inspector Classic

Severity levels for rules in Amazon Inspector Classic

Each Amazon Inspector Classic rule has an assigned severity level. This reduces the need to prioritize one rule over another in your analysis. 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 levels are distinguished by how likely the issue is to result in a compromise and how urgent it is to fix the issue.

The **Informational** level simply highlights a security configuration detail of your assessment target.

Here are the recommended ways to respond to issues based on their severity:

- **High** – High severity issues are extremely urgent. Amazon Inspector Classic recommends that you treat this security issue as an emergency and implement an immediate remediation.

- **Medium** – Medium severity issues are somewhat urgent. Amazon Inspector Classic recommends that you fix this issue at the next possible opportunity, for example, during your next service update.
- **Low** – Low severity issues are less urgent. Amazon Inspector Classic recommends that you fix this issue as part of one of your future service updates.
- **Informational** – These issues are purely informational. 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 Classic

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

Network assessments:

- Network Reachability

Host assessments:

- Common vulnerabilities and exposures
- Center for Internet Security (CIS) Benchmarks
- Security best practices for Amazon Inspector Classic

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 Classic 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. Do not install an agent on an operating system that Amazon Inspector Classic does not support. If an agent is present on an instance that runs an unsupported operating system, then the Network Reachability rules package will not work on that instance.

For more information, see Amazon Inspector Classic rules packages for supported operating systems.

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

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`
- `UnrecognizedPortWithListener`
- `NetworkExposure`

`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	
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

Service	TCP Ports	UDP Ports
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 Classic 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.

For the Common Vulnerabilities & Exploits (CVE) rules package, Amazon Inspector has mapped the provided CVSS Base Scoring and ALAS Severity levels provided:

Amazon Inspector Severity	CVSS Base Score	ALAS Severity (if CVSS not scored)
High	>= 5	Critical or Important
Medium	< 5 and >= 2.1	Medium
Low	< 2.1 and >= 0.8	Low
Informational	< 0.8	N/A

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)
- EU (London)
- EU (Stockholm)
- 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 Classic rules packages for supported operating systems.

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 Classic certifications, see the Amazon Web Services page on the CIS website.

Amazon Inspector Classic 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 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- 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 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 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 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- 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 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security 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 2 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 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 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 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- 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)

If a specific CIS benchmark appears in a finding that is produced by an Amazon Inspector Classic 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 Classic rules packages for supported operating systems.

Security best practices for Amazon Inspector Classic

Use Amazon Inspector Classic 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 Classic rules packages for supported operating systems.

Topics

Disable root login over SSH

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

Severity

Medium

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

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

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

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

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. You can do this by using the following option in the `pwquality.conf` file: `minlen`. For more information, see see https://linux.die.net/man/5/pwquality.conf.

If `pwquality.conf` is not available on your instance, you can set the `minlen` option using the `pam_cracklib.so` module. For more information, see `man pam_cracklib`.

The `minlen` option should be set to 14 or greater.

Configure password complexity

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

Severity

Medium

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`.

The expected value for each of these options is less than or equal to -1, as shown below:

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

Additionally, the `remember` option must be set to 12 or greater. For more information, see `man pam_unix`.

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

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.

> **Note**
>
> This rule is not supported for EC2 instances with ARM processors.

Severity

Medium

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

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 Classic assessment templates and assessment runs

Amazon Inspector Classic helps you discover potential security issues by using security rules to analyze your AWS resources. Amazon Inspector Classic 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 Classic analyzes and compares the data against a set of security rules packages. Finally, Amazon Inspector Classic 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 Classic 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 Classic assessment templates

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

- Rules packages that Amazon Inspector Classic uses to evaluate your assessment target

- Duration of the assessment run – You can set the duration of an assessment run anywhere between 3 minutes to 24 hours. We recommend setting the duration of assessment runs to 1 hour.
- Amazon SNS topics that Amazon Inspector Classic sends notifications to about your assessment run states and findings
- Amazon Inspector Classic 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 Classic 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 Classic 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 Classic assessment templates limits

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

For more information, see Amazon Inspector Classic service limits.

Creating an assessment template

To create an assessment template

1. Sign in to the AWS Management Console and open the Amazon Inspector Classic 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 Classic 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. (Optional) For **SNS topics**, specify an SNS topic that you want Amazon Inspector Classic to send notifications to about assessment run states and findings. Amazon Inspector Classic 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 Classic notifications.
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 Classic 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 Classic findings.

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 Classic automatically creates an Amazon CloudWatch Events rule for the assessment runs schedule that you are setting up. Amazon Inspector Classic 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 Classic 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.

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 Classic assessment runs limits .

If you use the Amazon Inspector Classic 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 a 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 Classic 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 Classic service limits.

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 **Create function** page, choose **Browse serverless app repository**, then enter **`inspector`** in the search field.
4. Choose the **inspector-scheduled-run** blueprint.
5. On the **Review, configure, and deploy** 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.
6. 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:

  JSON

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

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

Setting up an SNS topic for Amazon Inspector Classic 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 Classic.

To set up an SNS topic for notifications

1. Create an SNS topic. See Tutorial: Creating an Amazon SNS Topic. When you create the topic, expand the **Access policy - optional** section. Then do the following to permit the assessment to send messages to the topic:

   a. For **Choose method**, choose **Basic**.

   b. For **Define who can publish messages to the topic**, choose **Only the specified AWS accounts**, and then enter the ARN for the account in the Region that you're creating the topic in:

   - `US East (Ohio)` - *arn:aws:iam::646659390643:root*
   - `US East (N. Virginia)` - *arn:aws:iam::316112463485:root*
   - `US West (N. California)` - *arn:aws:iam::166987590008:root*
   - `US West (Oregon)` - *arn:aws:iam::758058086616:root*
   - `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*
   - `Europe (Frankfurt)` - *arn:aws:iam::537503971621:root*
   - `Europe (Ireland)` - *arn:aws:iam::357557129151:root*
   - `Europe (London)` - *arn:aws:iam::146838936955:root*
   - `Europe (Stockholm)` - *arn:aws:iam::453420244670:root*
   - `AWS GovCloud (US-East)` - *arn:aws-us-gov:iam::206278770380:root*
   - `AWS GovCloud (US-West)` - *arn:aws-us-gov:iam::850862329162:root*

   c. For **Define who can subscribe to this topic**, choose **Only the specified AWS accounts**, and then enter the ARN for the account in the Region in which you're creating the topic.

   d. To protect yourself against Inspector being used as a confused deputy as detailed in Confused deputy problem in the *IAM User Guide*, do the following:

      i. Choose **Advanced**. This will navigate you to the JSON editor.

      ii. Add the following condition:

```
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": <your account Id here>,
          "aws:SourceArn": "arn:aws:inspector:*:*:*"
        }
      }
```

e. (Optional) For additional information about aws:SourceAccount and aws:SourceArn, see Global condition context keys in the *IAM User Guide*.

f. Update other settings for the topic as needed, and then choose **Create topic**.

2. (Optional) To create an encrypted SNS topic, see Encryption at rest in the *SNS Developer Guide*.

3. To protect yourself against Inspector being used as a confused deputy for your KMS key, follow the additional steps below:

   a. Go to your CMK in the KMS console.

   b. Choose **Edit**.

   c. Add the following condition:

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. Create a subscription to the topic that you created. For more information, see Tutorial: Subscribing an Endpoint to an Amazon SNS Topic.

5. To confirm that the subscription is configured correctly, publish a message to the topic. For more information, see Tutorial: Publishing a Message to an Amazon SNS Topic.

Amazon Inspector Classic findings

Findings are potential security issues that Amazon Inspector Classic discovers during an assessment of your assessment target. Findings are displayed on the Amazon Inspector Classic 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 Classic 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 Classic findings.

To locate, analyze, and assign attributes to findings

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

   You can also see your findings in the **Notable Findings** section on the **Dashboard** page of the Amazon Inspector Classic 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 for 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 Classic assessment templates and assessment runs.

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**.

   Note that in the exported content, all datetime values are epoch timestamps.

6. To filter your current findings enter a single string you want to filter on, such as an instance ID or CVE number, in the filter bar above the findings table. To show or hide additional information columns, 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 Classic. 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 Classic *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 Classic 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**
>
> Starting on March 24, 2025, asssessment reports will no longer include severity information for network reachability findings. This information is available in the Amazon Inspector console.

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 Classic, 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 Classic

Exclusions are an output of Amazon Inspector Classic 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.

To avoid incurring unnecessary AWS fees, Amazon Inspector Classic 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.

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

Topics

Exclusion types

Amazon Inspector Classic can produce the following exclusion types.

Exclu Type	Descripti on	Recommend ation
No instar	There are no EC2 instances	Check that the tags in your

Exclu Type	Descripti on	Recommend ation
in target	with the tags specified in the assessmen t target.	assessmen t target match the tags of your target EC2 instance.
Agent is alreac runnir	An assessmen t run is already in progress on the target EC2 instance.	Wait until the current assessmen t run on the target EC2 instance has completed.

Exclu Type	Descripti on	Recommend ation
Agent not found	An Amazon Inspector Classic agent was not found on the target EC2 instance.	Install or reinstall an Amazon Inspector Classic agent on the target EC2 instance. For more informati on, see Installing Amazon Inspector Classic agents.

Exclu Type	Descripti on	Recommend ation
Agent is unhea	The Amazon Inspector Classic agent on the target EC2 instance is in an unhealthy state.	Check the status of the Amazon Inspector Classic agent on this instance and take necessary action. For more informati on, see Inspector Agents.

Exclu Type	Descripti on	Recommend ation
Unsup ed OS versio	The operating system of the target EC2 instance is not supported for Amazon Inspector Classic assessmen ts.	Remove the target EC2 instance from the assessmen t target, or create a target that doesn't include this instance. For a list of supported operating systems, see Amazon Inspector Classic Supported Operating Systems and Regions.

Exclu Type	Descripti on	Recommend ation
Depre d rules packa	The assessmen t template includes a deprecate d rules package.	Create an assessmen t template without the deprecate d rules package, and use it for future assessmen t runs.

Exclu Type	Descripti on	Recommend ation
Rules packa not suppc by OS	The operating system of the target EC2 instance is not supported by a rules package included in the assessmen t template.	Create an assessmen t template without the conflicti ng rules packages or remove the target EC2 instance from the assessmen t template. For a list of rules package support by operating system, see Rules Package Availabil ity Across Supported Operating Systems.

Exclu: Type	Descripti on	Recommend ation
Rules evalu: n error for single instar	An internal error has caused the rules evaluatio n to fail for this instance.	Attempt to run your assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.
Rules evalu: n error	An internal error has caused the rules evaluatio n to fail for your assessmen t.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – intern	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable from the internet. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – intern throu an Appli on Load Balan	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable from the internet through an Applicati on Load Balancer. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – intern throu an ELB load balan	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable from the internet though an ELB load balancer. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – VPN	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable from VPN. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – AWS Direct Conne	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable through AWS Direct Connect. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Exclu Type	Descripti on	Recommend ation
Netw Reach ity error – VPC peerir	An internal error has caused a Network Reachabil ity evaluatio n to fail on checks for ports reachable from a peered VPC. You might get findings for other Network Reachabil ity types.	Attempt to run the assessmen t again. Contact support if the exclusion persists when you rerun the assessmen t.

Previewing exclusions

Amazon Inspector Classic 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 Classic 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 Classic 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 Classic rules packages for supported operating systems

You can run Amazon Inspector Classic 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 rules package on any EC2 instance regardless of operating system.

Note

For more information about supported operating systems, see Amazon Inspector Classic supported operating systems and Regions.

Supp Oper Syste	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Amaz Linux 2	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2018	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2017	Supported	Supported	Supported	Supported	Deprecated

Supp Oper Syste	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Amaz Linux 2017	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2016	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2016	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2015	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2015	Supported	Supported	Supported	Supported	Deprecated
Amaz Linux 2014	Supported		Supported	Supported	
Amaz Linux 2014	Supported		Supported	Supported	
Amaz Linux 2013	Supported		Supported	Supported	

Supp Oper Syste	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Amaz Linux 2013	Supported		Supported	Supported	
Amaz Linux 2012	Supported		Supported	Supported	
Amaz Linux 2012	Supported		Supported	Supported	
Ubun 20.04 LTS	Supported		Supported	Supported	
Ubun 18.04 LTS	Supported	Supported	Supported	Supported	Deprecated
Ubun 16.04 LTS	Supported	Supported	Supported	Supported	Deprecated
Ubun 14.04 LTS	Supported	Supported	Supported	Supported	Deprecated

Supp Oper Syste	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	Supported		Supported	Supported	
RHEL 8.x	Supported		Supported	Supported	
RHEL 7.6 - 7.x	Supported	Supported	Supported	Supported	
RHEL 6.2 - 6.9, 7.2 - 7.5	Supported	Supported	Supported	Supported	Deprecated
Cent(7.6 - 7.X	Supported	Supported	Supported	Supported	

Supp Oper Syste	Common Vulnerabilities and Exposures	CIS Benchmarks	Network Reachability	Security Best Practices	Runtime Behavior Analysis
Cent(6.2 - 6.9, 7.2 - 7.5	Supported	Supported	Supported	Supported	Deprecated
Wind Serve 2019 Base	Supported		Supported		
Wind Serve 2016 Base	Supported	Supported	Supported		Deprecated
Wind Serve 2012 R2	Supported	Supported	Supported		Deprecated
Wind Serve 2012	Supported	Supported	Supported		Deprecated
Wind Serve 2008 R2	Supported	Supported	Supported		Deprecated

Logging Amazon Inspector Classic API calls with AWS CloudTrail

Amazon Inspector Classic 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 Classic. CloudTrail captures all API calls for Amazon Inspector Classic as events, including calls from the Amazon Inspector Classic console and code calls to the Amazon Inspector Classic 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 Classic. 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 Classic, 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 Classic API operations, see Actions in the *Amazon Inspector Classic API Reference*.

Amazon Inspector Classic information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon Inspector Classic, 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 Classic, 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 Classic 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 Classic read-only operations. Both request and response information is logged for all other Amazon Inspector Classic 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 Classic 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 Classic `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 Classic using Amazon CloudWatch

You can monitor Amazon Inspector Classic using Amazon CloudWatch, which collects and processes raw data into readable, near real-time metrics. By default, Amazon Inspector Classic 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 Classic sends to CloudWatch.

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

Amazon Inspector Classic CloudWatch metrics

The Amazon Inspector Classic 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
`TotalAssessmentRun Findings`	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

Metric	Description
TotalAssessmentRun Findings	Number of findings for this template

Aggregate metrics

Metric	Description
TotalAssessmentRuns	Number of assessment runs in this AWS account

Configuring Amazon Inspector Classic using AWS CloudFormation

For reference information about Amazon Inspector Classic 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 Classic rules packages in supported AWS Regions, see Amazon Inspector Classic ARNS for rules packages.

Integration with AWS Security Hub CSPM

AWS Security Hub CSPM provides you with a comprehensive view of your security state in AWS and helps you to check your environment against security industry standards and best practices. Security Hub CSPM collects security data from across AWS accounts, services, and supported third-party partner products and helps you to analyze your security trends and identify the highest priority security issues.

The Amazon Inspector integration with Security Hub CSPM enables you to send findings from Amazon Inspector to Security Hub CSPM. Security Hub CSPM can then include those findings in its analysis of your security posture.

Contents

How Amazon Inspector sends findings to Security Hub CSPM

In Security Hub CSPM, security issues are tracked as findings. Some findings come from issues that are detected by other AWS services or by third-party partners. Security Hub CSPM also has a set of rules that it uses to detect security issues and generate findings.

Security Hub CSPM provides tools to manage findings from across all of these sources. You can view and filter lists of findings and view details for a finding. See Viewing findings in the *AWS Security Hub User Guide*. You can also track the status of an investigation into a finding. See Taking action on findings in the *AWS Security Hub User Guide*.

All findings in Security Hub CSPM use a standard JSON format called the AWS Security Finding Format (ASFF). The ASFF includes details about the source of the issue, the affected resources, and

the current status of the finding. See AWS Security Finding Format (ASFF) in the *AWS Security Hub User Guide*.

Amazon Inspector is one of the AWS services that sends findings to Security Hub CSPM.

Types of findings that Amazon Inspector sends

Amazon Inspector sends all of the findings it generates to Security Hub CSPM.

Amazon Inspector sends the findings to Security Hub CSPM using the AWS Security Finding Format (ASFF). In ASFF, the `Types` field provides the finding type. Findings from Amazon Inspector can have the following values for `Types`.

- Software and Configuration Checks/Vulnerabilities/CVE
- Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Software and Configuration Checks/Industry and Regulatory Standards/CIS Host Hardening Benchmarks

Latency for sending findings

When Amazon Inspector creates a new finding, it is usually sent to Security Hub CSPM within five minutes.

Retrying when Security Hub CSPM is not available

If Security Hub CSPM is not available, Amazon Inspector retries sending the findings until they are received.

Updating existing findings in Security Hub CSPM

After it sends a finding to Security Hub CSPM, Amazon Inspector updates the finding to reflect additional observations of the finding activity. This will result in fewer Amazon Inspector findings in Security Hub CSPM than in Amazon Inspector.

Typical finding from Amazon Inspector

Amazon Inspector sends findings to Security Hub CSPM using the AWS Security Finding Format (ASFF).

Here is an example of a typical finding from Amazon Inspector.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
 is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
 reachable from the internet. You can install the Inspector agent on this instance
 and re-run the assessment to check for any process listening on this port. The
 instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
 eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
 the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
 from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
```

```
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
```

```
}
```

Enabling and configuring the integration

To use the integration with Security Hub CSPM, you must enable Security Hub CSPM. For information on how to enable Security Hub CSPM, see Setting up Security Hub in the *AWS Security Hub User Guide*.

When you enable both Amazon Inspector and Security Hub CSPM, the integration is enabled automatically. Amazon Inspector begins to send findings to Security Hub CSPM.

How to stop sending findings

To stop sending findings to Security Hub CSPM, you can use either the Security Hub CSPM console or the API.

See Disabling and enabling the flow of findings from an integration (console) or Disabling the flow of findings from an integration (Security Hub API, AWS CLI) in the *AWS Security Hub User Guide*.

Amazon Inspector Classic ARNs

Each resource type and rules package in Amazon Inspector Classic has a unique Amazon Resource Name (ARN) associated with it.

Contents

ARNs for Amazon Inspector Classic resources

In Amazon Inspector Classic, 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* :resource group/ *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 Classic ARNS for rules packages

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

Topics

- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

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

US East (N. Virginia)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7

Rules Package Name	ARN
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

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

Rules Package Name	ARN
Security Best Practices	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm

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

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

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-2:526

Rules Package Name	ARN
	946625049: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

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-2:454

Rules Package Name	ARN
	640832652:rulespackage/0-asL6HRgN

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

Europe (Frankfurt)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-central-1:53750

Rules Package Name	ARN
	3971621: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

Europe (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-1:35755712

Rules Package Name	ARN
	9151:rulespackage/0-SPzU33xe
Security Best Practices	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6

Europe (London)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
Network Reachability	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
Security Best Practices	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

Europe (Stockholm)

Rules Package Name	ARN
Common Vulnerabilities and Exposures	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd
CIS Operating System Security Configuration Benchmarks	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f
Network Reachability	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu
Security Best Practices	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf

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

Rules Package Name	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
Security Best Practices	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

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

Document history

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

Change	Description	Date
End of support notice	End of support notice: On May 20, 2026, AWS will end support for Amazon Inspector Classic. After May 20, 2026, you will no longer be able to access the Amazon Inspector Classic console or Amazon Inspector Classic resources . For more information, see Amazon Inspector Classic end of support.	May 20, 2025
Updated security best practices for passwords	The Amazon Inspector Classic security best practice requirements for EC2 instance password length and password complexity have been updated. See Configure password minimum length and Configure password complexity	March 8, 2021
Added support for newer operating system versions	Amazon Inspector Classic now supports the following operating system versions: Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x, and Windows Server 2019 Base.	October 15, 2020

Security information consolidated into a new security chapter	Security information for Amazon Inspector Classic, including information on managing identity and access management, is consolidated into a security chapter. See Security in Amazon Inspector Classic.	April 7, 2020
Updated documentation to remove support for the Runtime Behavior Analysis rules package.	Multiple topics were updated to remove information about the Runtime Behavior Analysis rules package, which is no longer supported.	September 5, 2019
Added OS Support	Added Amazon Inspector Classic support for CentOS 7.6. For more informati on, see Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems.	December 3, 2018
New content	Added the Amazon Inspector Classic Network Reachabil ity 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	Added Amazon Inspector Classic support for RHEL 7.6. For more informati on, see Amazon Inspector Classic Supported Operating Systems and Regions and Rules Packages Availability Across Supported Operating Systems.	October 30, 2018
Added OS support	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	Added Region support for `AWS GovCloud (US)`.	June 13, 2018

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

Change	Description	Date
New content	Added the ability to target all Amazon EC2 instances in an account. For more informati on, see Amazon Inspector Classic assessment targets.	May 24, 2018
Added OS support	Added Amazon Inspector Classic support for Amazon	May 15, 2018

Change	Description	Date
	Linux 2018.03 and Ubuntu 18.04.	
New content	Added ability to set up recurring Amazon Inspector Classic assessments.	April 30, 2018
New content	Added ability to install an Amazon Inspector Classic agent through the console.	April 30, 2018
Added OS support	Added Amazon Inspector Classic support for Amazon Linux 2.	March 13, 2018
Added OS support	Added Amazon Inspector Classic assessment support for Windows Server 2016 Base.	February 20, 2018
Added Region support	Added Amazon Inspector Classic support for the US `East (Ohio)` Region.	February 7, 2018
New content	Amazon Inspector Classic assessments can now run when the kernel module is unavailable.	January 11, 2018
Added Region support	Added Amazon Inspector Classic support for the EU `(Frankfurt)` Region.	December 19, 2017

Change	Description	Date
New content	Added ability to check Amazon Inspector Classic agent health with the Amazon Inspector Classic API and console.	December 15, 2017
New content	Added the following features: • Service-linked role usage • Amazon Inspector Classic agent AMI available in the AWS Marketplace • Amazon Inspector Classic CloudFormation templates	December 5, 2017
Added OS support	Added Amazon Inspector Classic assessment support for CentOS 7.4.	November 9, 2017
Added OS support	Added Amazon Inspector Classic assessment support for Amazon Linux 2017.09.	October 11, 2017
Added OS support	Added Amazon Inspector Classic assessment support for RHEL 7.4.	February 20, 2018
Added HIPAA eligibility	Amazon Inspector Classic is now HIPAA eligible.	July 31, 2017
New content	Added ability to automatic ally trigger Amazon Inspector Classic security assessmen t with Amazon CloudWatch Events.	July 27, 2017

Change	Description	Date
Added Region support	Added Amazon Inspector Classic support for the US `West (N. California)` Region.	June 6, 2018
Added OS support	Added Amazon Inspector Classic 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 Classic assessment support for Amazon Linux 2017.03.	April 25, 2017
New content and added OS support	Added: • Amazon Inspector Classic support for Ubuntu 16.04. • Availability of Lambda blueprint for automating Amazon Inspector Classic operations.	January 5, 2017
New OS support	Added Amazon Inspector Classic support for Microsoft Windows.	August 26, 2016
Added Region support	Added Amazon Inspector Classic support for the `Asia Pacific (Seoul)` Region.	August 26, 2016
Added Region support	Added Amazon Inspector Classic support for the `Asia Pacific (Mumbai)` Region.	April 25, 2016

Change	Description	Date
Added Region support	Added Amazon Inspector Classic support for the `Asia Pacific (Sydney)` Region.	April 25, 2016
Service launch	Amazon Inspector Classic serviced launched.	Oct 7, 2015

AWS Glossary

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