Amazon Inspector: User Guide
Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

What is Amazon Inspector? ........................................................................................................... 1  
Features ........................................................................................................................................ 1  
Accessing Amazon Inspector ....................................................................................................... 2  
Getting started tutorial ................................................................................................................. 4  
Before you begin ......................................................................................................................... 4  
Step 1: Activate Amazon Inspector ............................................................................................... 5  
Step 2: View Amazon Inspector findings ..................................................................................... 7  
Understanding the dashboard ....................................................................................................... 9  
Displaying the dashboard ............................................................................................................. 9  
Understanding dashboard components and interpreting data ..................................................... 9  
Understanding findings ............................................................................................................. 12  
Finding types ............................................................................................................................. 12  
Package vulnerability ................................................................................................................. 12  
Code vulnerability ...................................................................................................................... 13  
Network reachability .................................................................................................................. 13  
Locating and analyzing findings ................................................................................................. 14  
Finding details ............................................................................................................................ 14  
Inspector score and vulnerability intelligence ............................................................................. 16  
Amazon Inspector score .............................................................................................................. 16  
Vulnerability Intelligence ............................................................................................................ 18  
Severity levels for Amazon Inspector findings ............................................................................ 18  
Software package vulnerability severity .................................................................................... 18  
Code vulnerability severity .......................................................................................................... 19  
Network reachability severity .................................................................................................... 18  
Managing findings ..................................................................................................................... 21  
Viewing findings ......................................................................................................................... 21  
Filtering findings ......................................................................................................................... 22  
Creating filters in the Amazon Inspector console ....................................................................... 22  
Suppression rules ......................................................................................................................... 22  
Creating a suppression rule ........................................................................................................ 23  
Viewing suppressed findings ...................................................................................................... 23  
Changing suppression rules ....................................................................................................... 23  
Deleting suppression rules ......................................................................................................... 24  
Exporting findings reports ......................................................................................................... 24  
Step 1: Verify your permissions ................................................................................................. 25  
Step 2: Configure an S3 bucket ................................................................................................. 26  
Step 3: Configure an AWS KMS key .......................................................................................... 28  
Step 4: Configure and export a findings report ........................................................................ 30  
Troubleshoot errors ................................................................................................................... 32  
Automating responses to findings with EventBridge ................................................................. 32  
Event schema ............................................................................................................................. 33  
Creating an EventBridge rule to notify you of Amazon Inspector findings ................................ 34  
EventBridge for Amazon Inspector multi-account environments ............................................ 37  
Exporting SBOMs ....................................................................................................................... 38  
Amazon Inspector formats .......................................................................................................... 38  
Filters for SBOMs ....................................................................................................................... 41  
Configure and export SBOMs ....................................................................................................... 42  
Vulnerability database search ..................................................................................................... 43  
Search the Vulnerability database .............................................................................................. 43  
EventBridge schema ................................................................................................................... 45  
Amazon EventBridge base schema for Amazon Inspector ......................................................... 45  
Amazon Inspector finding event schema example .................................................................... 45  
Amazon Inspector initial scan complete event schema example ............................................ 53  
Amazon Inspector coverage event schema example .................................................................. 55
AWS managed policies ................................................................. 108
Using service-linked roles ................................................................ 114
Troubleshooting .............................................................................. 119
Monitoring Amazon Inspector .......................................................... 120
CloudTrail logs .............................................................................. 120
Compliance validation ..................................................................... 122
Resilience ..................................................................................... 122
Infrastructure security ..................................................................... 122
Incident response .......................................................................... 123
Integrations .................................................................................... 124
Integrating Amazon Inspector with Amazon ECR .............................. 124
Amazon Inspector integration with Security Hub .............................. 124
Amazon ECR integration ................................................................ 124
Activating the integration ............................................................... 124
Using the integration with a multi-account environment ................. 125
Security Hub integration ................................................................ 125
Viewing Amazon Inspector findings in AWS Security Hub ............... 125
Activating and configuring the integration ....................................... 128
Stopping the publication of findings to AWS Security Hub .......... 128
Supported operating systems and programming languages ............ 129
Supported operating systems for Amazon EC2 scanning ............... 129
Supported programming languages for Amazon Inspector Deep inspection ........................................................................ 131
Supported operating systems for Amazon ECR scanning .............. 131
Supported programming languages for Amazon ECR scanning .......... 133
Supported runtimes for Amazon Inspector Lambda standard scanning .......................................................... 133
Supported runtimes for Amazon Inspector Lambda code scanning ........................................................................ 134
Discontinued operating systems .................................................... 134
Deactivating Amazon Inspector ...................................................... 137
Deactivate Amazon Inspector ........................................................ 138
Quotas ......................................................................................... 139
Regions and endpoints .................................................................... 140
Region-specific feature availability .................................................. 140
Document history .......................................................................... 141
AWS Glossary ............................................................................ 147
What is Amazon Inspector?

Amazon Inspector is a vulnerability management service that continuously scans your AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector automatically discovers and scans running Amazon EC2 instances, container images in Amazon Elastic Container Registry (Amazon ECR), and AWS Lambda functions for known software vulnerabilities and unintended network exposure.

Amazon Inspector creates a finding when it discovers a software vulnerability or network configuration issue. A finding describes the vulnerability, identifies the affected resource, rates the severity of the vulnerability, and provides remediation guidance. You can analyze findings using the Amazon Inspector console, or view and process your findings through other AWS services. For more information, see Understanding findings in Amazon Inspector (p. 12).

Features of Amazon Inspector

Centrally manage multiple Amazon Inspector accounts

If your AWS environment has multiple accounts, you can centrally manage your environment through a single account by using AWS Organizations. Using this approach, you can designate an account as the delegated administrator account for Amazon Inspector.

Amazon Inspector can be activated for your entire organization with a single click. Additionally, you can automate activating the service for future members whenever they join your organization. The Amazon Inspector delegated administrator account can manage findings data and certain settings for members of the organization. This includes viewing aggregated findings details for all member accounts, activating or deactivating scans for member accounts, and reviewing scanned resources within the AWS organization.

Continuously scan your environment for vulnerabilities and network exposure

With Amazon Inspector, you don't need to manually schedule or configure assessment scans. Amazon Inspector automatically discovers and begins scanning your eligible resources (p. 57). Amazon Inspector continues to assess your environment throughout the lifecycle of your resources by automatically rescanning resources in response to changes that could introduce a new vulnerability, such as: installing a new package in an EC2 instance, installing a patch, and when a new common vulnerabilities and exposures (CVE) that impacts the resource is published. Unlike traditional security scanning software, Amazon Inspector has minimal impact on the performance of your fleet.

When vulnerabilities or open network paths are identified, Amazon Inspector produces a finding (p. 12) that you can investigate. The finding includes comprehensive details about the vulnerability, the affected resource, and remediation recommendations. If you appropriately remediate a finding, Amazon Inspector automatically detects the remediation and closes the finding.

Assess vulnerabilities accurately with the Amazon Inspector Risk score

As Amazon Inspector collects information about your environment through scans, it provides severity scores specifically tailored to your environment. Amazon Inspector examines the security metrics that compose the National Vulnerability Database (NVD) base score for a vulnerability and adjusts them...
according to your compute environment. For example, the service may lower the Amazon Inspector score of a finding for an Amazon EC2 instance if the vulnerability is exploitable over the network but no open network path to the internet is available from the instance. This score is in CVSS format and is a modification of the base Common Vulnerability Scoring System (CVSS) score provided by NVD.

**Identify high-impact findings with the Amazon Inspector dashboard**

The Amazon Inspector dashboard (p. 9) offers a high-level view of findings from across your environment. From the dashboard, you can access the granular details of a finding. The dashboard contains streamlined information about scan coverage in your environment, your most critical findings, and which resources have the most findings. The risk-based remediation panel in the Amazon Inspector dashboard presents the findings that affect the largest number of instances and images. This panel makes it easier to identify the findings with the greatest impact on your environment, review finding details, and review suggested solutions.

**Manage your findings using customizable views**

In addition to the dashboard, the Amazon Inspector console offers a Findings view. This page lists all findings for your environment and provides the details of individual findings. You can view findings grouped by category or vulnerability type. In each view, you can further customize your results using filters. You can also use filters to create suppression rules that hide unwanted findings from your views.

You can use filters and suppression rules to generate finding reports that show all findings or a customized selection of findings. Reports can be generated in CSV or JSON formats.

**Monitor and process findings with other services and systems**

To support integration with other services and systems, Amazon Inspector publishes findings to Amazon EventBridge (p. 32) as finding events. EventBridge is a serverless event bus service that can route findings data to targets such as AWS Lambda functions and Amazon Simple Notification Service (Amazon SNS) topics. With EventBridge, you can monitor and process findings in near-real time as part of your existing security and compliance workflows.

If you have activated AWS Security Hub (p. 125), then Amazon Inspector will also publish findings to Security Hub (p. 124). Security Hub is a service that provides a comprehensive view of your security posture across your AWS environment and helps you check your environment against security industry standards and best practices. With Security Hub, you can more easily monitor and process your findings as part of a broader analysis of your organization's security posture in AWS.

## Accessing Amazon Inspector

Amazon Inspector is available in most AWS Regions. For a list of Regions where Amazon Inspector is currently available, see Amazon Inspector endpoints and quotas in the Amazon Web Services General Reference. To learn more about AWS Regions, see Managing AWS Regions in the Amazon Web Services General Reference. In each Region, you can work with Amazon Inspector in the following ways.

**AWS Management Console**

The AWS Management Console is a browser-based interface that you can use to create and manage AWS resources. As part of that console, the Amazon Inspector console provides access to your Amazon Inspector account and resources. You can perform Amazon Inspector tasks from the Amazon Inspector console.

**AWS command line tools**

With AWS command line tools, you can issue commands at your system's command line to perform Amazon Inspector tasks. Using the command line can be faster and more convenient than using the console. The command line tools are also useful if you want to build scripts that perform tasks.
AWS provides two sets of command line tools: the AWS Command Line Interface (AWS CLI) and the AWS Tools for PowerShell. For information about installing and using the AWS CLI, see the AWS Command Line Interface User Guide. For information about installing and using the Tools for PowerShell, see the AWS Tools for PowerShell User Guide.

AWS SDKs

AWS provides SDKs that consist of libraries and sample code for various programming languages and platforms, including Java, Go, Python, C++, and .NET. The SDKs provide convenient, programmatic access to Amazon Inspector and other AWS services. They also handle tasks such as cryptographically signing requests, managing errors, and retrying requests automatically. For information about installing and using the AWS SDKs, see Tools to Build on AWS.

Amazon Inspector REST API

The Amazon Inspector REST API gives you comprehensive, programmatic access to your Amazon Inspector account and resources. With this API, you can send HTTPS requests directly to Amazon Inspector. However, unlike the AWS command line tools and SDKs, use of this API requires your application to handle low-level details such as generating a hash to sign a request.
Getting started with Amazon Inspector

This tutorial provides a hands-on introduction to Amazon Inspector.

Step 1 covers activating Amazon Inspector scans for a standalone account or as an Amazon Inspector delegated administrator with AWS Organizations in a multi-account environment.

Step 2 covers understanding Amazon Inspector findings in the console.

Note
In this tutorial, you complete tasks in your current AWS Region. To set up Amazon Inspector in other Regions, you must complete these steps in each of those Regions.

Topics
• Before you begin (p. 4)
• Step 1: Activate Amazon Inspector (p. 5)
• Step 2: View Amazon Inspector findings (p. 7)

Before you begin

Amazon Inspector is a vulnerability management service that continually scans your Amazon EC2 instances, Amazon ECR container images, and AWS Lambda functions for software vulnerabilities and unintended network exposure.

Note the following before you activate Amazon Inspector:

• Amazon Inspector is a Regional service. Any of the configuration procedures that you complete in this tutorial must be repeated in each Region that you want to monitor with Amazon Inspector.

• Amazon Inspector gives you the flexibility to activate Amazon EC2 instance, Amazon ECR container image, and AWS Lambda function scanning. You can manage the scanning types from the account management page in the Amazon Inspector console or using Amazon Inspector APIs.

• Amazon Inspector can provide Common Vulnerabilities and Exposures (CVE) data for your EC2 instances only if the Amazon EC2 Systems Manager (SSM) agent is installed and activated. This agent is preinstalled on many EC2 instances, but you might need to activate it manually. Regardless of SSM agent status, all of your EC2 instances are scanned for network exposure issues. For more information about configuring scans for Amazon EC2, see Scanning Amazon EC2 instances (p. 59). Amazon ECR and AWS Lambda function scanning do not require the use of an agent.

• An IAM user identity with administrator permissions in an AWS account can enable Amazon Inspector. For data protection purposes, we recommend that you protect your 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 manage Amazon Inspector. For information about the permissions required to enable Amazon Inspector, see AWS managed policy: AmazonInspector2FullAccess (p. 108).

• When you activate Amazon Inspector for the first time in any Region, it creates a service-linked role globally for your account called AWSServiceRoleForAmazonInspector2. This role includes the permissions and the trust policies that allow Amazon Inspector to collect software package details and
analyze Amazon VPC configurations in order to generate vulnerability findings. For more information, see Using service-linked roles for Amazon Inspector (p. 114). For more information about service-linked roles, see Using service-linked roles.

Step 1: Activate Amazon Inspector

The first step to using Amazon Inspector is to activate it for your AWS account. After you activate any Amazon Inspector scan type, Amazon Inspector immediately begins discovering and scanning all eligible resources.

If you want to manage Amazon Inspector for multiple accounts within your organization through a centralized administrator account, you must assign a delegated administrator for Amazon Inspector. Choose one of the following options to learn how to activate Amazon Inspector for your environment.

Standalone account environment

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. Choose Get Started.
3. Choose Activate Amazon Inspector.

When you activate Amazon Inspector in a standalone account, all scan types are activated by default. You can manage activated scan types from the account management page within the Amazon Inspector console or by using Amazon Inspector APIs. After Amazon Inspector is activated, it automatically discovers and begins scanning all eligible resources. Review the following scan type information to understand which resources are eligible by default:

Amazon EC2 scanning

To provide Common Vulnerabilities and Exposures (CVE) data for your EC2 instance, Amazon Inspector requires that the AWS Systems Manager (SSM) agent be installed and activated. This agent is pre-installed on many EC2 instances, but you may need to activate it manually. Regardless of SSM agent status, all of your EC2 instances will be scanned for network exposure issues. For more information about configuring scans for Amazon EC2, see Scanning Amazon EC2 instances with Amazon Inspector (p. 59).

Amazon ECR scanning

When you activate Amazon ECR scanning, Amazon Inspector converts all container repositories in your private registry that are configured for the default Basic scanning provided by Amazon ECR to Enhanced scanning with continual scanning. You can also optionally configure this setting to scan on-push only or to scan select repositories through inclusion rules. All images pushed within the last 30 days are scheduled for Lifetime scanning, this Amazon ECR scan setting can be changed at any time. For more information about configuring scans for Amazon ECR, see Scanning Amazon ECR container images with Amazon Inspector (p. 67).

AWS Lambda function scanning

When you activate AWS Lambda function scanning, Amazon Inspector discovers the Lambda functions in your account and immediately starts scanning them for vulnerabilities. Amazon Inspector scans new Lambda functions and layers when they are deployed, and rescans them when they are updated or when new Common Vulnerabilities and Exposures (CVEs) are published. Amazon Inspector offers two different levels of Lambda function scanning. By default when you first activate Amazon Inspector, Lambda standard scanning is activated, which scans package dependencies in your functions. You can additionally activate Lambda code scanning to scan the developer code in your functions for code vulnerabilities. For more information about configuring Lambda function scanning, see Scanning AWS Lambda functions with Amazon Inspector (p. 69).
Multi-account environment

**Important**
To complete these steps, you must be in the same organization as all the accounts you want to manage and have access to the AWS Organizations management account in order to delegate an administrator for Amazon Inspector within your organization. Additional permissions may be required to delegate an administrator. For more information, see Permissions required to designate a delegated administrator (p. 84).

**Note**
To programatically enable Amazon Inspector for multiple accounts in multiple Regions you can use a shell script developed by Amazon Inspector. For more information on using this script see the [inspector2-enablement-with-cli](https://github.com) on GitHub.

Delegating an administrator for Amazon Inspector

1. Log in to the AWS Organizations management account.
3. Within the **Delegated administrator** pane, enter the twelve-digit ID of the AWS account that you want to designate as the Amazon Inspector delegated administrator for the organization. Then choose **Delegate**. Then, in the confirmation window, choose **Delegate** again.

**Note**
Amazon Inspector is activated for your account when you delegate an administrator.

Adding member accounts

As a delegated administrator you can activate scanning for any member associated with the Organizations management account. This workflow activates all scan types for all member accounts. However, members can also activate Amazon Inspector for their own accounts, or scans for a service can be selectively activated by the delegated administrator. For more information, see Managing multiple accounts (p. 82).

1. Log in to the delegated administrator account.
3. In the navigation pane, choose **Account Management**. The **Accounts** table displays all of the member accounts associated with the Organizations management account.
4. From the **Account Management** page, you can choose **Activate scanning for all accounts** from the top banner to activate EC2 instances, ECR container images, and, AWS Lambda function scanning for all accounts in your organization. Alternatively, you can choose the accounts that you want to add as members by selecting them in the **Accounts** table. Then from the **Activate** menu, select **All scanning**.
5. (Optional) Turn on the **Automatically activate Inspector for new member accounts** feature and select the scan types to include to activate those scans for any new member accounts that are added to your organization.

Amazon Inspector currently offers scans for EC2 instances, ECR container images, and AWS Lambda functions. After you activate Amazon Inspector, it automatically starts discovering and scanning all eligible resources. Review the following scan type information to understand which resources are eligible by default:

**Amazon EC2 scanning**

To provide CVE vulnerability data for your EC2 instances, Amazon Inspector requires that the AWS Systems Manager (SSM) agent be installed and activated. This agent is pre-installed on many EC2 instances, but you may need to activate it manually. Regardless of SSM agent status, all of your EC2 instances will be scanned for network exposure issues. For more information
Step 2: View Amazon Inspector findings

You can view findings for your environment in the Amazon Inspector console or through the API. All findings are also pushed to Amazon EventBridge and AWS Security Hub (if activated). Additionally, container image findings are pushed to Amazon ECR.

The Amazon Inspector console offers several different viewing formats for your findings. The Amazon Inspector dashboard gives you a high-level overview of risks to your environment, while the Findings table lets you view the details of a specific finding.

In this step, you explore the details of a finding using the Findings table and Findings dashboard. For information about the Amazon Inspector dashboard, see Understanding the dashboard (p. 9).

To view details of findings for your environment in the Amazon Inspector console:

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. From the navigation pane, select Dashboard. You can select any of the links in the dashboard to navigate to a page in the Amazon Inspector console with more details about that item.
3. From the navigation pane, select Findings.
4. By default you will see the All findings tab, which displays all EC2 instance, ECR container image, AWS Lambda function findings for your environment.
5. In the Findings list, choose a finding name in the Title column to open the details pane for that finding. All findings have a Finding details tab. You can interact with the Finding details tab in the following ways:
   - For more details about the vulnerability, follow the link in the Vulnerability details section to open the documentation for this vulnerability.
   - To further investigate your resource, follow the Resource ID link in the Resource affected section to open the service console for the affected resource.

Package vulnerability type findings also have an Inspector Score and vulnerability intelligence tab explaining how the Amazon Inspector score was calculated for that finding and providing
information on the Common Vulnerability and Exploits (CVE) associated with the finding. For more details about finding types, see Finding types in Amazon Inspector (p. 12).
Understanding the Amazon Inspector dashboard

The Amazon Inspector dashboard provides a snapshot of aggregated statistics for your AWS resources in the current AWS Region. These statistics include key metrics for resource coverage and active vulnerabilities. The dashboard also displays groups of aggregated findings data for your account, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Container Registry (Amazon ECR) and AWS Lambda functions with most critical findings. To perform deeper analysis, you can view the supporting data for dashboard items.

If your account is the Amazon Inspector delegated administrator account for an organization, the dashboard includes account coverage, aggregated statistics, and findings data for all accounts in your organization, including your own account.

Displaying the dashboard

The dashboard shows an overview of your environment coverage and critical findings.

To display the dashboard:

2. In the navigation pane, choose Dashboard.
3. You can interact with the dashboard in the following ways:
   - The dashboard refreshes automatically every five minutes. However, you can refresh the data manually by selecting the refresh icon at the top-right corner of the page.
   - To view the supporting data for an item on the dashboard, choose the item.
   - If you manage multiple accounts through AWS Organizations as an Amazon Inspector delegated administrator, the dashboard displays aggregated statistics for your member accounts. To filter the dashboard and display data only for a particular account, enter the account ID in the Account box.

Understanding dashboard components and interpreting data

Each section of the Amazon Inspector dashboard provides insight into key metrics or active findings data that can help you understand the vulnerability posture of your AWS resources in the current AWS Region.

Environment coverage

The Environment coverage section provides statistics about the resources scanned by Amazon Inspector. In this section, you can see the count and percentage of Amazon EC2 instances, Amazon ECR images and AWS Lambda functions scanned by Amazon Inspector. If you manage multiple accounts through AWS Organizations as an Amazon Inspector delegated administrator, you will also see the total number of organization accounts, the number with Amazon Inspector activated, and the resulting coverage percentage for the organization. You can also use this section to determine which resources are not covered by Amazon Inspector. These resources may contain vulnerabilities
that could be exploited to put your organization at risk. For more details, see Assessing Amazon Inspector coverage of your AWS environment (p. 75).

Choosing a coverage group takes you to the Account management page for the grouping you select. The account management page shows you details about which accounts, Amazon EC2 instances, and Amazon ECR repositories are covered by Amazon Inspector.

The following coverage groups are available:

- Account
- Instances
- Container repositories
- Container images
- Lambda

Critical findings

The Critical findings section provides a count of the critical vulnerabilities in your environment and a total count of all findings in your environment. In this section, the counts are shown per resource and assessment type. For more information about critical findings and how Amazon Inspector determines criticality, see Understanding findings in Amazon Inspector (p. 12).

Choosing a critical finding group takes you to the All findings page and automatically applies filters to show all critical findings that match the grouping you selected.

The following critical finding groups are available:

- ECR container images findings
- Amazon EC2 findings
- Network reachability findings
- AWS Lambda function findings

Risk-based remediations

The Risk-based remediations section shows the top five software packages with critical vulnerabilities that affect the most resources in your environment. Remediating these packages can significantly reduce the number of critical risks to your environment. Choose the software package name to see associated vulnerability details and affected resources.

Accounts with the most critical findings

The Accounts with the most critical findings section shows the top five AWS accounts in your environment with the most critical findings, and the total number of findings for that account. This section is only viewable from the delegated administrator account when Amazon Inspector is configured for multi-account scanning with AWS Organizations. This view helps delegated administrators understand which accounts may be most at risk within the organization.

Choose Account ID to see more information about the affected member account.

Amazon ECR repositories with most critical findings

The Elastic Container Registry (ECR) Repositories with most critical findings section shows the top five Amazon ECR repositories in your environment with the most critical container image findings. The view shows the repository name, AWS account identifier, the repository creation date, number of critical vulnerabilities, and total number of vulnerabilities. This view helps you identify which repositories may be most at risk.

Choose Repository name to see more information about the affected repository.

Container images with most critical findings

The Container images with most critical findings section shows the top five container images in your environment with the most critical findings. The view shows image tag data, repository
name, image digest, AWS account identifier, number of critical vulnerabilities, and total number of vulnerabilities. This view helps application owners identify which container images may need to be rebuilt and relaunched.

Choose Container image to see more information about the affected container image.

**Instances with most critical findings**

The Instances with most critical findings section shows the top five Amazon EC2 instances with the most critical findings. The view shows instance identifier, AWS account identifier, Amazon Machine Image (AMI) identifier, number of critical vulnerabilities, and total number of vulnerabilities. This view helps infrastructure owners identify which instances may require patching.

Choose Instance ID to see more information about the affected Amazon EC2 instance.

**Amazon Machine Images (AMI) with most critical findings**

The Amazon Machine Images (AMIs) with most critical findings section shows the top five AMIs in your environment with the most critical findings. The view shows the AMI identifier, AWS account identifier, number of affected EC2 instances running in the environment, the AMI creation date, the operating system platform of the AMI, the number of critical vulnerabilities, and the total number of vulnerabilities. This view helps infrastructure owners identify which AMIs may require rebuilding.

Choose Affected instances to see more information about the instances launched from the affected AMI.

**AWS Lambda functions with most critical findings**

The AWS Lambda functions with most critical findings section shows the top five Lambda functions in your environment with the most critical findings. The view shows the Lambda function name, AWS account identifier, runtime environment, the number of critical vulnerabilities, the number of high vulnerabilities, and the total number of vulnerabilities. This view helps infrastructure owners identify which Lambda functions may require remediation.

Choose Function name to see more information about the affected AWS Lambda function.
Understanding findings in Amazon Inspector

In Amazon Inspector, a finding is a detailed report about a vulnerability that affects one of your AWS resources. Amazon Inspector generates a finding whenever it detects a vulnerability in an Amazon EC2 instance, a container image in an Amazon ECR repository, or an AWS Lambda function. Each finding has the name of the detected vulnerability and provides a severity rating, information about the affected resource, and details such as how to remediate the reported vulnerability.

Amazon Inspector continually scans your compute environment and stores your active findings until it detects that they are remediated. A remediated finding is automatically detected and closed, and then deleted after 30 days. A finding is assigned one of the following states:

**Active**

The finding is identified by Amazon Inspector and has not been remediated. Active findings are subject to suppression rules and, if applicable, the status is changed to **Suppressed**.

**Suppressed**

The finding meets one or more criteria of one or more suppression rules. Suppressed findings are hidden from most views, except for the **Suppressed findings** list. For more information about suppressed findings, see [ Suppressing Amazon Inspector findings with suppression rules (p. 22)](#).

**Closed**

After a vulnerability is remediated, Amazon Inspector automatically detects it and changes the state of the finding to closed. Closed findings are deleted after 30 days if there are no other changes.

**Topics**

- Finding types in Amazon Inspector (p. 12)
- Locating and analyzing Amazon Inspector findings (p. 14)
- Amazon Inspector finding details (p. 14)
- Inspector score and vulnerability intelligence (p. 16)
- Severity levels for Amazon Inspector findings (p. 18)

Finding types in Amazon Inspector

Amazon Inspector generates findings for Amazon Elastic Compute Cloud (Amazon EC2) instances, container images in Amazon Elastic Container Registry (Amazon ECR) repositories, and AWS Lambda functions. Amazon Inspector can generate the following types of findings.

**Package vulnerability**

Package vulnerability findings identify software packages in your AWS environment that are exposed to Common Vulnerabilities and Exposures (CVEs). Attackers can exploit these unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of data, or to access other systems. The CVE system is a reference method for publicly known information security vulnerabilities and exposures. For more information, see [https://www.cve.org/](https://www.cve.org/).
CVE detections for Linux are added to Amazon Inspector within 24 hours of release by vendor security advisories. CVE detections for Windows are added to Amazon Inspector within 48 hours of being released by Microsoft. You can use the Amazon Inspector Vulnerability database search (p. 43) to see if a CVE detection is supported.

Amazon Inspector can generate package vulnerability findings for EC2 instances, ECR container images, and Lambda functions. Package vulnerability findings have additional details unique to this finding type, these are the Inspector score and vulnerability intelligence (p. 16).

**Code vulnerability**

Code vulnerability findings identify lines in your code that attackers could exploit. Code vulnerabilities include injection flaws, data leaks, weak cryptography, or missing encryption in your code.

Amazon Inspector evaluates your Lambda function application code using automated reasoning and machine learning that analyzes your application code for overall security compliance. It identifies policy violations and vulnerabilities based on internal detectors developed in collaboration with Amazon CodeGuru. For a list of possible detections, see CodeGuru Detector Library.

**Important**

Amazon Inspector code scanning captures code snippets to highlight detected vulnerabilities. These snippets may show hardcoded credentials or other sensitive materials in plaintext.

Amazon Inspector can generate Code vulnerability findings for Lambda functions if you have Amazon Inspector Lambda code scanning (p. 71) activated.

Code snippets detected in connection with a code vulnerability are stored by the CodeGuru service. By default an AWS owned key controlled by CodeGuru is used to encrypt your code, however, you can use your own customer managed key for encryption through the Amazon Inspector API. For more information see Encryption at rest for code in your findings (p. 93).

**Network reachability**

Network reachability findings indicate that there are open network paths to Amazon EC2 instances in your environment. These findings appear when your TCP and UDP ports are reachable from the VPC edges, such as 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 highlight network configurations that may be overly permissive, such as mismanaged security groups, Access Control Lists, or internet gateways, or that may allow for potentially malicious access.

Amazon Inspector only generates network reachability findings for Amazon EC2 instances. Amazon Inspector performs scans for network reachability findings every 24 hours.

Amazon Inspector evaluates the following configurations when scanning for network paths:

- Amazon EC2 instances
- AWS Lambda functions
- Application Load Balancers
- Direct Connect
- Elastic Load Balancers
- Elastic Network Interfaces
- Internet Gateways
- Network Access Control Lists
- Route Tables
- Security Groups
Locating and analyzing Amazon Inspector findings

Use the following procedure to view and analyze your Amazon Inspector findings.

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. In the Findings table, choose a finding name in the Title column to open its details pane.
3. (Optional) View the findings grouped by one of the following categories by selecting that category from the navigation pane or the Findings table:
   - Vulnerability
   - Account
   - Instance
   - Container image
   - Repository
   - Lambda
   - All findings

The details for each finding differ depending on the finding type, resources involved, and type of vulnerability. For information about available finding fields, see Amazon Inspector finding details (p. 14).

Amazon Inspector finding details

In the Amazon Inspector console, you can view details for each finding. Finding details vary based on finding type.

To view the details for a finding

1. log in to the Amazon Inspector console at https://console.aws.amazon.com/inspector/
2. Select the Region to view findings in
3. In the navigation pane, choose Findings to display the findings list
4. (Optional) Use the filter bar to select a specific finding. For more information, see Filtering Amazon Inspector findings (p. 22).
5. Choose a finding to view it’s details panel.

The Finding details tab contains the basic identifying features of the finding. This includes the title of the finding as well as a basic description of the vulnerability identified, remediation suggestions, and a severity score. For information about scoring, see Severity levels for Amazon Inspector findings (p. 18).
Finding details

The details available for a finding varies depending on finding type and the **Resource affected**.

All findings contain the AWS Account ID number the finding was identified for, a severity, a finding **Type**, the date the finding was created at, and a **Resource affected** section with details about that resource.

The finding **Type** determines the remediation and vulnerability intelligence information available for the finding. Select from the following tabs to review the type of information available by finding type:

### Package Vulnerability

Package vulnerability findings are available for EC2 instances, ECR container images, and Lambda functions. See [Package vulnerability](p. 12) for more info.

Package vulnerability findings also include [Inspector score and vulnerability intelligence](p. 16).

This finding type has the following details:

- **Fix available** – Indicates if the vulnerability is fixed in a newer version of the affected packages.
  
  Has one of the following values:
  
  - YES, which means all the affected packages have a fixed version.
  - NO, which means no affected packages have a fixed version.
  - PARTIAL, which means one or more (but not all) of the affected packages have a fixed version.

- **Exploit available** – Indicates the vulnerability has a known exploit.
  
  - YES, which means the vulnerability discovered in your environment has a known exploit.
  - NO, which means this vulnerability doesn't have a known exploit.

- **Affected packages** – Lists each package identified as vulnerable in the finding, and the details of each package:
  
  - **Installed version / Fixed version** – The version number of the currently installed package that a vulnerability was detected for. Compare the installed version number with the value after the slash (`/`). The second value is the version number of the package that fixes the detected vulnerability as provided by the Common Vulnerabilities and Exposures (CVEs) or advisory associated with the finding. If the vulnerability has been fixed in multiple versions, this field lists the most recent version that includes the fix. If a fix isn't available, this value is **None available**.

  **Note**

  If a finding was detected before Amazon Inspector began including this field in findings, the value for this field is empty. However, a fix may be available.

  - **Package manager** – The package manager used to configure this package.

  - **Remediation** – If a fix is available through an updated package or programming library, this section includes the commands that you can run to make the update. You can copy the provided command and run it in your environment.

  **Note**

  Remediation commands are provided from vendor data feeds and may vary depending on your system configuration. Review finding references or operating system documentation for more specific guidance.

- **Vulnerability details** – Provides a link to the Amazon Inspector preferred source for the CVE identified in the finding, such as National Vulnerability Database (NVD), REDHAT, or another OS vendor. Additionally, you will find the severity scores for the finding. For more information about severity scoring such as, see [Severity levels for Amazon Inspector findings](p. 18). The following scores are included, including the scoring vectors for each:

  - EPSS score
  - Inspector score
  - CVSS 3.1 from Amazon CVE
  - CVSS 3.1 from NVD
• CVSS 2.0 from NVD (where applicable, for older CVEs)

• **Related vulnerabilities** – Specifies other vulnerabilities related to the finding. Typically these are other CVEs that impact the same package version, or other CVEs within the same group as the finding CVE, as determined by the vendor.

**Code vulnerability**

Code vulnerability findings are available for Lambda functions only. See Code vulnerability (p. 13) for more info. This finding type has the following details:

• **Fix available** – For code vulnerabilities this value is always YES.

• **Detector name** – The name of the CodeGuru detector used to detect the code vulnerability. For a list of possible detections, see the CodeGuru Detector Library.

• **Detector tags** – The CodeGuru tags associated with the detector, CodeGuru uses tags to categorize detections.

• **Relevant CWE** – IDs of the Common Weakness Enumeration (CWE)s associated with the code vulnerability.

• **File path** – The file location of the code vulnerability.

• **Vulnerability location** – For Lambda code scanning code vulnerabilities, this field shows the exact lines of code where Amazon Inspector found the vulnerability.

• **Suggested remediation** – This suggests how the code can be edited to remediate the finding.

**Network reachability**

Network reachability findings are available for EC2 instances only. See Network reachability (p. 13) for more info. This finding type has the following details:

• **Open port range** – The port range through which the EC2 instance could be accessed.

• **Open network paths** – Shows the open access path to the EC2 instance. Select an item on the path for more information.

• **Remediation** – Recommends a method for closing the open network path.

**Inspector score and vulnerability intelligence**

In the Amazon Inspector console, when you select a finding, you can view The Inspector score and vulnerability intelligence tab shows the scoring details for a package vulnerability finding, as well as vulnerability intelligence details. These details are only available for Package vulnerability (p. 12) findings.

**Amazon Inspector score**

The Amazon Inspector score is a contextualized score that Amazon Inspector creates for each EC2 instance finding. The Amazon Inspector score is determined by correlating the base CVSS v3.1 score information with information collected from your compute environment during scans, such as network reachability results and exploitability data. For example, the Amazon Inspector score of a finding may be lower than the base score if the vulnerability is exploitable over the network but Amazon Inspector determines that no open network path to the vulnerable instance is available from the internet.

The base score for a finding is the CVSS v3.1 base score provided by the vendor. RHEL, Debian, or Amazon vendor base scores are supported, for other vendors, or cases where the vendor hasnt provided a score Inspector uses the base score from the National Vulnerability Database (NVD). Inspector uses the Common Vulnerability Scoring System Version 3.1 Calculator to calculate the score. You can see the source of the base score of an individual finding in the finding’s details under vulnerability details, as Vulnerability source (or packageVulnerabilityDetails.source in the finding JSON)
Note
Amazon Inspector score isn't available for Linux instances running Ubuntu. This is because Ubuntu defines its own vulnerability severities that may differ from the associated CVE severity.

Amazon Inspector score details

When you open a finding's details you can select the Inspector score and vulnerability intelligence this panel shows the difference between the base score and the Inspector score. This section explains how Amazon Inspector assigned the severity rating based on a combination of the Amazon Inspector score and the vendor score for the software package. If the scores differ this panel shows an explanation of why.

In the CVSS score metrics section you can see a table with comparisons between the CVSS base score metrics and the Inspector score. The metrics compared are the base metrics defined in the CVSS specification document maintained by first.org. The following is a summary of the base metrics:

Attack Vector
The context by which a vulnerability can be exploited. For Inspector findings this can be Network, Adjacent Network, or Local.

Attack Complexity
This describes the level of difficulty an attacker will face when exploiting the vulnerability. A Low score means that the attacker will need to meet little or no additional conditions to exploit the vulnerability. A High score means that an attacker will need invest a considerable amount of effort in order carry out a successful attack with this vulnerability.

Privilege Required
This describes the level of privilege an attacker will need to exploit a vulnerability.

User Interaction
This metric states if a successful attack using this vulnerability requires a human user, other than the attacker.

Scope
This states whether a vulnerability in one vulnerable component impacts resources in components beyond the vulnerable component's security scope. If this value is Unchanged the affected resource and the impacted resource are the same. If this value is Changed then the vulnerable component can be exploited to impact resources managed by different security authorities.

Confidentiality
This measures the level of impact to the confidentiality of data within a resource when the vulnerability is exploited. This ranges from None, where no confidentiality is lost, to High where all information within a resource is divulged or confidential information such as passwords or encryption keys can be divulged.

Integrity
This measures the level of impact to the integrity of data within the impacted resource if the vulnerability is exploited. The score ranges from None, where the exploit does not allow an attacker to modify any information, to High, where if exploited, the vulnerability would allow an attacker to modify any or all files, or the files that could be modified have serious consequences.

Availability
This measures the level of impact to the availability of the impacted resource when the vulnerability is exploited. The score ranges from None, when the vulnerability does not impact availability at all, to High, where if exploited, the attacker can completely deny availability to the resource, or cause a service to become unavailable.
Vulnerability Intelligence

This section summarizes available intelligence about the CVE from Amazon as well as industry standard security intelligence sources such as Recorded Future, and Cybersecurity and Infrastructure Security Agency (CISA).

Note

Intel from CISA, Amazon or Recorded Future will not be available for all CVEs.

You can view vulnerability intelligence details in the console or by using the [BatchGetFindingDetails](#) API. The following details are available in the console:

**ATT&CK**

This section shows the MITRE tactics, techniques, and procedures (TTPs) associated with the CVE. The associated TTPs are shown, if there are more than two applicable TTPs you can select the link to see a complete list. Selecting a tactic or technique opens information about it on the MITRE website.

**CISA**

This section covers relevant dates associated with the vulnerability. The date Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation, and the Due date CISA expects systems to be patched by. This information is sourced from CISA.

**Known malware**

This section lists known Malware kits and tools that exploit this vulnerability.

**Evidence**

This section summarizes the most critical security events involving this vulnerability. If more than 3 events have the same criticality level the top three most recent events are displayed.

**Last time reported**

This section shows the Last known public exploit date for this vulnerability.

Severity levels for Amazon Inspector findings

When Amazon Inspector generates a vulnerability finding, it automatically assigns a severity to the finding. A finding's severity reflects the principal characteristics of the finding and can therefore help you assess and prioritize your findings. A finding's severity doesn't imply or otherwise indicate the criticality or importance that an affected resource might have for your organization.

A finding's severity rating is driven by a numerical score that corresponds to one of the following severity levels: informational, low, medium, high, or critical.

The method by which Amazon Inspector determines the severity differs based on the finding type. See the following sections about to learn more about how Amazon Inspector determines the severity rating for each finding type.

Software package vulnerability severity

Amazon Inspector uses the NVD/CVSS score as the basis of severity scoring for software package vulnerabilities. The NVD/CVSS score is the vulnerability severity score published by the NVD and defined by the CVSS. The NVD/CVSS score is a composition of security metrics, such as attack complexity, exploit code maturity, and privileges required. Amazon Inspector produces a numerical score from 1 to 10 that reflects the vulnerability's severity. Amazon Inspector categorizes this as a base score because it reflects...
the severity of a vulnerability according to its intrinsic characteristics, which are constant over time. This score also assumes the reasonable worst-case impact across different deployed environments. The CVSS v3 standard maps CVSS scores to the following severity ratings.

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Informational</td>
</tr>
<tr>
<td>0.1–3.9</td>
<td>Low</td>
</tr>
<tr>
<td>4.0–6.9</td>
<td>Medium</td>
</tr>
<tr>
<td>7.0–8.9</td>
<td>High</td>
</tr>
<tr>
<td>9.0–10.0</td>
<td>Critical</td>
</tr>
</tbody>
</table>

Package vulnerability findings can also have a severity of Untriaged. This means that the vendor hasn't yet set a vulnerability score for the detected vulnerability. In this case, we recommend using the reference URLs for the finding to research that vulnerability and respond accordingly.

Package vulnerability findings include the following scores and associated scoring vectors as part of their finding details:
- EPSS score
- Inspector score
- CVSS 3.1 from Amazon CVE
- CVSS 3.1 from NVD
- CVSS 2.0 from NVD (where applicable)

Code vulnerability severity

For code vulnerability findings Amazon Inspector uses the severity levels defined by the Amazon CodeGuru detectors that generated the finding. Each detector is assigned a severity using the CVSS v3 scoring system. For an explanation of the severities CodeGuru uses see Severity definitions in the CodeGuru guide. For a list of detectors by severity, select from the supported programming languages below:
- Python detectors by severity
- Java detectors by severity

Network reachability severity

Amazon Inspector determines the severity for a network reachability vulnerability based on the service, ports, and protocols that are exposed and by the type of open path. The following table defines these severity ratings. The value in the Open path rating column represents open paths from virtual gateways, peered VPCs, and AWS Direct Connect networks. All other exposed services, ports, and protocols have an Informational severity rating.

<table>
<thead>
<tr>
<th>Service</th>
<th>TCP ports</th>
<th>UDP ports</th>
<th>Internet path rating</th>
<th>Open path rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>67, 68, 546, 547</td>
<td>67, 68, 546, 547</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>Service</td>
<td>Port(s)</td>
<td>Port(s) over TLS</td>
<td>Severity</td>
<td>Category</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------</td>
<td>------------------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>9300, 9200</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td>21</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Global catalog</td>
<td>3268</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>LDAP</td>
<td>3269</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>80</td>
<td>Low</td>
<td>Informational</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>443</td>
<td>Low</td>
<td>Informational</td>
</tr>
<tr>
<td>Kerberos</td>
<td>88, 464, 543, 544, 749, 751</td>
<td>88, 464, 749, 750, 751</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>LDAP</td>
<td>389</td>
<td>389</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>LDAP over TLS</td>
<td>636</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>MongoDB</td>
<td>27017, 27018, 27019, 28017</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>MySQL</td>
<td>3306</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>137, 139</td>
<td>137, 138</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>NFS</td>
<td>111, 2049, 4045, 1110</td>
<td>111, 2049, 4045, 1110</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521, 1630</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>5432</td>
<td>NA</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>Print services</td>
<td>515</td>
<td>NA</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>RDP</td>
<td>3389</td>
<td>3389</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>RPC</td>
<td>111, 135, 530</td>
<td>111, 135, 530</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>SMB</td>
<td>445</td>
<td>445</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>22</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>SQL Server</td>
<td>1433</td>
<td>1434</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>Syslog</td>
<td>601</td>
<td>514</td>
<td>Medium</td>
<td>Informational</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>23</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>WINS</td>
<td>1512, 42</td>
<td>1512, 42</td>
<td>Medium</td>
<td>Informational</td>
</tr>
</tbody>
</table>
Managing findings in Amazon Inspector

Amazon Inspector offers several ways to sort, group, and manage your findings. These features help you tailor findings to your environment, aggregate findings by different views, and focus on vulnerabilities to your specific AWS environment.

Findings appear in various views based on their state: active, suppressed, or closed. By default, each view shows only active findings. An active finding represents a potential security issue detected by Amazon Inspector that indicates a vulnerability or potential threat. Suppressed findings are active findings that you have excluded using suppression rules. Amazon Inspector automatically sets a finding's status to closed when it detects that the finding is remediated. You do not manually close findings.

You can also view findings in AWS Security Hub, a service that provides a comprehensive view of your security state across your AWS environment. For more information, see Amazon Inspector integration with AWS Security Hub (p. 125). Container image findings are also available in the Amazon ECR console, and you can view findings for all resources using the AWS Command Line Interface (AWS CLI) or API.

Topics
- Viewing Amazon Inspector findings (p. 21)
- Filtering Amazon Inspector findings (p. 22)
- Suppressing Amazon Inspector findings with suppression rules (p. 22)
- Exporting findings reports from Amazon Inspector (p. 24)
- Creating custom responses to Amazon Inspector findings with Amazon EventBridge (p. 32)

Viewing Amazon Inspector findings

The Amazon Inspector console displays findings in tabbed views based on related groupings. Each view includes information that can help you analyze specific vulnerabilities, identify your most vulnerable resources, and gauge the overall impact of vulnerabilities in your environment. You can navigate to a different finding view by choosing an option under the Findings navigation side panel. You can also create a filter in each view to focus on specific types of findings. For more information about using filters, see Filtering Amazon Inspector findings (p. 22).

Findings can be grouped by the following parameters:

- **By vulnerability** – Lists the most critical vulnerabilities detected in your environment. Choose a vulnerability title from this view to open a details pane with additional information.
- **By account** – Lists your accounts, Amazon Inspector scan coverage percent for each account, and the total number of Critical and High severity findings for each account. This grouping is only available to delegated administrators.
- **By instance** – Lists the most vulnerable Amazon EC2 instances in your environment.
- **By container image** – Lists the most vulnerable Amazon ECR container images in your environment.
- **By container repository** – Shows the repositories with the most vulnerabilities.
- **By Lambda function** – Shows the Lambda functions with the most vulnerabilities.
Filtering findings

- **All findings** – Shows a complete list of findings for your environment. This is the default view when you navigate to the **Findings** page. In this view you can filter by active, suppressed, and closed findings.

You can create suppression rules based on filters to exclude findings from the findings views. For more information, see *Suppressing Amazon Inspector findings with suppression rules* (p. 22).

**Filtering Amazon Inspector findings**

A finding filter allows you to view only the findings that match the criteria you specify. Findings that do not match the filter criteria are excluded from your view. You can create finding filters using the Amazon Inspector console. To use these filters to automatically suppress existing and future findings, see *Suppressing Amazon Inspector findings with suppression rules* (p. 22).

**Creating filters in the Amazon Inspector console**

In each findings view, you can use the filter functionality to locate findings with specific characteristics. Filters are removed when you move to a different tabbed view.

A filter is made up of a filter criteria, which consists of a filter attribute paired with a filter value. Findings that do not match your filter criteria are excluded from the findings list. For example, to see all findings that are associated with your administrator account, you can choose the AWS account ID attribute and pair it with the value of your twelve digit AWS account ID.

Some filter criteria apply to all findings, while others are available for specific resource types or finding types only.

**To apply a filter to the findings view**

2. In the navigation pane, choose **Findings**. The default view displays all findings with an **Active** status.
3. To filter findings by criteria, select the **Add filter** bar to see a list of all applicable filter criteria for that view. Different filter criteria are available in different views.
4. Choose a criterion that you want to filter by from the list.
5. From the criterion input pane enter the desired filter values to define that criterion.
6. Choose **Apply** to apply that filter criterion to your current results. You can continue to add other filter criteria by selecting the filter input bar again.
7. (Optional) To view your suppressed or closed findings, choose **Active** in the filter bar, and then choose **Suppressed** or **Closed**. Choose **Show all** to see active, suppressed, and closed findings in the same view.

**Suppressing Amazon Inspector findings with suppression rules**

You can use suppression rules to automatically exclude Amazon Inspector findings that match specified criteria. For example, you can create a rule to suppress all findings with a low vulnerability score. This helps focus your view on only the findings that are the most critical to you. Suppression rules don’t have any impact on the finding itself and don’t prevent Amazon Inspector from generating a finding. Suppression rules are only used to filter your list of findings.
If Amazon Inspector generates a new finding that matches a suppression rule, the service automatically sets the status of the finding to **Suppressed**. The findings that match suppression rule criteria don’t appear by default.

Amazon Inspector stores suppressed findings until they are remediated. Amazon Inspector detects remediated findings and closes them automatically. Closed findings are stored for 30 days and then deleted if there is no further activity on the finding.

Suppressed findings are published as events to AWS Security Hub and Amazon EventBridge. Automatically suppress unwanted findings in Security Hub by changing the status of the findings in Security Hub using an EventBridge rule, for more information see [How to create auto-suppression rules in AWS Security Hub](#). Suppression rules don't close or remediate a finding. They only affect whether the finding appears in the list by default. You can view suppressed findings at any time in the Amazon Inspector console. Amazon Inspector automatically changes the status of suppressed findings to closed if it detects that the issue was remediated.

**Note**
Member accounts in an organization cannot create or manage suppression rules.

## Creating a suppression rule

You can create suppression rules to filter the list of findings that are shown by default. You can create a suppression rule programmatically by using the [CreateFilter API](#) and specifying SUPRESS as the value for **action**.

### To create a suppression rule (console)
2. In the navigation pane, choose **Suppression rules**. Then choose **Create rule**.
3. For each criterion, do the following:
   - Select the filter bar to see a list of filter criteria that you can add to your suppression rule.
   - Select the filter criteria for your suppression rule.
4. When you have finished adding criteria, enter a name for the rule and an optional description.
5. Choose **Save rule**. Amazon Inspector immediately applies the new suppression rule and hides any findings that match the criteria.

## Viewing suppressed findings

By default, Amazon Inspector does not display suppressed findings in the Amazon Inspector console. However, you can view the findings suppressed by a particular rule.

### To view suppressed findings
2. In the navigation pane, select **Suppression rules**.
3. In the suppression rules list, select the title of the rule.

## Changing suppression rules

You can make changes to suppression rules at any time.
To modify suppression rules

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. In the navigation pane, select Suppression rules.
3. Select the title of the suppression rule that you want to modify.
4. Make the intended changes, then choose Save to update the rule.

Deleting suppression rules

You can delete suppression rules. If you delete a suppression rule, Amazon Inspector stops suppressing new and existing occurrences of findings that meet the rule criteria and that aren't suppressed by other rules.

After you delete a suppression rule, new and existing occurrences of findings that met the rule's criteria have a status of Active. This means that they appear by default on the Amazon Inspector console. In addition, Amazon Inspector publishes these findings to AWS Security Hub and Amazon EventBridge as events.

To delete a suppression rule

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. In the navigation pane, select Suppression rules.
3. Select the check box next to the title of the suppression rule you want to delete.
4. Choose Delete, and then confirm your choice to permanently delete the rule.

Exporting findings reports from Amazon Inspector

In addition to sending findings to Amazon EventBridge and AWS Security Hub, you can optionally export findings to an Amazon Simple Storage Service (Amazon S3) bucket as a findings report. A findings report is a CSV or JSON file that contains the details of findings that you choose to include in the report. It provides a detailed snapshot of your findings at a specific point in time. For each finding, the file includes details such as the Amazon Resource Name (ARN) of the affected resource, the date and time when the finding was created, the associated Common Vulnerabilities and Exposures (CVE) ID, and the finding's severity, status, and Amazon Inspector and CVSS scores.

When you configure a findings report, you start by specifying which findings to include in the report. By default, Amazon Inspector includes data for all of your findings in the current AWS Region that have a status of Active. If you're the delegated Amazon Inspector administrator for an organization, this includes findings data for all the member accounts in your organization.

You can optionally customize a report by filtering the data. With filters, you can include or exclude data for findings that have specific characteristics—for example, all Critical findings that were created during a specific time range, all Active findings for a particular resource, or all Critical findings of a specific type. If you're the Amazon Inspector administrator for an organization, you might use filters to create a report that includes findings for a specific AWS account in your organization—for example, all an account's Critical findings that have a status of Active and for which a fix is available. You might then share the report with the account owner for remediation.

Note

When you export a findings report using the CreateFindingsReport API you will only see Active findings by default. To see Suppressed or Closed findings you must specify SUPPRESSED or CLOSED as values for the findingStatus filter criteria.
When you export a findings report, Amazon Inspector encrypts the data with an AWS Key Management Service (AWS KMS) key that you specify, and adds the report to an S3 bucket that you also specify. The encryption key must be a customer managed, AWS Key Management Service (AWS KMS) symmetric encryption key that's in the current AWS Region. In addition, the key policy must allow Amazon Inspector to use the key. The S3 bucket must also be in the current Region, and the bucket’s policy must allow Amazon Inspector to add objects to the bucket.

After Amazon Inspector finishes encrypting and storing your report, you can download the report from the S3 bucket that you specified or move it to another location. Alternatively, you might keep the report in the same S3 bucket and use that bucket as a repository for findings reports that you subsequently export.

This topic guides you through the process of using the AWS Management Console to export a findings report. The process consists of verifying that you have the permissions that you need, configuring the resources that you need, and then configuring and exporting the report.

Note
You can export only one findings report a time. If an export is currently in progress, wait until that export is complete before you try to export another report.

Tasks
• Step 1: Verify your permissions (p. 25)
• Step 2: Configure an S3 bucket (p. 26)
• Step 3: Configure an AWS KMS key (p. 28)
• Step 4: Configure and export a findings report (p. 30)
• Troubleshoot export errors (p. 32)

After you export a findings report for the first time, steps 1–3 can be optional. This depends primarily on whether you want to use the same S3 bucket and AWS KMS key for subsequent reports.

If you prefer to export a report programmatically after steps 1–3, use the CreateFindingsReport operation of the Amazon Inspector API.

Step 1: Verify your permissions

Before you export a findings report from Amazon Inspector, verify that you have the permissions that you need to both export findings reports and configure resources for encrypting and storing the reports. To verify your permissions, use AWS Identity and Access Management (IAM) to review the IAM policies that are attached to your IAM identity. Then compare the information in those policies to the following list of actions that you must be allowed to perform to export a findings report.

Amazon Inspector

For Amazon Inspector, verify that you're allowed to perform the following actions:
• inspector2:ListFindings
• inspector2:CreateFindingsReport

These actions allow you to retrieve findings data for your account and to export that data in findings reports.

If you plan to export large reports programmatically, you might also verify that you're allowed to perform the following actions: inspector2:GetFindingsReportStatus, to check the status of reports, and inspector2:CancelFindingsReport, to cancel exports that are in progress.

AWS KMS

For AWS KMS, verify that you're allowed to perform the following actions:
Step 2: Configure an S3 bucket

For Amazon S3, verify that you're allowed to perform the following actions:

- s3:CreateBucket
- s3:DeleteObject
- s3:PutBucketAcl
- s3:PutBucketPolicy
- s3:PutBucketPublicAccessBlock
- s3:PutObject
- s3:PutObjectAcl

These actions allow you to create and configure the S3 bucket where you want Amazon Inspector to store your report. They also allow you to add and delete objects from the bucket.

If you plan to use the Amazon Inspector console to export your report, also verify that you're allowed to perform the s3:ListAllMyBuckets and s3:GetBucketLocation actions. These actions allow you to retrieve and display information about the S3 buckets for your account. You can then choose one of these buckets to store the report.

If you're not allowed to perform one or more of the required actions, ask your AWS administrator for assistance before you proceed to the next step.

Step 2: Configure an S3 bucket

After you verify your permissions, you're ready to configure the S3 bucket where you want to store your findings report. It can be an existing bucket for your own account, or an existing bucket that's owned by another AWS account and you're allowed to access. If you want to store your report in a new bucket, create the bucket before you proceed.

The S3 bucket must be in the same AWS Region as the findings data that you want to export. For example, if you're using Amazon Inspector in the US East (N. Virginia) Region and you want to export findings data for that Region, the bucket must also be in the US East (N. Virginia) Region.

In addition, the bucket's policy must allow Amazon Inspector to add objects to the bucket. This topic explains how to update the bucket policy and it provides an example of the statement to add to the
For detailed information about adding and updating bucket policies, see Using bucket policies in the Amazon Simple Storage Service User Guide.

If you want to store your report in an S3 bucket that’s owned by another account, work with the bucket’s owner to update the bucket’s policy. Also obtain the URI for the bucket. You’ll need to enter this URI when you export your report.

To update the bucket policy

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. In the navigation pane, choose Buckets.
3. Choose the S3 bucket where you want to store the findings report.
4. Choose the Permissions tab.
5. In the Bucket policy section, choose Edit.
6. Copy the following example statement to your clipboard:

```json
{
  "Version": "2012-10-17",
  "Statement": [ 
    {
      "Sid": "allow-inspector",
      "Effect": "Allow",
      "Principal": {
        "Service": "inspector2.amazonaws.com"
      },
      "Action": [ "s3:PutObject", "s3:PutObjectAcl", "s3:AbortMultipartUpload" ],
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
        }
      }
    }]
}
```

7. In the Bucket policy editor on the Amazon S3 console, paste the preceding statement into the policy to add it to the policy.

When you add the statement, ensure that the syntax is valid. Bucket policies use JSON format. This means that you need to add a comma before or after the statement, depending on where you add the statement to the policy. If you add the statement as the last statement, add a comma after the closing brace for the preceding statement. If you add it as the first statement or between two existing statements, add a comma after the closing brace for the statement.

8. Update the statement with the correct values for your environment, where:

   - **DOC-EXAMPLE-BUCKET** is the name of the bucket.
   - **111122223333** is the account ID for your AWS account.
   - **Region** is the AWS Region in which you’re using Amazon Inspector and want to allow Amazon Inspector to add reports to the bucket. For example, us-east-1 for the US East (N. Virginia) Region.
Note
If you're using Amazon Inspector in a manually enabled AWS Region, also add the appropriate Region code to the value for the Service field. This field specifies the Amazon Inspector service principal.
For example, if you're using Amazon Inspector in the Middle East (Bahrain) Region, which has the Region code me-south-1, replace inspector2.amazonaws.com with inspector2.me-south-1.amazonaws.com in the statement.

Note that the example statement defines conditions that use two IAM global condition keys:

- **aws:SourceAccount** – This condition allows Amazon Inspector to add reports to the bucket only for your account. It prevents Amazon Inspector from adding reports to the bucket for other accounts. More specifically, the condition specifies which account can use the bucket for the resources and actions specified by the aws:SourceArn condition.

  To store reports for additional accounts in the bucket, add the account ID for each additional account to this condition. For example:

  ```json
  "aws:SourceAccount": [111122223333, 444455556666, 123456789012]
  ```

- **aws:SourceArn** – This condition restricts access to the bucket based on the source of the objects that are being added to the bucket. It prevents other AWS services from adding objects to the bucket. It also prevents Amazon Inspector from adding objects to the bucket while performing other actions for your account. More specifically, the condition allows Amazon Inspector to add objects to the bucket only if the objects are findings reports, and only if those reports are created by the account and in the Region specified in the condition.

  To allow Amazon Inspector to perform the specified actions for additional accounts, add Amazon Resource Names (ARNs) for each additional account to this condition. For example:

  ```json
  "aws:SourceArn": [
    "arn:aws:inspector2:Region:444455556666:report/**",
    "arn:aws:inspector2:Region:123456789012:report/**"
  ]
  ```

  The accounts specified by the aws:SourceAccount and aws:SourceArn conditions should match.

  Both conditions help prevent Amazon Inspector from being used as a confused deputy during transactions with Amazon S3. Although we don't recommend it, you can remove these conditions from the bucket policy.

9. When you finish updating the bucket policy, choose **Save changes**.

### Step 3: Configure an AWS KMS key

After you verify your permissions and configure the S3 bucket, determine which AWS KMS key you want Amazon Inspector to use to encrypt your findings report. The key must be a customer managed, symmetric encryption KMS key. In addition, the key must be in the same AWS Region as the S3 bucket that you configured to store the report.

The key can be an existing KMS key from your own account, or an existing KMS key that another account owns. If you want to use a new KMS key, create the key before proceeding. If you want to use an existing key that another account owns, obtain the Amazon Resource Name (ARN) of the key. You'll need to
enter this ARN when you export your report from Amazon Inspector. For information about creating and reviewing the settings for KMS keys, see Managing keys in the AWS Key Management Service Developer Guide.

After you determine which KMS key you want to use, give Amazon Inspector permission to use the key. Otherwise, Amazon Inspector won't be able to encrypt and export the report. To give Amazon Inspector permission to use the key, update the key policy for the key. For detailed information about key policies and managing access to KMS keys, see Key policies in AWS KMS in the AWS Key Management Service Developer Guide.

To update the key policy

Note
The following procedure is for updating an existing key to allow Amazon Inspector to use it. If you do not already have an existing key see https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html for guidance on creating one.

2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. In the navigation pane, choose Customer managed keys.
4. Choose the KMS key that you want to use to encrypt the report. The key must be a symmetric encryption (SYMMETRIC_DEFAULT) key.
5. On the Key policy tab, choose Edit. If you do not see a key policy with an Edit button, you must first select Switch to policy view.
6. Copy the following example statement to your clipboard:

```json
{
   "Sid": "Allow Amazon Inspector to use the key",
   "Effect": "Allow",
   "Principal": {
      "Service": "inspector2.amazonaws.com"
   },
   "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey*
   ],
   "Resource": "*",
   "Condition": {
      "StringEquals": {
         "aws:SourceAccount": "111122223333"
      },
      "ArnLike": {
      }
   }
}
```

7. In the Key policy editor on the AWS KMS console, paste the preceding statement into the key policy to add it to the policy.

When you add the statement, ensure that the syntax is valid. Key policies use JSON format. This means that you need to add a comma before or after the statement, depending on where you add the statement to the policy. If you add the statement as the last statement, add a comma after the closing brace for the preceding statement. If you add it as the first statement or between two existing statements, add a comma after the closing brace for the statement.

8. Update the statement with the correct values for your environment, where:

   • 111122223333 is the account ID for your AWS account.
• **Region** is the AWS Region in which you want to allow Amazon Inspector to encrypt reports with the key. For example, us-east-1 for the US East (N. Virginia) Region.

**Note**
If you're using Amazon Inspector in a manually enabled AWS Region, also add the appropriate Region code to the value for the Service field. For example, if you're using Amazon Inspector in the Middle East (Bahrain) Region, replace inspector2.amazonaws.com with inspector2.me-south-1.amazonaws.com.

Like the example statement for the bucket policy in the preceding step, the Condition fields in this example use two IAM global condition keys:

• **aws:SourceAccount** – This condition allows Amazon Inspector to perform the specified actions only for your account. More specifically, it determines which account can perform the specified actions for the resources and actions specified by the aws:SourceArn condition.

To allow Amazon Inspector to perform the specified actions for additional accounts, add the account ID for each additional account to this condition. For example:

```json
"aws:SourceAccount": [111122223333,444455556666,123456789012]
```

• **aws:SourceArn** – This condition prevents other AWS services from performing the specified actions. It also prevents Amazon Inspector from using the key while performing other actions for your account. In other words, it allows Amazon Inspector to encrypt S3 objects with the key only if the objects are findings reports, and only if those reports are created by the account and in the Region specified in the condition.

To allow Amazon Inspector to perform the specified actions for additional accounts, add ARNs for each additional account to this condition. For example:

```json
"aws:SourceArn": [
  "arn:aws:inspector2:us-east-1:444455556666:report/*",
  "arn:aws:inspector2:us-east-1:123456789012:report/*"
]
```

The accounts specified by the aws:SourceAccount and aws:SourceArn conditions should match.

These conditions help prevent Amazon Inspector from being used as a confused deputy during transactions with AWS KMS. Although we don't recommend it, you can remove these conditions from the statement.

9. When you finish updating the key policy, choose **Save changes**.

### Step 4: Configure and export a findings report

After you verify your permissions and you configure resources to encrypt and store your findings report, you're ready to configure and export the report.

#### To configure and export a findings report

2. In the navigation pane, under **Findings**, choose **All findings**.
3. (Optional) By using the filter bar above the **Findings** table, add filter criteria (p. 22) that specify which findings to include in the report. As you add criteria, Amazon Inspector updates the table to include only those findings that match the criteria. The table provides a preview of the data that your report will contain.

   **Note**
   We recommend that you add filter criteria. If you don't, the report will include data for all of your findings in the current AWS Region that have a status of **Active**. If you're the Amazon Inspector administrator for an organization, this includes findings data for all the member accounts in your organization. If a report includes data for all or many findings, it can take a long time to generate and export the report, and you can export only one report at a time.

4. Choose **Export findings**.

5. In the **Export settings** section, for **Export file type**, specify a file format for the report:
   - To create a JavaScript Object Notation (.json) file that contains the data, choose **JSON**.
     - If you choose the **JSON** option, the report will include all the fields for each finding. For a list of possible JSON fields see the **Finding** data type in the Amazon Inspector API reference.
   - To create a comma-separated values (.csv) file that contains the data, choose **CSV**.
     - If you choose the **CSV** option, the report will include only a subset of the fields for each finding, approximately 45 fields that report key attributes of a finding. The fields include: **Finding Type**, **Title**, **Severity**, **Status**, **Description**, **First Seen**, **Last Seen**, **Fix Available**, **AWS account ID**, **Resource ID**, **Resource Tags**, and **Remediation**. These are in addition to fields that capture scoring details and reference URLs for each finding. The following is a sample of the CSV headers in a findings report:

   | Id | Account | AWS | KMS key | Finding | Tag | Version | Vector | NVD | CVSS3 | Vendor | Advisory | CVSS2 | Vector | Age | Exploited | Last | Exploit | First | Fix | Available | Remediation | Resources | Platforms | Packages | Installed | Affected | Version | File | Paths | Network | Image | Container | Layers | Lambda | Urls | Vpc | Ami | Resource | Id | Remediation | Network | Region | Lambda | At | At | Type | Updated |
|----|---------|-----|---------|---------|-------|--------|--------|------|-------|--------|---------|-------|-------|-----|----------|------|---------|--------|------|----------|-----------|----------|----------|---------|----------|--------|-------|------|-------|--------|-------|-------|--------|-------|--------|-----|-----|------|-------|-------|-------|--------|-------|

6. Under **Export location**, for **S3 URI**, specify the S3 bucket where you want to store the report:

   - To store the report in a bucket that your account owns, choose **Browse S3**. Amazon Inspector displays a table of the S3 buckets for your account. Select the row for the bucket that you want, and then choose **Choose**.
     - **Tip**
     To also specify an Amazon S3 path prefix for the report, append a slash (/) and the prefix to the value in the **S3 URI** box. Amazon Inspector then includes the prefix when it adds the report to the bucket, and Amazon S3 generates the path specified by the prefix.
     - For example, if you want to use your AWS account ID as a prefix and your account ID is 111122223333, append /111122223333 to the value in the **S3 URI** box. A prefix is similar to a directory path within an S3 bucket. It allows you to group similar objects together in a bucket, much like you might store similar files together in a folder on a file system. For more information, see **Organizing objects in the Amazon S3 console using folders** in the Amazon Simple Storage Service User Guide.
   - To store the report in a bucket that another account owns, enter the URI for the bucket—for example, **s3://DOC-EXAMPLE_BUCKET**, where **DOC-EXAMPLE_BUCKET** is the name of the bucket. The bucket owner can find this information for you in the bucket's properties.

7. For **KMS key**, specify the AWS KMS key that you want to use to encrypt the report:

   - To use a key from your own account, choose the key from the list. The list displays customer managed, symmetric encryption KMS keys for your account.
• To use a key that another account owns, enter the Amazon Resource Name (ARN) of the key. The key owner can find this information for you in the key’s properties. For more information, see Finding the key ID and key ARN in the AWS Key Management Service Developer Guide.

8. Choose Export.

Amazon Inspector generates the findings report, encrypts it with the KMS key that you specified, and adds it to the S3 bucket that you specified. Depending on the number of findings that you chose to include in the report, this process can take several minutes or hours. When the export is complete, Amazon Inspector displays a message indicating that your findings report was exported successfully. Optionally choose View report in the message to navigate to the report in Amazon S3.

Note that you can export only one report a time. If an export is currently in progress, wait until that export is complete before you try to export another report.

Troubleshoot export errors

If an error occurs when you try to export a findings report, Amazon Inspector displays a message describing the error. You can use the information in this topic as a guide to identify possible causes and solutions for the error.

For example, verify that the S3 bucket is in the current AWS Region and the bucket’s policy allows Amazon Inspector to add objects to the bucket. Also verify that the AWS KMS key is enabled in the current Region, and ensure that the key policy allows Amazon Inspector to use the key.

After you address the error, try to export the report again.

Cannot have multiple reports error

If you are attempting to create a report but Amazon Inspector is already generating a report, you will receive an error stating Reason: Cannot have multiple reports in-progress. This error occurs because Amazon Inspector can only generate one report for an account at a time.

To resolve the error you can wait for the other report to finish or cancel it before requesting a new report.

You can check the status of a report by using the GetFindingsReportStatus operation, this operation returns the report ID of any report that is currently being generated.

If you need to, you can use the report ID given by the GetFindingsReportStatus operation to cancel a export that is currently in progress by using the CancelFindingsReport operation.

Creating custom responses to Amazon Inspector findings with Amazon EventBridge

Amazon Inspector creates an event for Amazon EventBridge for newly generated findings, newly aggregated findings, and changes in the state of findings. Anything other than a change to the updatedAt and lastObservedAt fields will publish a new event. This means new events for a finding are generated when you take actions such as restarting a resource or changing the tags associated with a resource. However, the finding ID in the id field remains the same. Events are emitted on a best-effort basis.

Note
If your account is an Amazon Inspector delegated administrator, EventBridge publishes events to your account in addition to the member account from which they originated.
When you use EventBridge events with Amazon Inspector, you can automate tasks to help you respond to security issues revealed by Amazon Inspector findings.

Amazon Inspector emits events to the default event bus in the same Region. This means that you must configure event rules for each Region in which you are running Amazon Inspector to see events for that Region.

To receive notifications about Amazon Inspector findings based on EventBridge events, you must create an EventBridge rule and a target for Amazon Inspector. This rule allows EventBridge to send notifications for findings that Amazon Inspector generates to the target specified in the rule. For more information, see [Amazon EventBridge rules](https://docs.aws.amazon.com/AmazonEventBridge/latest,userGuide) in the *Amazon EventBridge User Guide*.

### Event schema

The following is an example of the Amazon Inspector event format for an EC2 finding event. For example schema of other finding types and event types, see *EventBridge schema* (p. 45).

```json
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "It was discovered that the sound subsystem in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:00:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "source": "NVD",
                "version": "3.1"
            }],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM"
        }
    }
}
```
Creating an EventBridge rule to notify you of Amazon Inspector findings

To increase the visibility of Amazon Inspector findings, you can use EventBridge to set up automated finding alerts that are sent to a messaging hub. This topic shows you how to send alerts for CRITICAL and HIGH severity findings to email, Slack, or Amazon Chime. You’ll learn how to set up an Amazon Simple Notification Service topic and then connect that topic to an EventBridge event rule.

**Step 1. Set up an Amazon SNS topic and endpoint**

To set up automatic alerts, you must first set up a topic in Amazon Simple Notification Service and add an endpoint. For more information, refer to the SNS guide.

This procedure establishes where you want to send Amazon Inspector findings data. The SNS topic can be added to an EventBridge event rule during or after the creation of the event rule.
Email setup

Creating an SNS topic

2. From the navigation pane, select Topics, and then select Create Topic.
3. In the Create topic section, select Standard. Next, enter a topic name, such as Inspector_to_Email. Other details are optional.
4. Choose Create Topic. This opens a new panel with details for your new topic.
5. In the Subscriptions section, select Create Subscription.
6. a. From the Protocol menu, select Email.
   b. In the Endpoint field, enter the email address that you would like to receive notifications.
      
      **Note**
      
      You will be required to confirm your subscription through your email client after creating the subscription.
   c. Choose Create subscription.
7. Look for a subscription message in your inbox and choose Confirm Subscription.

Slack setup

Creating an SNS topic

2. From the navigation pane, select Topics, and then select Create Topic.
3. In the Create topic section, select Standard. Next, enter a topic name, such as Inspector_to_Slack. Other details are optional. Choose Create topic to complete endpoint creation.
4. Select Configure new channel to open the configuration details pane.
   a. Enter a name for the channel.
   b. For Slack channel, choose the channel that you want to use.
   c. In Slack, copy the channel ID of the private channel by right-clicking on the channel name and selecting Copy Link.
   d. On the AWS Management Console, in the AWS Chatbot window, paste the channel ID that you copied from Slack into the Private channel ID field.
   e. In Permissions, choose to create an IAM role using a template if you do not already have a role.
   f. For Policy templates, choose Notification permissions. This is the IAM policy template for AWS Chatbot. This policy provides the necessary read and list permissions for CloudWatch alarms, events, and logs, and for Amazon SNS topics.
   g. For Channel guardrail policies, choose AmazonInspector2ReadOnlyAccess.
Amazon Inspector User Guide

Creating an EventBridge rule to notify you of Amazon Inspector findings

5. Select **Configure**.

**Amazon Chime setup**

**Creating an SNS topic**

2. Select **Topics** from the navigation pane, and then select **Create Topic**.
3. In the **Create topic** section, select **Standard**. Next, enter a topic name, such as **Inspector_to_Chime**. Other details are optional. Choose **Create topic** to complete.

**Configuring an AWS Chatbot client**

2. From the **Configured clients** panel, select **Configure new client**.
3. Choose **Chime**, and then choose **Configure** to confirm.
4. From the **Configuration details** pane, enter a name for the channel.
5. In Amazon Chime, open the desired chat room.
   a. Choose the gear icon in the upper-right corner and choose **Manage webhooks and bots**.
   b. Select **Copy URL** to copy the webhook URL to your clipboard.
6. On the AWS Management Console, in the AWS Chatbot window, paste the URL you copied into the **Webhook URL** field.
7. In **Permissions**, choose to create an IAM role using a template if you do not already have a role.
8. For **Policy templates**, choose **Notification permissions**. This is the IAM policy template for AWS Chatbot. It provides the necessary read and list permissions for CloudWatch alarms, events, and logs, and for Amazon SNS topics.
9. Choose the Region in which you previously created your SNS topic, and then select the Amazon SNS topic you created to send notifications to the Amazon Chime room.
10. Select **Configure**.

**Step 2. Create an EventBridge rule for Amazon Inspector findings**

1. Open the Amazon EventBridge console at [https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Select **Rules** from the navigation pane, and then select **Create rule**.
3. Enter a name and optional description for your rule.
4. Select **Rule with an event pattern** and then **Next**.
5. In the **Event Pattern** pane, choose **Custom patterns (JSON editor)**.
6. Paste the following JSON into the editor:

```json
{
    "source": ["aws.inspector2"],
    "detail-type": ["Inspector2 Finding"],
    "detail": {
        "severity": ["HIGH", "CRITICAL"],
        "status": "ACTIVE"
    }
}
```
Note
This pattern sends notifications for any active CRITICAL or HIGH severity finding detected by Amazon Inspector.

Select Next when you are finished entering the event pattern.

7. On the Select targets page, choose AWS service. Then, for Select target type, choose SNS topic.
8. For Topic, select the name of the SNS topic you created in step 1. Then choose Next.
9. Add optional tags if needed and choose Next.
10. Review your rule and then choose Create rule.

EventBridge for Amazon Inspector multi-account environments

If you're an Amazon Inspector delegated administrator, EventBridge rules appear on your account based on applicable findings from your member accounts. If you set up findings notifications through EventBridge in your administrator account, as detailed in the preceding section, you'll receive notifications about multiple accounts. In other words, you'll be notified of findings and events generated by your member accounts in addition to those generated by your own account.

You can use the accountId from the finding's JSON details to identify the member account from which the Amazon Inspector finding originated.
Exporting SBOMs with Amazon Inspector

You can use the Amazon Inspector console or API to generate Software Bill of Materials (SBOM) for your resources. An SBOM is a nested inventory of all the open source and third-party software components of your codebase. Amazon Inspector provides SBOMs for individual resources in your environment. SBOMs exported from Amazon Inspector can help you gain visibility into information about your software supply, such as your most commonly used packages, and associated vulnerabilities across your organization.

You can export SBOMs for all supported resources that are being actively monitored by Amazon Inspector. You can review the status of your resources by Assessing Amazon Inspector coverage of your AWS environment (p. 75).

**Note**
Amazon Inspector doesn't support exporting SBOM for Windows EC2 instances.

Amazon Inspector formats

Amazon Inspector supports exporting SBOMs in **CycloneDX 1.4** and **SPDX 2.3** compatible formats. Amazon Inspector exports SBOMs as JSON files to the Amazon S3 bucket you choose.

**Note**
SPDX format exports from Amazon Inspector are compatible with systems using **SPDX 2.3**, however they don't contain the Creative Commons Zero (CC0) field. This is because including this field would allow users to redistribute or edit the material.

**Example of CycloneDX 1.4 SBOM format from Amazon Inspector**

```json
{
    "bomFormat": "CycloneDX",
    "specVersion": "1.4",
    "version": 1,
    "metadata": {
        "timestamp": "2023-06-02T01:17:46Z",
        "component": null,
        "properties": [
            {
                "name": "imageId",
                "value": "sha256:c8ee97f70527776ef223080741f61fcd6a3a9107810ea9649f904aa4269fda6c6"
            },
            {
                "name": "architecture",
                "value": "arm64"
            },
            {
                "name": "accountId",
                "value": "111122223333"
            },
            {
                "name": "resourceType",
                "value": "AWS_ECR_CONTAINER_IMAGE"
            }
        ]
    }
}
```
Example of SPDX 2.3 SBOM format from Amazon Inspector
{ "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
"spdxVersion": "SPDX-2.3",
"creationInfo": {
"created": "2023-06-02T21:19:22Z",
"creators": [
"Organization: 409870544328",
"Tool: Amazon Inspector SBOM Generator"
]
},
"documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
"comment": "",
"packages": [
{ "name": "elfutils-libelf",
"versionInfo": "0.176-2.amzn2",
"downloadLocation": "NOASSERTION",
"sourceInfo": "/var/lib/rpm/Packages",
"filesAnalyzed": false,
"externalRefs": [{
"referenceCategory": "PACKAGE-MANAGER",
"referenceType": "purl",
"referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
}],
"SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
},
{ "name": "libcurl",
"versionInfo": "7.79.1-1.amzn2.0.1",
"downloadLocation": "NOASSERTION",
"sourceInfo": "/var/lib/rpm/Packages",
"filesAnalyzed": false,
"externalRefs": [{
"referenceCategory": "PACKAGE-MANAGER",
"referenceType": "purl",
"referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
},
{ "referenceCategory": "SECURITY",
"referenceType": "vulnerability",
"referenceLocator": "CVE-2022-32205"
}],
"SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
},
{ "name": "hunspell-en-US",
"versionInfo": "0.20121024-6.amzn2.0.1",
"downloadLocation": "NOASSERTION",
"sourceInfo": "/var/lib/rpm/Packages",
"filesAnalyzed": false,
"externalRefs": [{
"referenceCategory": "PACKAGE-MANAGER",
"referenceType": "purl",
"referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
}],
"SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6ce4a5e7e079d844fe5"
},
{ "name": "grub2-tools-minimal",
"versionInfo": "2.06-2.amzn2.0.6",
"downloadLocation": "NOASSERTION",
"sourceInfo": "/var/lib/rpm/Packages",
"filesAnalyzed": false,
Filters for SBOMs

When you export SBOMs you can include filters to create reports for specific subsets of resources. If you don't supply a filter the SBOMs for all active, supported resources are exported. And if you are a delegated administrator this includes resources for all members too. The following filters are available:

- **AccountID** — This filter can be used to export SBOMs for any resources associated with specific Account ID.
- **EC2 instance tag** — This filter can be used to export SBOMs for EC2 instances with specific tags.
- **Function name** — This filter can be used to export SBOMs for specific Lambda functions.
Configure and export SBOMs

To export SBOMs, you must first configure an Amazon S3 bucket and an AWS KMS key that Amazon Inspector is allowed to use. You can use filters to export SBOMs for specific subsets of your resources. To export SBOMs for multiple accounts in an AWS Organization, follow these steps while signed in as the Amazon Inspector delegated administrator.

Prerequisites

- Supported resources that are being actively monitored by Amazon Inspector.
- An Amazon S3 bucket configured with a policy that allows Amazon Inspector to add objects to. For information on configuring the policy see Configure export permissions (p. 25).
- A AWS KMS key configured with a policy that allows Amazon Inspector to use to encrypt your reports. For information on configuring the policy see Configure a AWS KMS key for export (p. 28).

Note

If you have previously configured an Amazon S3 bucket and a AWS KMS key for findings export (p. 24) you can use the same bucket and key for SBOM export.

To Export SBOMs (console)

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. Using the AWS Region selector in the upper-right corner of the page, select the Region with the resources you want to export SBOM for.
3. In the navigation pane, choose Export SBOMs.
4. (Optional) In the Export SBOMs page, use the Add filter menu to select a subset of resources to create reports for. If no filter is provided Amazon Inspector will export reports for all active resources. If you are a delegated administrator this will include all active resources in your organization.
5. Under Export setting select the format you want for the SBOM.
6. Enter an Amazon S3 URI or choose Browse Amazon S3 to select an Amazon S3 location to store the SBOM.
7. Enter a AWS KMS key configured for Amazon Inspector to use to encrypt your reports.

To export SBOMs (API)

- To export SBOMs for your resources programmatically, use the CreateSbomExport operation of the Amazon Inspector API.

In your request, use the reportFormat parameter to specify the SBOM output format, choose CYCLONEDX_1_4 or SPDX_2_3. The s3Destination parameter is required and you must specify an S3 bucket configured with a policy that allows Inspector to write to it. Optionally use resourceFilterCriteria parameters to limit the scope of the report to specific resources.
Amazon Inspector Vulnerability database search

You can search Amazon Inspector’s vulnerability database to check if common vulnerabilities and exposures (CVE) are covered by inspector scans. Amazon Inspector uses information from it's vulnerability database to populate basic details for finding relating to that CVE. Amazon Inspector also includes additional details for each finding, such as which versions a CVE is fixed in, and remediation instructions. For more information see, Amazon Inspector finding details (p. 14).

Note
At this time Amazon Inspector vulnerability database search only supports searching for CVE IDs, however, Amazon Inspector tracks, and produces findings for, other software vulnerabilities in the database.

Search the Vulnerability database

Amazon Inspector must be active in the current region to use Vulnerability database search.

Console

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/
2. From the side navigation bar, select Vulnerability database search.
3. Enter a single CVE ID in the search bar.
4. Select Search.

API

Run the SearchVulnerabilities API operation and provide a single CVE ID as filterCriteria in the format of: CVE-<year>-<ID>

If Amazon Inspector covers a CVE the console search will return various details about it from Amazon Inspector’s vulnerability database. The following detail categories are provided:

Details

Contains the description of the CVE, This includes platforms it can be detected on, related vulnerabilities, associated Common Weakness Enumeration (CWE), and dates the CVE was created and last updated. In this section you can also review various scoring and severity data for the SVE such as: National Vulnerability Database (NVD) severity, Common Vulnerability Scoring System (CVSS) score, and Exploit Prediction Scoring System (EPSS) score.

Vulnerability Intelligence

Contains threat intelligence data from Amazon, including associated MITRE techniques, exploit targets, and last known exploit time. Also contains intelligence data from Cybersecurity and Infrastructure Security Agency (CISA). This includes remediation actions, the date CISA added this CVE to it's catalog, and the date time CISA expects vendors to provide a fix.

References

Provides various links to relevant sources covering this CVE.
If Amazon Inspector doesn't cover the CVE ID you search for you will get a **No matches** response. If Amazon Inspector doesn't support a CVE it's because Amazon Inspector doesn't cover the OS or programming language package associated with that CVE. For a list of supported operating systems and packages, see [Operating systems and programming languages supported by Amazon Inspector (p. 129)](#).
Amazon EventBridge event schema for Amazon Inspector events

To support integration with other applications, services, and systems, such as monitoring or event management systems, Amazon Inspector automatically publishes findings to Amazon EventBridge as events. EventBridge is a serverless event bus service that delivers a stream of real-time data from applications and other AWS services to targets such as AWS Lambda functions, Amazon Simple Notification Service topics, and Amazon Kinesis Data Streams streams. To learn more about EventBridge and EventBridge events, see the Amazon EventBridge User Guide.

Amazon Inspector publishes events for findings, resource coverage changes, and initial scans of individual resources. Each event is a JSON object that conforms to the EventBridge schema for AWS events. Because the data is structured as an EventBridge event, you can more easily monitor, process, and act upon findings and supported Amazon Inspector events by using other applications, services, and tools.

Topics
- Amazon EventBridge base schema for Amazon Inspector (p. 45)
- Amazon Inspector finding event schema example (p. 45)
- Amazon Inspector initial scan complete event schema example (p. 53)
- Amazon Inspector coverage event schema example (p. 55)

Amazon EventBridge base schema for Amazon Inspector

The following is an example of the basic schema for an EventBridge event for Amazon Inspector. Event details differ based on the type of event.

```
{
  "version": "0",
  "id": "Event ID",
  "detail-type": "Inspector2 *event type*",
  "source": "aws.inspector2",
  "account": "AWS account ID (string)",
  "time": "event timestamp (string)",
  "region": "AWS Region (string)",
  "resources": [  
    "*IDs or ARNs of the resources involved in the event*"
  ],
  "detail": {
    "*Details of an Amazon Inspector event type*"
  }
}
```

Amazon Inspector finding event schema example

The following is an examples of the schema for an EventBridge event for Amazon Inspector findings. Finding events are created when Amazon Inspector identifies a software vulnerability or network issue in
one of your resources. For a guide to creating notifications in response to this type of event, see *Creating custom responses to Amazon Inspector findings with Amazon EventBridge (p. 32).*

The following fields identify a finding event:

- The detail-type field is set to `Inspector2 Finding`.
- The detail object describes the finding.

Select from the options to see finding event schemas for different resources and finding types.

Amazon EC2 package vulnerability finding

```json
{
  "version": "0",
  "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-01-19T22:46:15Z",
  "region": "us-east-1",
  "resources": ["i-0c2a343f1948d5205"],
  "detail": {
    "awsAccountId": "111122223333",
    "description": "It was discovered that the sound subsystem in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service (system crash).",
    "exploitAvailable": "YES",
    "exploitabilityDetails": {
      "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
    },
    "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
    "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
    "fixAvailable": "YES",
    "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
    "packageVulnerabilityDetails": {
      "cvss": [
        {
          "baseScore": 4.7,
          "source": "NVD",
          "version": "3.1"
        }
      ],
      "relatedVulnerabilities": [],
      "source": "UBUNTU_CVE",
      "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
      "vendorSeverity": "medium",
      "vulnerabilityId": "CVE-2022-3303",
      "vulnerablePackages": [{
        "arch": "X86_64",
        "epoch": 0,
```
Amazon Inspector finding event schema example

```json
{
  "fixedInVersion": "0:5.15.0.1027.31-20.04.16",
  "name": "linux-image-aws",
  "packageManager": "OS",
  "remediation": "apt update & apt install --only-upgrade linux-image-aws",
  "version": "5.15.0.1026.30-20.04.16"
}
```

```
}
```

Amazon EC2 network reachability finding

```json
{
  "version": "0",
  "id": "d038af63-1621-1b75-d014-a5e45628ef3e",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-01-20T09:17:57Z",
  "region": "us-east-1",
  "resources": ["i-0a96278c2206a8e4b"],
  "detail": {
    "awsAccountId": "111122223333",
    "description": "On the instance i-0a96278c2206a8e4b, the port range 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI eni-0976efe678170408f."
  }
}
```

22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI eni-0976efe678170408f.
Amazon Inspector finding event schema example

```json
{ "componentId": "igw-72069c09", "componentType": "AWS::EC2::InternetGateway" },
{ "componentId": "acl-91d74eec", "componentType": "AWS::EC2::NetworkAcl" },
{ "componentId": "sg-0aaed0af4500b0165", "componentType": "AWS::EC2::SecurityGroup" },
{ "componentId": "eni-0976efe67817040f", "componentType": "AWS::EC2::NetworkInterface" },
{ "componentId": "i-0a96278c2206a8e4b", "componentType": "AWS::EC2::Instance" }
],

"openPortRange": { "begin": 22, "end": 22 },

"protocol": "TCP",

"remediation": { "recommendation": { "text": "You can restrict access to your instance by modifying the Security Groups or ACLs in the network path." }

"resources": [
{ "details": {
"awsEc2Instance": {
"iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-profile/AmazonSSMRoleForInstancesQuickSetup",
"imageId": "ami-b5ee17698237e91",
"ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
"ipV6Addresses": [],
"keyName": "example-inspector-test",
"launchedAt": "Jan 19, 2023, 7:25:02 PM",
"platform": "AMAZON_LINUX_2",
"subnetId": "subnet-8213f2a3",
"type": "t2.micro",
"vpcId": "vpc-ab6650d1"
},

"id": "i-0a96278c2206a8e4b",
"partition": "aws",
"region": "us-east-1",
"type": "AWS_EC2_INSTANCE"
}],

"severity": "MEDIUM",
"status": "ACTIVE",
"title": "Port 22 is reachable from an Internet Gateway",
"type": "NETWORK_REACHABILITY",
"updatedAt": "Jan 20, 2023, 9:17:57 AM"
}
```

Amazon ECR package vulnerability finding

```json
{ "version": "0",
"id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
"detail-type": "Inspector2 Finding",
```
"source": "aws.inspector2",
"account": "111122223333",
"time": "2023-01-19T21:59:00Z",
"region": "us-east-1",
"resources": [
    "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/sha256:98f0304b3a3b7c12ce641177a99d1f5be56f532473a528fda38d53d519cafb13"
]
"detail": {
    "awsAccountId": "111122223333",
    "description": "libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, several TLS and SSH settings were left out from the configuration match checks, making them match too easily.",
    "exploitAvailable": "NO",
    "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
    "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
    "fixAvailable": "YES",
    "inspectorScore": 7.5,
    "inspectorScoreDetails": {
        "adjustedCvss": {
            "adjustments": [],
            "cvssSource": "NVD",
            "score": 7.5,
            "scoreSource": "NVD",
            "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
            "version": "3.1"
        }
    },
    "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
    "packageVulnerabilityDetails": {
        "cvss": [
            {
                "baseScore": 5,
                "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                "source": "NVD",
                "version": "2.0"
            },
            {
                "baseScore": 7.5,
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "source": "NVD",
                "version": "3.1"
            }
        ]
    },
    "relatedVulnerabilities": [],
    "source": "NVD",
    "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
    "vendorSeverity": "HIGH",
    "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
    "vulnerabilityId": "CVE-2022-27782",
    "vulnerablePackages": [
        {
            "arch": "X86_64",
            "epoch": 0,
            "fixedInVersion": "0:7.61.1-22.el8_6.3",
            "name": "libcurl",
            "packageName": "OS"
        }
    ]
}
Lambda package vulnerability finding

```json
{
  "version": "0",
  "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  
  "remediation": {
    "recommendation": {
      "text": "None Provided"
    }
  },
  "resources": [
    {
      "details": {
        "awsEcrContainerImage": {
          "architecture": "amd64",
          "imageHash": "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f552473a528fda38d53d519cafb13",
          "imageTags": [
            "o3"
          ],
          "platform": "ORACLE_LINUX_8",
          "pushedAt": "Jan 19, 2023, 7:38:39 PM",
          "registry": "111122223333",
          "repositoryName": "inspector2"
        }
      }
    },
    {
      "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/sha256:98f0304b3a3b7c12ce641177a99d1f3be56f552473a528fda38d53d519cafb13",
      "partition": "aws",
      "region": "us-east-1",
      "type": "AWS_ECR_CONTAINER_IMAGE"
    }
  ],
  "severity": "HIGH",
  "status": "ACTIVE",
  "title": "CVE-2022-27782 - libcurl, curl",
  "type": "PACKAGE_VULNERABILITY",
  "updatedAt": "Jan 19, 2023, 9:59:00 PM"
}
```
"account": "111122223333",
"time": "2023-01-19T19:20:25Z",
"region": "us-east-1",
"resources": [
],
"detail": {
  "awsAccountId": "111122223333",
  "description": "Those using Woodstox to parse XML data may be vulnerable to
Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running on
user supplied input, an attacker may supply content that causes the parser to crash by
stackoverflow. This effect may support a denial of service attack.",
  "exploitAvailable": "NO",
  "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
  "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
  "fixAvailable": "YES",
  "inspectorScore": 7.5,
  "inspectorScoreDetails": {
    "adjustedCvss": {
      "cvssSource": "NVD",
      "score": 7.5,
      "scoreSource": "NVD",
      "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
      "version": "3.1"
    }
  },
  "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
  "packageVulnerabilityDetails": {
    "cvss": [
      {
        "baseScore": 7.5,
        "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
        "source": "NVD",
        "version": "3.1"
      }
    ],
  ],
  "relatedVulnerabilities": [],
  "source": "NVD",
  "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
  "vendorSeverity": "HIGH",
  "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
  "vulnerabilityId": "CVE-2022-40152",
  "vulnerablePackages": [
    {
      "epoch": 0,
      "filePath": "lib/woodstox-core-6.2.7.jar",
      "fixedInVersion": "6.4.0",
      "name": "com.fasterxml.woodstox:woodstox-core",
      "packageManager": "JAR",
      "remediation": "Update woodstox-core to 6.4.0",
      "version": "6.2.7"
    }
  ],
  "remediation": {
    "recommendation": {
      "text": "None Provided"
    }
  },
  "resources": [
    {
      "details": 
    }
  ]}
Lambda code vulnerability finding

```json
{
   "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
   "awsAccountId": "111122223333",
   "type": "CODE_VULNERABILITY",
   "description": "Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior or failure of the Lambda function."
}
```

Lambda code vulnerability finding

```json
{
   "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
   "awsAccountId": "111122223333",
   "type": "CODE_VULNERABILITY",
   "description": "Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior or failure of the Lambda function."
}
```
Note
The detail value returns the JSON details of a single finding as an object. It does not return the entire findings response syntax, which supports multiple findings within an array.

Amazon Inspector initial scan complete event schema example

The following is an example of the EventBridge event schema for an Amazon Inspector event for completing an initial scan. This event is created when Amazon Inspector completes an initial scan of one of your resources.

The following fields identify an initial scan complete event:
• The detail-type field is set to Inspector2 Scan.
• The detail object contains a finding-severity-counts object that details the number of findings in the applicable severity categories, such as CRITICAL, HIGH, and MEDIUM.

Select from the options to see different initial scan event schemas by resource type.

Amazon EC2 instance initial scan

```json
{
  "version": "0",
  "id": "28a46762-6ac8-6cc4-4f55-bc09ab99af928",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-01-20T22:52:35Z",
  "region": "us-east-1",
  "resources": [
    "i-087d63509b8c97098"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "instance-id": "i-087d63509b8c97098",
    "version": "1.0"
  }
}
```

Amazon ECR image initial scan

```json
{
  "version": "0",
  "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-01-20T22:52:35Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "image-digest": "sha256:965fbcaee99b0a467ed5657caceae165018ef44a4d2d46c7cdea80a9dfe0d1ea",
    "image-tags": [
      "ubuntu22"
    ]
  }
}
```
Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
  }
}
```

Amazon Inspector coverage event schema example

The following is an example of the EventBridge event schema for an Amazon Inspector event for coverage. This event is created when Amazon Inspector scan coverage for a resource is changed. The following fields identify a coverage event:

- The detail-type field is set to Inspector2 Coverage.
- The detail object contains a scanStatus object that indicates the new scanning status for the resource.

```
{
  "version": "0",
  "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
  "detail-type": "Inspector2 Coverage",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-01-20T22:51:39Z",
  "region": "us-east-1",
  "resources": [
    "i-087d63509b8c97098"
  ],
  "detail": {
    "scan-status": {
      "reason": "UNMANAGED_EC2_INSTANCE",
      "version": "1.0"
    }
  }
}
```
"statusCodeValue": "INACTIVE",
"scanType": "PACKAGE",
"eventTimestamp": "2023-01-20T22:51:35.665501Z",
"version": "1.0"}
Scanning resources with Amazon Inspector

Amazon Inspector uses its own, purpose-built scanning engine. This engine monitors your resources for software vulnerabilities or open network paths that can result in compromised workloads, malicious use of resources, or unauthorized access to your data. When Amazon Inspector detects a vulnerability, it creates a finding. Findings include details associated with the detection to help you remediate the vulnerability. You can review findings on the Amazon Inspector console and by using the Amazon Inspector API. For more information, see Managing findings in Amazon Inspector (p. 21).

When activated, Amazon Inspector automatically discovers all eligible resources and begins continuous scans of those resources. Amazon Inspector scans for software vulnerabilities and unintended network exposure. Amazon Inspector also runs scans in response to events, such as the installation of a new application or patch.

When you activate Amazon Inspector for the first time, your account is automatically enrolled in all scan types. The following topics cover specific details about the scan types Amazon Inspector provides. Amazon Inspector categorizes scan types based on the resource type impacted by a vulnerability. The following topics cover which resources Amazon Inspector scans, what initiates new scans for those resources, and how to configure scans for each resource type.

Topics
- Overview of Amazon Inspector scan types (p. 57)
- Activating a scan type (p. 58)
- Scanning Amazon EC2 instances with Amazon Inspector (p. 59)
- Scanning Amazon ECR container images with Amazon Inspector (p. 67)
- Scanning AWS Lambda functions with Amazon Inspector (p. 69)
- Deactivating a scan type (p. 73)

When you activate Amazon Inspector for the first time, your account is automatically enrolled in the following scan types: Amazon EC2 scanning, Amazon ECR Scanning, Lambda standard scanning. Lambda code scanning is an optional layer of Lambda function scanning that you can activate at any time.

Overview of Amazon Inspector scan types

Amazon Inspector offers a range of different scan types focused on specific resource types in your AWS environment.

Amazon EC2 scanning

When you activate Amazon EC2 scanning Amazon Inspector scans your Amazon EC2 instances for operating system package and programming language package vulnerabilities, and network reachability. To collect Common Vulnerabilities and Exposures (CVE) data for your EC2 instance, Amazon Inspector requires your instance to have an active AWS Systems Manager (SSM) agent installed. This agent is pre-installed on many EC2 instances, but you may need to activate it.
manually. Regardless of SSM agent status, Amazon Inspector scans all your EC2 instances for network exposure issues. For more information about scans for Amazon EC2, see Scanning Amazon EC2 instances with Amazon Inspector (p. 59).

**Amazon ECR scanning**

When you activate Amazon ECR scanning, Amazon Inspector converts all container repositories in your private registry that are configured for the default Basic scanning provided by Amazon ECR to Enhanced scanning with continual scanning. You can also optionally configure this setting to scan on-push only or to scan select repositories through inclusion rules. Images pushed to Amazon ECR are scanned for a Lifetime duration, this Amazon ECR scan setting can be changed at any time. For more information about scans for Amazon ECR, see Scanning Amazon ECR container images with Amazon Inspector (p. 67).

**Lambda standard scanning**

When you activate Lambda standard scanning, Amazon Inspector discovers the Lambda functions in your account and immediately starts scanning them for vulnerabilities. Amazon Inspector scans new Lambda functions and layers when they’re deployed, and rescans them when they’re updated or when new Common Vulnerabilities and Exposures (CVEs) are published. For more information about Lambda function scanning, see Scanning AWS Lambda functions with Amazon Inspector (p. 69).

**Lambda standard scanning + Lambda code scanning**

This can option combines Lambda standard scanning with Lambda code scanning. When Lambda code scanning is activated Amazon Inspector discovers the Lambda functions and layers in your account and scans for code vulnerabilities your application package dependencies. Lambda code scanning scans the custom application code in your Lambda functions for code vulnerabilities. These two scan types must be activated together. For more information see Amazon Inspector Lambda code scanning (p. 71).

### Activating a scan type

You can activate a new Amazon Inspector scan type at any time. Once a scan type is activated, Amazon Inspector will immediately begin scanning eligible resources for that scan type. For an overview of the available scan types see Overview of Amazon Inspector scan types (p. 57). The following describes what happens when you first activate each scan type:

- **Amazon EC2 scanning** — When you activate Amazon Inspector Amazon EC2 scanning for an account, Amazon Inspector scans all eligible instances in your account for package vulnerabilities and network reachability issues. The Amazon Inspector SSM plug-in is installed on all your SSM-managed Windows hosts. For more information, see Scanning Windows instances (p. 64). Additionally, The following SSM associations used by Amazon Inspector are created:
  - InspectorDistributor-do-not-delete
  - InspectorInventoryCollection-do-not-delete
  - InspectorLinuxDistributor-do-not-delete
  - InvokeInspectorLinuxSsmPlugin-do-not-delete
  - InvokeInspectorSsmPlugin-do-not-delete.

- **Amazon ECR scanning** — When you activate Amazon ECR container image scanning for an account, the Amazon ECR scan type for private repositories in that account changes from Basic scanning with Amazon ECR to Enhanced scanning with Amazon Inspector. Then all eligible Amazon ECR container images pushed within the last 30 days are scanned for package vulnerabilities. Additionally your Amazon ECR automated rescan duration (p. 68) is set to Lifetime.

- **Lambda standard scanning** — When you activate Lambda standard scanning in an account, all Lambda functions in your account that were invoked or updated in the last 90 days are scanned for package vulnerabilities. Additionally a CloudTrail service linked channel is created in your account.
• **Lambda standard scanning + Lambda code scanning** — These Lambda function scan types are activated together. When you activate Lambda code scanning in an account, all Lambda functions in your account that were invoked or updated in the last 90 days are scanned for code vulnerabilities.

## Activating scans

If you are the delegated administrator for Amazon Inspector in an AWS organization you can enable various Amazon Inspector scan types for multiple accounts in multiple Regions automatically using a shell script developed by Amazon Inspector [inspector2-enablement-with-cli](https://github.com/aws-kingman/inspector2-enablement-with-cli) on GitHub. Otherwise, to complete this procedure for a multi-account environment through the console, complete the following steps while signed in as the Amazon Inspector delegated administrator.

### Console

**To activate scans**

2. Using the AWS Region selector in the upper-right corner of the page, select the Region where you want to activate a new scan type.
3. In the navigation pane, choose **Account management**.
4. On the **Account management** page, select the accounts for which you would like to activate a scan type.
5. Choose **Activate** and select the type of scanning you would like to activate.
6. *(Recommended)* Repeat these steps in each AWS Region for which you want to activate that scan type.

### API

Run the **Enable** API operation. In the request, provide the account IDs you are activating scans for, and idempotency token, and one or more of **EC2**, **ECR**, **LAMBDA**, or **LAMBDA_CODE** for `resourceTypes` to activate scans of that type.

## Scanning Amazon EC2 instances with Amazon Inspector

Amazon Inspector scans packages installed on your Amazon EC2 instances for vulnerabilities. Amazon Inspector also scans your EC2 instances for network reachability issues. To perform an EC2 scan Amazon Inspector extracts package metadata from your EC2 instances. Then, Amazon Inspector compares this metadata against rules collected from security advisories to produce findings. For information about the types of findings produced for these issues, see [Finding types in Amazon Inspector (p. 12)](#).

Amazon Inspector uses [AWS Systems Manager](https://aws.amazon.com/systems-manager/) (SSM) and the SSM Agent to collect information about the software application inventory of your EC2 instances. This data is then scanned by Amazon Inspector for software vulnerabilities. Amazon Inspector can only scan for software vulnerabilities in [operating systems supported by Systems Manager](https://aws.amazon.com/systems-manager/). For information about the operating systems that Amazon Inspector supports, see [Supported operating systems for Amazon EC2 scanning (p. 129)](#).

Amazon Inspector does not require the SSM Agent to scan EC2 instances for open network paths. There are no prerequisites for this type of scanning.

For instructions on activating Amazon EC2 scans see [Activating a scan type (p. 58)](#).
Scan behaviors for Amazon EC2 scanning

Amazon Inspector performs Network reachability scans for EC2 instances once every 24 hours.

Upon activation, Amazon Inspector scans all SSM-managed instances in your account. Amazon Inspector initiates new vulnerability scans of SSM-managed EC2 instances in the following situations:

- When you launch a new EC2 instance.
- When you install new software on an existing EC2 instance (Linux and Mac).
- When Amazon Inspector adds a new common vulnerabilities and exposures (CVE) item to its database, and that CVE is relevant to your EC2 instance (Linux and Mac).

You can check when an EC2 instance was last checked for vulnerabilities from the **Instances** tab on the **Account management** page, or by using the **ListCoverage** API. Amazon Inspector updates the **Last scanned at** field for an Amazon EC2 instance in response to the following events:

- When Amazon Inspector completes an initial scan of an EC2 instance.
- When Amazon Inspector evaluates SSM inventory (every 30 minutes by default) for an EC2 instance.
- When Amazon Inspector re-scans an EC2 instance because a new CVE item impacting that instance was added to the Amazon Inspector database.

Supported operating systems and programming languages

Amazon Inspector scans supported Mac, Windows, and Linux EC2 instance for vulnerabilities in operating system packages. For Linux instances, Amazon Inspector can produce findings for application programming language packages using **Amazon Inspector Deep inspection for Amazon EC2 Linux instances** (p. 62). For Mac and Windows instances only operating system packages are scanned.

For information about supported operating systems and programming languages, see **Supported operating systems for Amazon EC2 scanning** (p. 129).

Configuring the SSM Agent

In order for Amazon Inspector to detect software vulnerabilities for an Amazon EC2 instance, the instance must be a **managed instance** in Amazon EC2 Systems Manager (SSM). An SSM managed instance has the SSM Agent installed and running, and SSM has permission to manage the instance. If you are already using SSM to manage your instances, no other steps are needed for Amazon Inspector to begin scans.

The SSM Agent is installed by default on EC2 instances created from some Amazon Machine Images (AMIs). For more information, see **About SSM Agent** in the **AWS Systems Manager User Guide**. However, even if it’s installed, you may need to activate the SSM Agent manually, and grant SSM permission to manage your instance.

The following procedure describes how to configure an Amazon EC2 instance as a managed instance using an IAM instance profile. The procedure also provides links to more detailed information in the **AWS Systems Manager User Guide**.

**AmazonSSMManagedInstanceCore** is the recommended policy to use when you attach an instance profile. This policy has all the permissions needed for Amazon Inspector EC2 scanning.
Note
You can also automate SSM management of all your EC2 instances, without the use of IAM instance profiles using SSM Default Host Management Configuration. For more information, see Default Host Management Configuration.

To configure SSM for an Amazon EC2 instance

1. If it's not already installed by your operating system vendor, install the SSM Agent. For more information, see Working with SSM Agent.
2. Use the AWS CLI to verify that the SSM Agent is running. For more information, see Checking SSM Agent status and starting the agent.
3. Grant permission for SSM to manage your instance. You can grant permission by creating an IAM instance profile and attaching it to your instance. We recommend using the AmazonSSMManagedInstanceCore policy, because this policy has the permissions for SSM Distributor, SSM Inventory and SSM State manager, that Amazon Inspector needs for scans. For instructions on creating an instance profile with these permissions and attaching it an instance, see Configure instance permissions for Systems Manager Systems Manager.
4. (Optional) Activate automatic updates for the SSM Agent. For more information, see Automating updates to SSM Agent.
5. (Optional) Configure Systems Manager to use an Amazon Virtual Private Cloud endpoint. For more information, see Create Amazon VPC endpoints.

Important
Amazon Inspector requires a Systems Manager State Manager association in your account to collect software application inventory. Amazon Inspector automatically creates an association called InspectorInventoryCollection-do-not-delete if one doesn't already exist. Amazon Inspector also requires a resource data sync and automatically creates one called InspectorResourceDataSync-do-not-delete if one doesn't already exist. For more information, see Configuring resource data sync for Inventory in the AWS Systems Manager User Guide. Each account can have a set number of resource data syncs per Region. For more information, see Maximum number of resource data syncs (per AWS account per Region) in AWS Systems Manager endpoints and quotas. If you have reached this maximum you will need to delete a Resource data syncs, see Managing resource data syncs.

Resources created for scanning

Amazon Inspector requires a number of resources in your account to run Amazon EC2 scans. The following resources are created when you first activate Amazon Inspector EC2 scanning:

InspectorInventoryCollection-do-not-delete

This is a Systems Manager State Manager (SSM) association that Amazon Inspector uses to collect software application inventory from your Amazon EC2 instances. If your account already has an SSM association for collecting inventory from InstanceIds*, Amazon Inspector will use that instead of creating it's own.

InspectorResourceDataSync-do-not-delete

This is a resource data sync that Amazon Inspector uses to send collected inventory data from your Amazon EC2 instances to an Amazon S3 bucket owned by Amazon Inspector. For more information, see Configuring resource data sync for Inventory in the AWS Systems Manager User Guide.

InspectorDistributor-do-not-delete

This is an SSM association Amazon Inspector uses for scanning Windows instances. This association installs the Amazon Inspector SSM plugin on your Windows instances. If the plugin file is inadvertently deleted this association will reinstall it at the next association interval.
InvokeInspectorSsmPlugin-do-not-delete

This is an SSM association Amazon Inspector uses for scanning Windows instances. This association allows Amazon Inspector to initiate scans using the plugin, you can also use it to set custom intervals for scans of Windows instances. For more information, see Setting custom schedules for Windows instance scans (p. 66).

InspectorLinuxDistributor-do-not-delete

This is an SSM association Amazon Inspector uses for Amazon EC2 Linux Deep inspection. This association installs the Amazon Inspector SSM plugin on your Linux instances.

InvokeInspectorLinuxSsmPlugin-do-not-delete

This is an SSM association Amazon Inspector uses for Amazon EC2 Linux Deep inspection. This association allows Amazon Inspector to initiate scans using the plugin.

Note

If any of these resources are deleted while Amazon EC2 scanning is still active in your account Amazon Inspector will attempt to recreate them at the next scan interval. When you deactivate Amazon EC2 scanning these resources are deleted.

Amazon Inspector Deep inspection for Amazon EC2 Linux instances

Note

On April 17, 2023, Amazon Inspector expanded its Amazon EC2 scanning coverage to include Deep inspection.

With Deep inspection Amazon Inspector can detect package vulnerabilities for application programming language packages in your Linux-based Amazon EC2 instances. Amazon Inspector scans default paths for programming language package libraries. You can also configure custom paths in addition to the default ones. For more information, see Custom paths for Amazon Inspector Deep inspection (p. 63).

Amazon Inspector performs Deep inspection scans using data collected from an Amazon Inspector SSM plugin. To manage the plugin and perform Deep inspection for Linux, Amazon Inspector automatically creates the following SSM associations in your account when it activates Deep inspection: InspectorLinuxDistributor-do-not-delete, and InvokeInspectorLinuxSsmPlugin-do-not-delete.

Amazon Inspector collects updated application inventory from instances for Deep inspection every 6 hours.

For a list of programming languages that Amazon Inspector supports for Deep inspection see, Supported programming languages: Amazon EC2 Deep inspection (p. 131).

Note

Deep inspection is not supported for Windows or Mac instances.

Activating or deactivating Deep inspection

Note

Deep inspection is automatically activated as part of Amazon EC2 scanning for accounts that activate Amazon Inspector after April 17, 2023.

You can check to see if Deep inspection is active for an account in the Amazon Inspector console from the Amazon EC2 scanning column on the Account management page. If Deep inspection isn't active, this column will say Activated (Deep inspection deactivated). To check the activation status programmatically, use the GetEc2DeepInspectionConfiguration API. Or, for multiple accounts, use the BatchGetMemberEc2DeepInspectionStatus API.
If you activated Amazon Inspector before April 17, 2023, you can activate Deep inspection through the console banner or the `UpdateEc2DeepInspectionConfiguration` API. If you're the delegated administrator for an organization in Amazon Inspector, you can use the `BatchUpdateMemberEc2DeepInspectionStatus` API to activate it for yourself and your member accounts.

You can deactivate Deep inspection through the `UpdateEc2DeepInspectionConfiguration` API. Member accounts in an organization can't deactivate Deep inspection. Instead, the member account must be deactivated by their delegated administrator using the `BatchUpdateMemberEc2DeepInspectionStatus` API.

**About the Amazon Inspector SSM plugin for Linux**

Amazon Inspector uses the Amazon Inspector SSM plugin to perform Deep inspection of your Linux instances. The Amazon Inspector SSM plugin is automatically installed on your Linux instances in the following directory: `/opt/aws/inspector/bin`. The name of the executable is `inspectorssmplugin`.

**Note**

Amazon Inspector uses Systems Manager Distributor to deploy the plugin in your Amazon EC2 instance. Systems Manager Distributor supports the operating systems listed as Supported package platforms and architectures in the Systems Manager guide. Your Amazon EC2 instance's operating system must be supported by Systems Manager Distributor and Amazon Inspector for Amazon Inspector to perform Deep inspection scans.

Amazon Inspector creates the following file directories to manage data collected for Deep inspection by the Amazon Inspector SSM plugin:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - The `packages.txt` in this directory stores the full paths to packages discovered by Deep inspection. If Amazon Inspector detected the same package multiple times on your instance this file lists each location that package was found.

Amazon Inspector stores logs for the plugin in the `/var/log/amazon/inspector` directory.

**Uninstalling the Amazon Inspector SSM plugin**

If the `inspectorssmplugin` file is inadvertently deleted, the `InspectorLinuxDistributor-do-not-delete` SSM association will try to reinstall the plugin at the next scan interval.

If you deactivate Deep inspection or Amazon EC2 scanning, the plugin will be automatically uninstalled from all Linux hosts.

**Custom paths for Amazon Inspector Deep inspection**

You can configure custom paths for Amazon Inspector to search when it performs Deep inspection of your Linux Amazon EC2 instances.

All accounts can define up to 5 custom paths for their individual account. If you're the delegated administrator for your organization, you can define 5 additional paths that will apply across your entire organization. This amounts to a total of up to 10 custom paths scanned per account in the organization.

Amazon Inspector scans all custom paths in addition to the following default paths that are scanned for all accounts:

- `/usr/lib`
- `/usr/lib64`
- `/usr/local/lib`
• /usr/local/lib64

**Note**
Custom paths must be local paths. Amazon Inspector doesn't scan mapped network paths like Network File System (NFS) mounts or Amazon S3 file system mounts.

**Formatting for custom paths**
The following is an example of the format for a custom path: /home/usr1/project01
Your custom paths can't be longer than 256 characters.

There is a 5,000 package limit per instance and a maximum package inventory collection time limit of 15 minutes. We recommend that you try to choose custom paths to help you avoid these limits.

**Set a custom path in the console**

**Console**
Sign in as the Amazon Inspector delegated administrator and follow the steps following to add custom paths for your organization.

2. Using the AWS Region selector in the upper-right corner of the page, select the Region where you want to activate Lambda standard scanning.
3. From the side navigation panel, under **General settings**, select **EC2 scanning settings**.
4. Under **Custom paths for your own account**, select **Edit** to add paths for your individual account. If you’re the delegated administrator, you can choose **Edit** in the **Custom paths for your organization** pane to add custom paths for all accounts within the organization.
5. Enter your custom paths in the text boxes.
6. Choose **Save** to save your custom paths. Amazon Inspector will include these paths in its next Deep inspection.

**API**
Run the **UpdateEc2DeepInspectionConfiguration**. For **packagePaths** specify an array of paths to scan.

**Scanning Windows EC2 instances with Amazon Inspector**

**Note**
On August 31, 2022, Amazon Inspector expanded its Amazon EC2 scanning coverage to include EC2 instances running Windows.

Amazon Inspector automatically discovers all supported Windows instances and includes them in continuous scanning without any extra actions. For information about which instances are supported, see [Supported operating systems for Amazon EC2 scanning](p. 129).

Unlike scans for Linux based instances, Amazon Inspector runs Windows scans at regular intervals. Windows instances are initially scanned at discovery and then scanned every 6 hours. However, the default 6-hour scan interval is adjustable. For more information, see [Setting custom schedules for Windows instance scans](p. 66). The following is an overview of how Amazon Inspector scans Windows instances:

2. The InspectorDistributor-do-not-delete SSM association uses the AWS-ConfigureAWSPackage SSM document and the AmazonInspector2-InspectorSsmPlugin SSM Distributor package to install the Amazon Inspector SSM plug-in on your Windows instances. See About the Amazon Inspector SSM plug-in for Windows (p. 65) for more information.

3. The InvokeInspectorSsmPlugin-do-not-delete SSM association runs the Amazon Inspector SSM plug-in at regular intervals to collect instance data and generate Amazon Inspector findings. By default, the interval is every 6 hours. However, you can customize this by setting a cron expression or rate expression for the association using SSM. For more information, see Reference: Cron and rate expressions for Systems Manager in the AWS Systems Manager User Guide.

Note
Amazon Inspector stages updated Open Vulnerability and Assessment Language (OVAL) definition files to the S3 bucket inspector2-oval-prod-REGION. This S3 bucket contains the OVAL definitions used in scans and shouldn't be modified. Changing this setting will prevent Amazon Inspector from scanning for new CVEs as they're released.

Amazon Inspector scan requirements for Windows instances

To scan a Windows instance, Amazon Inspector requires the instance to meet the following criteria:

- The instance is an SSM managed instance. For instructions about setting up your instance for scanning, see Configuring the SSM Agent (p. 60).
- The instance operating system is one of the supported Windows operating systems. For a complete list of supported operating systems, see Supported operating systems for Amazon EC2 scanning (p. 129).
- The instance has the Amazon Inspector SSM plug-in installed. Amazon Inspector automatically installs the Amazon Inspector SSM plug-in for managed instances upon discovery. See the next topic for details about the plugin.

Note
If your host is running in an Amazon VPC without outgoing internet access, Windows scanning requires your host to be able to access Regional Amazon S3 endpoints. To learn how to configure an Amazon S3 Amazon VPC endpoint, see Create a gateway endpoint in the Amazon Virtual Private Cloud User Guide. If your Amazon VPC endpoint policy is restricting access to external S3 buckets, you must specifically allow access to the bucket maintained by Amazon Inspector in your AWS Region that stores the OVAL definitions used to evaluate your instance. This bucket has the following the format: inspector2-oval-prod-REGION.

About the Amazon Inspector SSM plug-in for Windows

The Amazon Inspector SSM plug-in is required for Amazon Inspector to scan your Windows instances. The Amazon Inspector SSM plug-in is automatically installed on your Windows instances in the following system location: C:\Program Files\Amazon\Inspector. The executable binary file installed at this location is named InspectorSsmPlugin.exe.

The following file locations are created to store data collected by the Amazon Inspector SSM plug-in:

- C:\ProgramData\Amazon\Inspector\Input
- C:\ProgramData\Amazon\Inspector\Output
- C:\ProgramData\Amazon\Inspector\Logs
Uninstalling the Amazon Inspector SSM plug-in

If the InspectorSsmPlugin.exe file is inadvertently deleted, the InspectorDistributor-do-not-delete SSM association will reinstall the plugin at the next Windows scan interval. If you want to uninstall the Amazon Inspector SSM plug-in, you can use the **Uninstall** action on the AmazonInspector2-ConfigureInspectorSsmPlugin document.

Additionally, the Amazon Inspector SSM plug-in will be automatically uninstalled from all Windows hosts if you deactivate Amazon EC2 scanning.

**Note**
If you uninstall the SSM Agent before deactivating Amazon Inspector, the Amazon Inspector SSM plug-in will remain on the Windows host but will no longer send data to the Amazon Inspector SSM plug-in. For more information, see [Deactivating Amazon Inspector](p. 137).

Setting custom schedules for Windows instance scans

You can customize the time between your Windows Amazon EC2 instance scans by setting a cron expression or rate expression for the InvokeInspectorSsmPlugin-do-not-delete association using SSM. For more information, see [Reference: Cron and rate expressions for Systems Manager](in the AWS Systems Manager User Guide) or use the following instructions.

Select from the following code examples to change the scan cadence for Windows instances from the default 6 hours to 12 hours using either a rate expression or a cron expression.

The following examples require you to use the **AssociationId** for the association named InvokeInspectorSsmPlugin-do-not-delete. You can retrieve your **AssociationId** by running the following AWS CLI command:

```
$ aws ssm list-associations --association-filter-list "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

**Note**
The **AssociationId** is Regional, so you need to first retrieve a unique ID for each AWS Region. You can then run the command to change the scan cadence in each Region where you want to set a custom scan schedule for Windows instances.

**Example rate expression**
```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

**Example cron expression**
```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

Excluding instances from Amazon Inspector scans

You can tag certain instances to exclude them from Amazon Inspector scans. Excluding instances from scans can help prevent unactionable alerts. You are not charged for excluded instances.
To exclude an EC2 instance from scans, tag the instance with the following key:

- **InspectorEc2Exclusion**

Value is optional.

For more information about adding tags to EC2 instances, see [Tag your Amazon EC2 resources](#).

---

**Scanning Amazon ECR container images with Amazon Inspector**

Amazon Inspector scans container images stored in Amazon ECR for software vulnerabilities to generate **Package Vulnerability** findings. For information about the types of findings produced for these issues, see [Finding types in Amazon Inspector](#) (p. 12).

When you activate Amazon Inspector scans for Amazon ECR, you set Amazon Inspector as your preferred scanning service for your private registry. This replaces the default basic scanning, which is provided at no charge by Amazon ECR, with **Enhanced scanning**, which is provided and billed through Amazon Inspector.

The enhanced scanning provided by Amazon Inspector gives you the benefit of vulnerability scanning for both operating system and programming language packages at the registry level. You can review findings discovered using enhanced scanning at the image level, for each layer of the image, on the Amazon ECR console. Additionally, you can review and work with these findings in other services not available for basic scanning findings, including AWS Security Hub and Amazon EventBridge. You can view findings discovered by scans on the Amazon Inspector console at [https://console.aws.amazon.com/inspector/](https://console.aws.amazon.com/inspector/). For information about working with findings, see [Managing findings in Amazon Inspector](#) (p. 21).

For instructions on activating Amazon ECR scans see [Activating a scan type](#) (p. 58).

**Scan behaviors for Amazon ECR scanning**

When you first activate Amazon ECR scanning, Amazon Inspector scans eligible images pushed in the last 30 days. By default, images are scanned for a **Lifetime** duration. However, you can configure a different duration through the console or API. For more information, see [Configuring the ECR automated re-scan duration](#) (p. 68). After ECR scanning is activated all images pushed to ECR are continually scanned for the configured automated rescan duration.

Amazon Inspector initiates new vulnerability scans of container images in the following situations:

- Whenever a new container image is pushed.
- Whenever Amazon Inspector adds a new common vulnerabilities and exposures (CVE) item to its database, and that CVE is relevant to that container image (continuous scanning only).

You can check when a container image was last checked for vulnerabilities from the **Container images** tab on the **Account management** page, or by using the **ListCoverage** API. Amazon Inspector updates the **Last scanned at** field of an Amazon ECR image in response to the following events:

- When Amazon Inspector completes an initial scan of a container image.
- When Amazon Inspector re-scans a container image because a new common vulnerabilities and exposures (CVE) item that impacts that container image was added to the Amazon Inspector database.
Supported operating systems and media types

For information about supported operating systems, see Supported operating systems for Amazon ECR scanning (p. 131).

Amazon Inspector scans of Amazon ECR repositories cover the following supported media types:

- "application/vnd.docker.distribution.manifest.v1+json"
- "application/vnd.docker.distribution.manifest.v1+prettyjws"
- "application/vnd.oci.image.manifest.v1+json"
- "application/vnd.docker.distribution.manifest.v2+json"

Note
Scratch images and DockerV2ListMediaType images aren't supported.

Configuring enhanced scanning for Amazon ECR repositories

When you activate Amazon Inspector scans for Amazon ECR container images, you change the scanning configuration setting for your private registry. The scan type for your registry is changed from Basic scanning to Enhanced scanning provided by Amazon Inspector. For more information see Image scanning in the Amazon ECR user guide.

You can manage settings for enhanced scanning at the repository level in ECR. You can choose continuous scanning or on-push scanning for your repositories. Continuous scanning includes on-push scans and automated rescans. On-push scanning scans only when you initially push an image. For both options, you can refine the scanning scope through inclusion filters. By default, when you first activate enhanced scanning your settings are set to Continuously scan all repositories.

To configure your enhanced scanning settings

1. Open the Amazon ECR console at https://console.aws.amazon.com/ecr/.
2. By using the AWS Region selector in the upper-right corner of the page, select the Region that has the repositories that you are scanning.
3. In the navigation pane, choose Private registry, then choose Scanning.
4. Under Scan type, make sure Enhanced scanning is selected. If it's not, select Enhanced scanning.
   By default, the Continuously scan all repositories option is selected which turns on complete Amazon Inspector scan coverage for all repositories.
5. Deselect Continuously scan all repositories to filter which repositories are scanned continuously or on-push.

For more information on configuring enhanced scans see Using enhanced scanning in the Amazon ECR user guide.

Configuring the ECR automated re-scan duration

The Amazon ECR automated re-scan duration setting determines how long Amazon Inspector continuously monitors images pushed into repositories. When the number of days from when an image is first pushed exceeds the automated re-scan duration configuration, Amazon Inspector stops monitoring the image. When Amazon Inspector stops monitoring an image, it changes the scan status of the image to inactive with a reason code of expired. Then all associated findings for the image are scheduled to be closed.
You can set the Amazon ECR automated re-scan duration in Amazon Inspector to best suit your environment. For example, if you build images often, you can use a shorter scan duration. However, if you continue to use images for long periods of time you can choose a longer scan duration. The default scan duration for new accounts, including new accounts added to an organization, is **Lifetime**. This means Amazon Inspector scans your images until they're deleted.

When you set the automated re-scan duration from a delegated administrator account that setting is applied to all member accounts in the organization.

The following scan duration options are available.

- 30 days
- 180 days
- Lifetime (default)

**To configure the ECR automated re-scan duration**

2. In the navigation pane, under **General settings**, choose **ECR scanning settings**.
3. Under **ECR re-scan duration**, choose the duration that you want.
4. Choose **Save**. Your new setting applies immediately.

If you increase the duration, for example, from **30 days** to **180 days**, Amazon Inspector applies the change to all images actively being scanned in repositories configured for continual scanning. However, images with a scan status of **expired** remain expired.

If you decrease the duration, for example, from **Lifetime** to **180 days**, Amazon Inspector applies the change to all active images being scanned in repositories configured for continual scanning. Images that are older than your new setting have their scan status changed to **expired** and are no longer monitored. For scanning to be resumed, you must push the image to the repository again.

---

**Scanning AWS Lambda functions with Amazon Inspector**

Amazon Inspector support for AWS Lambda functions provides continuous, automated security vulnerability assessments for Lambda functions and layers. Amazon Inspector offers two types of scanning for Lambda. These scan types look for different types of vulnerabilities.

**Amazon Inspector Lambda standard scanning**

This is the default Lambda scan type. Lambda standard scanning scans application dependencies within a Lambda function and its layers for **package vulnerabilities** (p. 12). For more information, see [Lambda standard scanning](p. 71).

**Amazon Inspector Lambda code scanning**

This scan type scans the custom application code in your functions and layers for **code vulnerabilities** (p. 13). You can either activate Lambda standard scanning or activate Lambda standard scanning together with Lambda code scanning. For more information, see [Amazon Inspector Lambda code scanning](p. 71).

When you activate Lambda scanning Amazon Inspector creates the following AWS CloudTrail service-linked channels in your account:
Scan behaviors for Lambda function scanning

Upon activation, Amazon Inspector scans all Lambda functions invoked or updated in the last 90 days in your account. Amazon Inspector initiates vulnerability scans of Lambda functions in the following situations:

- As soon Amazon Inspector discovers an existing Lambda function.
- When you deploy a new Lambda function to the Lambda service.
- When you deploy an update to the application code or dependencies of an existing Lambda function or its layers.
- Whenever Amazon Inspector adds a new common vulnerabilities and exposures (CVE) item to its database, and that CVE is relevant to your function.

Amazon Inspector monitors each Lambda function throughout its lifetime until it's either deleted or excluded from scanning.

You can check when a Lambda function was last checked for vulnerabilities from the Lambda functions tab on the Account management page, or by using the ListCoverage API. Amazon Inspector updates the Last scanned at field for a Lambda function in response to the following events:

- When Amazon Inspector completes an initial scan of a Lambda function.
- When a Lambda function is updated.
- When Amazon Inspector re-scans a Lambda function because a new CVE item impacting that function was added to the Amazon Inspector database.

Supported runtimes and eligible functions

Amazon Inspector supports different runtimes for Lambda standard scanning and Lambda code scanning. For a list of supported runtimes for each scan type, see Supported runtimes: Amazon Inspector Lambda standard scanning (p. 133) and Supported runtimes: Amazon Inspector Lambda code scanning (p. 134).

In addition to having a supported runtime, a Lambda function needs to meet the following criteria to be eligible for Amazon Inspector scans:

- The function has been invoked or updated in the last 90 days.
- The function is marked $LATEST.
- The function isn't excluded from scans by tags.
Note
Lambda functions that haven't been invoked or modified in the last 90 days are automatically excluded from scans. Amazon Inspector will resume scanning an automatically excluded function if it is invoked again or if changes are made to the Lambda function code.

Amazon Inspector Lambda standard scanning

Amazon Inspector Lambda standard scanning identifies software vulnerabilities in the application package dependencies used in your Lambda function code and layers. For example, if your Lambda function uses a version of the python-jwt package with a known vulnerability, Lambda standard scanning will generate a finding for that function.

If Amazon Inspector detects a vulnerability in your Lambda function application package dependencies, Amazon Inspector produces a detailed Package Vulnerability type finding.

For instructions on activating a scan type see Activating a scan type (p. 58).

Note
Deactivating Amazon Inspector Lambda standard scanning will also deactivate Amazon Inspector Lambda code scanning.

Excluding functions from Lambda standard scanning

You can tag certain functions to exclude them from Amazon Inspector Lambda standard scans. Excluding functions from scans can help prevent unactionable alerts.

To exclude a Lambda function from Lambda standard scanning, tag the function with the following key-value pair:

• Key: InspectorExclusion
  • Value: LambdaStandardScanning

To exclude a function from Lambda standard scanning

1. Log in to the Lambda console at https://console.aws.amazon.com/lambda/.
2. Select Functions.
3. From the functions table, select the name of a function that you would like to exclude from Amazon Inspector Lambda standard scanning.
4. Select Configuration and choose Tags from the menu.
5. Select Manage tags, and then Add new tag.
6. In the Key field, enter InspectorExclusion, then, in the Value field, enter LambdaStandardScanning.
7. Select Save to add the tag and exclude your function from Amazon Inspector Lambda standard scanning.

For more information about adding tags in Lambda, see Using tags on Lambda functions.

Amazon Inspector Lambda code scanning

Important
Code scanning captures code snippets from Lambda functions to highlight detected vulnerabilities. These snippets may show hardcoded credentials or other sensitive materials in plaintext.
Amazon Inspector Lambda code scanning scans the custom application code within a Lambda function for code vulnerabilities based on AWS security best practices. Lambda code scanning can detect injection flaws, data leaks, weak cryptography, or missing encryption in your code. For information about the available Regions, see Region-specific feature availability (p. 140).

Lambda standard scanning is a feature that evaluates the application package dependencies used in a function for common vulnerabilities and exposures (CVE). You can activate Lambda code scanning together with Lambda standard scanning.

Amazon Inspector evaluates your Lambda function application code using automated reasoning and machine learning that analyzes your application code for an overall security compliance. It identifies policy violations and vulnerabilities based on internal detectors developed in collaboration with Amazon CodeGuru. For a list of possible detections, see the CodeGuru Detector Library.

If Amazon Inspector detects a vulnerability in your Lambda function application code, Amazon Inspector produces a detailed Code Vulnerability type finding. This finding type includes the issue's exact location in the code, a code snippet showing the issue, and a suggested remediation.

**Important**
You are responsible for the remediation suggestions that you accept. Always review remediation suggestions before accepting them. You may need to make edits to remediation suggestions to ensure that your code does what you intended.

### Encrypting your code in code vulnerability findings

Code snippets detected in connection with a code vulnerability finding using Lambda code scanning are stored by the CodeGuru service. By default an AWS owned key controlled by CodeGuru is used to encrypt your code, however, you can use your own customer managed key for encryption through the Amazon Inspector API. For more information see Encryption at rest for code in your findings (p. 93).

Lambda code scanning can be activated together with Lambda standard scanning. For instructions on activating a scan type see Activating a scan type (p. 58).

### Excluding functions from Lambda code scanning

You can tag certain functions to exclude them from Amazon Inspector Lambda code scans. Excluding functions from scans can help prevent unactionable alerts.

To exclude a Lambda function from Amazon Inspector, Lambda code scans tag the function with the following key-value pair:

- **Key**: InspectorCodeExclusion
- **Value**: LambdaCodeScanning

**To exclude a function from Lambda code scanning**

1. Log in to the Lambda console at https://console.aws.amazon.com/lambda/.
2. Select **Functions**.
3. From the functions table, select the name of a function that you would like to exclude from Amazon Inspector Lambda code scanning.
4. Select **Configuration** and choose **Tags** from the menu.
5. Select **Manage tags**, and then **Add new tag**.
6. In the **Key** field, enter InspectorCodeExclusion, then, in the **Value** field, enter LambdaCodeScanning.
7. Select **Save** to add the tag and exclude your function from Amazon Inspector Lambda code scanning.
Deactivating a scan type

You can deactivate a new Amazon Inspector scan type at any time. When you deactivate a scan type you lose access to any existing findings you have that were produced by that scan type. If you reactivate the scan type your eligible resources are scanned and Amazon Inspector will produce new findings. To keep a record of your findings data you can export your findings before you deactivate. For more information, see Exporting findings reports from Amazon Inspector (p. 24).

When you deactivate a scan type certain changes may occur in that AWS account depending on the scan type being deactivated. The following are the changes that will occur when you deactivate these scan types:

- **Amazon EC2 scanning** — When you deactivate Amazon Inspector Amazon EC2 scanning for an account, the following SSM associations used by Amazon Inspector are deleted:
  - InspectorDistributor-do-not-delete
  - InspectorInventoryCollection-do-not-delete
  - InspectorLinuxDistributor-do-not-delete
  - InvokeInspectorLinuxSsmPlugin-do-not-delete
  - InvokeInspectorSsmPlugin-do-not-delete. Additionally, the Amazon Inspector SSM plug-in installed through this association is removed from all of your Windows hosts. For more information, see Scanning Windows instances (p. 64).

- **Amazon ECR scanning** — When you deactivate Amazon ECR container image scanning for an account, the Amazon ECR scan type for that account changes from Enhanced scanning with Amazon Inspector to Basic scanning with Amazon ECR.

- **Lambda standard scanning** — When you deactivate Lambda standard scanning in an account, it will deactivate Lambda code scanning if code scanning was also active. Additionally the CloudTrail service linked channel created when scanning was enabled is deleted.

Deactivating scans

Deactivating all scan types for an account deactivates Amazon Inspector for that account in that AWS Region. For more information, see Deactivating Amazon Inspector (p. 137).

To complete this procedure for a multi-account environment, follow these steps while signed in as the Amazon Inspector delegated administrator.

### Console

To deactivate scans

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. By using the AWS Region selector in the upper-right corner of the page, select the Region where you want to deactivate scans.
3. In the navigation pane, choose Account management.
4. Choose the Accounts tab to show the scanning status of an account.
5. Select the check box of each account for which you want to deactivate scans.
6. Choose Actions, and, from the Deactivate options, select the scan type you wish to deactivate.
7. (Recommended) Repeat these steps in each AWS Region for which you want to deactivate that scan type.
API

Run the Disable API operation. In the request, provide the account IDs you are deactivating scans for, and for resourceTypes provide one or more of EC2, ECR, LAMBDA, or LAMBDA_CODE to deactivate scans.
Assessing Amazon Inspector coverage of your AWS environment

To help you assess and interpret Amazon Inspector coverage of your AWS environment, the Account management page on the Amazon Inspector console provides statistics and details about the status of Amazon Inspector scanning for your accounts and resources. With this page, you can review aggregated statistics and other data for your resources. You can also perform in-depth analysis of Amazon Inspector coverage for individual resources and drill down to review findings for specific resources. If you're the delegated Amazon Inspector administrator for an organization, the data includes statistics and details for all the accounts in your organization.

To assess Amazon Inspector coverage of your AWS environment

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. In the navigation pane, choose Account management.
3. On the Account management page, choose the tab for one of five different coverage views:
   - Accounts, for account-level coverage.
   - Instances, for coverage of Amazon Elastic Compute Cloud (Amazon EC2) instances.
   - Repositories, for coverage of Amazon Elastic Container Registry (Amazon ECR) repositories.
   - Images, for coverage of Amazon ECR container images.
   - Lambda, for coverage of Lambda functions.

The topics in this section describe the information that each tab provides, including the scanning status that an individual resource can have.

Topics
- Assessing account-level coverage (p. 75)
- Assessing coverage of Amazon EC2 instances (p. 76)
- Assessing coverage of Amazon ECR repositories (p. 76)
- Assessing coverage of Amazon ECR container images (p. 77)
- Assessing coverage of AWS Lambda functions (p. 77)
- Assessing the scanning status of individual resources (p. 78)

Assessing account-level coverage

If your account is not part of an organization or is not the delegated Amazon Inspector administrator account for an organization, the Accounts tab provides information about your account and the status of resource scanning for your account. On this tab, you can activate or deactivate scanning for all or only specific types of resources for your account. For more information, see Scanning resources with Amazon Inspector (p. 57).

If your account is the delegated Amazon Inspector administrator account for an organization, the Accounts tab provides automatic activation settings for accounts in your organization, and it lists all the accounts in your organization. For each account, the list indicates whether Amazon Inspector is activated for the account and, if so, the resource scanning types that are activated for the account.
As the delegated administrator, you can use this tab to change the automatic activation settings for your organization. You can also activate or deactivate specific types of resource scanning for individual member accounts. For more information, see Activating Amazon Inspector scans for member accounts (p. 85).

Assessing coverage of Amazon EC2 instances

The **Instances** tab shows Amazon EC2 instances in your AWS environment. The lists are organized into groups on the following tabs:

- **All** – Shows all the instances in your environment. The **Status** column indicates the current scanning status for an instance. For a list of possible status values and a description of each one, see Assessing the scanning status of individual resources (p. 78).
- **Scanning** – Shows all the instances that Amazon Inspector is actively monitoring and scanning in your environment.
- **Not scanning** – Shows all the instances that Amazon Inspector is not monitoring and scanning in your environment. The **Reason** column indicates why Amazon Inspector is not monitoring and scanning an instance.

An EC2 instance can appear on the **Not scanning** tab for any of several reasons. Amazon Inspector uses AWS Systems Manager (SSM) and the SSM Agent to automatically monitor and scan your EC2 instances for vulnerabilities. If an instance does not have the SSM Agent running, does not have an AWS Identity and Access Management (IAM) role that supports Systems Manager, or is not running a supported operating system or architecture, Amazon Inspector cannot monitor and scan the instance. For more information, see Scanning Amazon EC2 instances (p. 59).

On each tab, the **Account** column specifies the AWS account that owns an instance. The **Last scanned** column shows you when Amazon Inspector last checked that resource for vulnerabilities. This can include checks when there is an update to finding metadata, when there is an update to the application inventory of the resource, or when a rescan is done in response to a new CVE. For more information see Scan behaviors for Amazon EC2 scanning (p. 60).

To review additional details about an EC2 instance, choose the link in the **EC2 instance** column. Amazon Inspector then displays details about the instance and current findings for the instance. To review the details of a finding, choose the link in the **Title** column. For information about these details, see Amazon Inspector finding details (p. 14).

Assessing coverage of Amazon ECR repositories

The **Repositories** tab shows Amazon ECR repositories in your AWS environment. The lists are organized into groups on the following tabs:

- **All** – Shows all the repositories in your environment. The **Status** column indicates the current scanning status for a repository. For a list of possible status values and a description of each one, see Assessing the scanning status of individual resources (p. 78).
- **Activated** – Shows all the repositories that Amazon Inspector is configured to monitor and scan in your environment. The **Status** column indicates the current scanning status for a repository.
- **Not activated** – Shows all the repositories that Amazon Inspector is not monitoring and scanning in your environment. The **Reason** column indicates why Amazon Inspector is not monitoring and scanning a repository.

On each tab, the **Account** column specifies the AWS account that owns a repository.
To review additional details about a repository, choose the repository’s name. Amazon Inspector then displays a list of container images in the repository and details for each image. The details include the image tag, image digest, and scanning status. They also include key finding statistics, such as the number of **Critical** findings for the image. To drill down and review supporting data for finding statistics, choose the image tag for the image.

### Assessing coverage of Amazon ECR container images

The **Images** tab shows Amazon ECR container images in your AWS environment. The lists are organized into groups on the following tabs:

- **All** – Shows all the container images in your environment. The **Status** column indicates the current scanning status for an image. For a list of possible status values and a description of each one, see [Assessing the scanning status of individual resources](p. 78).
- **Scanning** – Shows all the container images that Amazon Inspector is configured to monitor and scan in your environment. The **Status** column indicates the current scanning status for an image.
- **Not scanning** – Shows all the container images that Amazon Inspector is not monitoring and scanning in your environment. The **Reason** column indicates why Amazon Inspector is not monitoring and scanning an image.

A container image can appear on the **Not activated** tab for any of several reasons. The image might be stored in a repository that Amazon Inspector scans are not activated for, or Amazon ECR filtering rules prevent that repository from being scanned. Or a new image has not been pushed within the duration that you specified for automated re-scans of images in the repository. For more information, see [Scanning Amazon ECR container images](p. 67).

On each tab, the **Repository name** column specifies the name of the repository that stores a container image. The **Account** column specifies the AWS account that owns the repository. The **Last scanned** column shows you when Amazon Inspector last checked that resource for vulnerabilities. This can include checks when there is an update to finding metadata, when there is an update to the application inventory of the resource, or when a rescan is done in response to a new CVE. For more information see [Scan behaviors for Amazon ECR scanning](p. 67).

To review additional details about a container image, choose the link in the **ECR container image** column. Amazon Inspector then displays details about the image and current findings for the image. To review the details of a finding, choose the link in the **Title** column. For information about these details, see [Amazon Inspector finding details](p. 14).

### Assessing coverage of AWS Lambda functions

The **Lambda** tab shows Lambda functions in your AWS environment. This page two tables, one that shows function coverage details for Lambda standard scanning and another for Lambda code scanning. You can group functions based on the following tabs:

- **All** – Shows all the Lambda functions in your environment. The **Status** column indicates the current scanning status for a Lambda function. For a list of possible status values and a description of each one, see [Assessing the scanning status of individual resources](p. 78).
- **Scanning** – Shows the Lambda functions that Amazon Inspector is configured to scan. The **Status** column indicates the current scanning status for each Lambda function.
- **Not scanning** – Shows the Lambda functions that Amazon Inspector is not configured to scan. The **Reason** column indicates why Amazon Inspector is not monitoring and scanning a function.
A Lambda function can appear on the **Not scanning** tab for several reasons. The Lambda function might belong to an account that hasn't been added to Amazon Inspector or filtering rules prevent this function from being scanned. For more information, see [Scanning AWS Lambda functions](#) (p. 69).

On each tab, the **Function name** column specifies the name of the Lambda function. The **Account** column specifies the AWS account that owns the function. The **Runtime** specifies the function's runtime. The **Status** column indicates the current scanning status for each Lambda function. The **Resource tags** shows the tags that have been applied to the function. The **Last scanned** column shows you when Amazon Inspector last checked that resource for vulnerabilities. This can include checks when there is an update to finding metadata, when there is an update to the application inventory of the resource, or when a rescan is done in response to a new CVE. For more information see [Scan behaviors for Lambda function scanning](#) (p. 70).

### Assessing the scanning status of individual resources

By using the **Instances**, **Repositories**, and **Images** tabs on the **Account management** page, you can check the status of Amazon Inspector scanning for individual resources of a specified type: choose **All** on the appropriate tab, and then refer to the **Status** column. The **Status** column indicates the current status of Amazon Inspector scanning for a resource.

#### Amazon EC2 instances

For an Amazon Elastic Compute Cloud (Amazon EC2) instance, the possible **Status** values are:

- **Actively monitoring** – Amazon Inspector is continuously monitoring and scanning the instance.
- **EC2 instance stopped** – Amazon Inspector paused scanning for the instance because the instance is in a stopped state. Any existing findings will persist until the instance is terminated. If the instance is restarted, Amazon Inspector will automatically resume scanning for the instance.
- **Internal error** – An internal error occurred when Amazon Inspector attempted to scan the instance. Amazon Inspector will automatically address the error and resume scanning as soon as possible.
- **No inventory** – Amazon Inspector couldn't find the software application inventory to scan for the instance. The Amazon Inspector associations for the instance might have been deleted or they might have failed to run.

To remediate this issue, use AWS Systems Manager to ensure that the InspectorInventoryCollection-do-not-delete association exists and its association status is successful. In addition, use AWS Systems Manager Fleet Manager to verify the software application inventory for the instance.

- **Pending disable** – Amazon Inspector has stopped scanning the instance. The instance is being disabled, pending completion of clean-up tasks.
- **Pending initial scan** – Amazon Inspector has queued the instance for an initial scan.
- **Resource terminated** – The instance was terminated. Amazon Inspector is currently cleaning up existing findings and coverage data for the instance.
- **Stale inventory** – Amazon Inspector wasn't able to collect an updated software application inventory that was captured within the past 7 days for the instance.

To remediate this issue, use AWS Systems Manager to ensure that the required Amazon Inspector associations exist and are running for the instance. In addition, use AWS Systems Manager Fleet Manager to verify the software application inventory for the instance.
• **Unmanaged EC2 instance** – Amazon Inspector isn’t monitoring or scanning the instance. The instance isn’t managed by AWS Systems Manager.

To remediate this issue, you can use the [AWSSupport-TroubleshootManagedInstance runbook](https://aws.amazon.com/support/knowledge-center/aws-support-troubleshoot-managed-instance/) provided by AWS Systems Manager Automation. After you configure AWS Systems Manager to manage the instance, Amazon Inspector will automatically begin to continuously monitor and scan the instance.

• **Unsupported OS** – Amazon Inspector isn’t monitoring or scanning the instance. The instance uses an operating system or architecture that Amazon Inspector doesn’t support. For a list of operating systems that Amazon Inspector supports, see [Supported operating systems for Amazon EC2 scanning](p. 129).

• **Actively monitoring with partial errors** – This status means that EC2 scanning is active, but there are errors associated with [Amazon Inspector Deep inspection for Amazon EC2 Linux instances](p. 62). The possible Deep inspections errors are:
  - **Deep inspection package collection limit exceeded** – The instance has exceeded the 5000 package limit for Inspector Deep inspection. To resume Deep inspection for this instance you can try to adjust the custom paths associated with the account.
  - **Deep inspection daily ssm inventory limit exceeded** – The SSM agent couldn't send inventory to Inspector because the SSM quota for [inventory data collected per instance per day](https://aws.amazon.com/premiumsupport/knowledge-center/awssupport-ssm-quota-how-to-see/) has already been reached for this instance. For more information, see [Amazon EC2 Systems Manager endpoints and quotas](https://aws.amazon.com/premiumsupport/knowledge-center/awssupport-ssm-quota-how-to-see/).
  - **Deep inspection collection time limit exceeded** – Inspector failed to extract the package inventory because the package collection time exceeding the maximum threshold of 15 minutes.
  - **Deep inspection has no inventory** – Inspector plug-in hasn't yet been able to collect an inventory of packages for this instance. This is usually the result of a pending scan, however, if this status persists after 6 hours, use Amazon EC2 Systems Manager to ensure that the required Amazon Inspector associations exist and are running for the instance.

For details about configuring the scanning settings for an EC2 instance, see [Scanning Amazon EC2 instances](p. 59).

### Amazon ECR repositories and container images

For an Amazon Elastic Container Registry (Amazon ECR) repository or container image, the possible **Status** values are:

• **Activated (Continuous)** – For a repository, Amazon Inspector is continuously monitoring and scanning container images in the repository. The enhanced scanning setting for the repository is set to continuous scanning. Continuous scanning includes an initial scan of new images when they are pushed to the repository and automated re-scans of images in the repository.

For a container image, Amazon Inspector is continuously monitoring and scanning the image. Enhanced scanning is enabled for the repository that stores the image, and the enhanced scanning setting for the repository is set to continuous scanning.

• **Access denied** – Amazon Inspector isn’t allowed to access the repository or any container images in the repository.

To remediate this issue, ensure that AWS Identity and Access Management (IAM) policies for the repository allow Amazon Inspector to access the repository.

• **Deactivated (Manual)** – Amazon Inspector isn’t monitoring or scanning any container images in the repository. The Amazon ECR scanning setting for the repository is set to basic, manual scanning.

To start scanning images in the repository with Amazon Inspector, change the scanning setting for the repository to enhanced scanning, and then choose whether to scan images continuously or only when a new image is pushed.
- **Activated (Continuous)** – For a repository, Amazon Inspector is continuously monitoring and scanning container images in the repository. The enhanced scanning setting for the repository is set to continuous scanning. Continuous scanning includes an initial scan of new images when they are pushed to the repository and automated re-scans of images in the repository.

For a container image, Amazon Inspector is continuously monitoring and scanning the image. Enhanced scanning is activated for the repository that stores the image, and the enhanced scanning setting for the repository is set to continuous scanning.

- **Activated (On push)** – For a repository, Amazon Inspector automatically scans individual container images in the repository when a new image is pushed. The enhanced scanning setting for the repository is set to scan on push.

For a container image, Amazon Inspector automatically scans the image each time a new image is pushed. Enhanced scanning is activated for the repository that stores the image, and the enhanced scanning setting for the repository is set to scan on push.

- **Internal error** – An internal error occurred when Amazon Inspector attempted to scan the repository or container image. Amazon Inspector will automatically address the error and resume scanning as soon as possible.

- **Pending initial scan** – This status doesn't apply to repositories. For a container image, Amazon Inspector has queued the image for an initial scan.

- **Scan eligibility expired (Continuous)** – This status doesn't apply to repositories. For a container image, Amazon Inspector suspended scanning for the image. The image hasn't been updated within the duration that you specified for automated re-scans of images in the repository. To resume scanning for the image, update the image.

- **Scan eligibility expired (On push)** – This status doesn't apply to repositories. For a container image, Amazon Inspector suspended scanning for the image. The image hasn't been updated within the duration that you specified for automated re-scans of images in the repository. To resume scanning for the image, update the image.

- **Scan frequency manual (Manual)** – Amazon Inspector doesn't scan the Amazon ECR container image. The Amazon ECR scanning setting for the repository that stores image is set to basic, manual scanning. To start scanning the image automatically with Amazon Inspector, change the repository setting to enhanced scanning, and then choose whether to scan images continuously or only when a new image is pushed.

- **Unsupported OS** – This status doesn't apply to repositories. For a container image, Amazon Inspector isn't monitoring or scanning the image. The image is based on an operating system that Amazon Inspector doesn't support, or it uses a media type that Amazon Inspector doesn't support.

For a list of operating systems that Amazon Inspector supports, see [Supported operating systems for Amazon ECR scanning](p. 131). For a list of media types that Amazon Inspector supports, see [Supported media types](p. 68).

For details about configuring the scanning settings for repositories and images, see [Scanning Amazon ECR container images](p. 67).

### AWS Lambda functions

For a Lambda function, the possible **Status** values are:

- **Actively monitoring** – Amazon Inspector is continuously monitoring and scanning Lambda functions. Continuous scanning includes an initial scan of new functions when they are pushed to the repository and automated re-scans of functions when they are updated or when new Common Vulnerabilities and Exposures (CVEs) are released.

- **Excluded by tag** – Amazon Inspector isn't scanning this function because it has been excluded from scans by tags.
• **Scan eligibility expired**—Amazon Inspector is not monitoring this function because it has been 90 days or more since it was last invoked or updated.

• **Internal error**—An internal error occurred when Amazon Inspector attempted to scan the function. Amazon Inspector will automatically address the error and resume scanning as soon as possible.

• **Pending initial scan**—Amazon Inspector has queued the function for an initial scan.

• **Unsupported**—The Lambda function has an unsupported runtime.
Managing multiple accounts in Amazon Inspector with AWS Organizations

With Amazon Inspector, you can manage multiple accounts that are associated through AWS Organizations. To manage multiple Amazon Inspector accounts, the AWS Organizations management account designates an account within the organization as the delegated administrator account for Amazon Inspector. The delegated administrator manages Amazon Inspector for the organization and is granted special permissions to perform tasks on behalf of your organization. These tasks include activating or deactivating scans for member accounts, viewing aggregated finding data from the entire organization, and the creation and management of suppression rules.

**Note**
To programatically enable Amazon Inspector for multiple accounts in multiple Regions you can use a shell script developed by Amazon Inspector. For more information on using this script see the inspector2-enablement-with-cli on GitHub.

**Topics**
- Understanding the relationship between administrator and member accounts in Amazon Inspector (p. 82)
- Designating a delegated administrator for Amazon Inspector (p. 83)

Understanding the relationship between administrator and member accounts in Amazon Inspector

When you use Amazon Inspector in a multiple-account environment, the Amazon Inspector delegated administrator account has access to certain metadata. This metadata includes Amazon EC2 and Amazon ECR configuration data and security finding results for member accounts. The administrator account can also create finding suppression rules that are applied to member accounts. For more information, see Suppressing Amazon Inspector findings with suppression rules (p. 22).

An Amazon Inspector delegated administrator account can perform the following tasks for member accounts:

- View and manage the status of Amazon Inspector for associated accounts, including activating and deactivating Amazon Inspector.
- Activate or deactivate scanning types for all member accounts in the organization.
- View aggregated finding data across the organization and finding details for all member accounts within the organization.
- Create and manage suppression rules that apply to findings for all accounts in the organization.
- Activate Amazon ECR enhanced scanning for all members of the organization.
- View resource coverage for the entire organization.
Designating an administrator

- Define the duration for automated re-scans of ECR container images for all member accounts in the organization. The delegated administrator’s scan duration setting overrides any setting that the member account previously set. All accounts in the organization share the ECR automated re-scan duration of the delegated administrators and different re-scan durations can’t be set for individual accounts.
- Specify five custom paths for Amazon Inspector Deep inspection for EC2 that will be used across all accounts in the organization. This is in addition to the five custom paths that a delegated administrator can set for their individual account. For more information about configuring Deep inspection custom paths see, Custom paths for Amazon Inspector Deep inspection (p. 63).
- Activate and deactivate Amazon Inspector Deep inspection for member accounts.
- Export SBOMs for any member accounts in the organization.

Member accounts within an organization can also perform the following tasks in Amazon Inspector:

- Activate Amazon Inspector for their own account.
- View resource coverage for their own account.
- View findings details for their own account.
- View the ECR container image automated re-scan duration setting for their own account.
- Specify five custom paths for Amazon Inspector Deep inspection for EC2 that will be used for their individual account. These paths are scanned in addition to any custom paths the delegated administrator has specified for the organization. For more information about configuring Deep inspection paths, see Custom paths for Amazon Inspector Deep inspection (p. 63).
- View the custom paths set by your delegated administrator for Amazon Inspector Deep inspection.
- Export SBOMs for any resources associated with their account.

**Note**
After activation, Amazon Inspector can be deactivated only by a delegated administrator account.

Designating a delegated administrator for Amazon Inspector

### Important considerations for delegated administrators

Take note of the following factors that define how the delegated administrator operates in Amazon Inspector:

**A delegated administrator can manage a maximum of 5,000 members.**

Each Amazon Inspector delegated administrator has a quota of 5,000 member accounts. However, your organization could include more than 5,000 accounts. If you exceed 5,000 member accounts, you will receive a notification through the Amazon CloudWatch Personal Health Dashboard and in an email to the delegated administrator account.

**A delegated administrator is Regional.**

Unlike AWS Organizations, Amazon Inspector is a Regional service. This means that a delegated administrator must be designated in each Region and must add and activate scans for members in each AWS Region for which you would like to manage Amazon Inspector.
An organization can have only one delegated administrator.

You can only have one delegated administrator for Amazon Inspector for an organization. If you have designated an account as a delegated administrator in one AWS Region, that account must be your delegated administrator in all other Regions.

Changing a delegated administrator does not deactivate Amazon Inspector for member accounts.

If you remove the delegated administrator, Amazon Inspector is not deactivated in those accounts, and scan settings will not be affected.

Your AWS Organization must have all features activated.

All features is the default setting for AWS Organizations. If it is not activated, see Activating all features in your organization.

Permissions required to designate a delegated administrator

You must have permission to activate Amazon Inspector and to designate an Amazon Inspector delegated administrator.

Add the following statement to the end of an IAM policy to grant these permissions.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Designating a delegated administrator for your AWS organization

The following procedure shows you how to designate a delegated administrator for your AWS organization. When this designation is complete, Amazon Inspector is activated for both the Organizations management account and the chosen delegated administrator account.

**Note**

Only the Organizations management account can designate a delegated administrator.

Activating Amazon Inspector for the first time creates the service-linked role AWSServiceRoleForAmazonInspector for the account. For more information about how Amazon Inspector uses service-linked roles, see Using service-linked roles for Amazon Inspector (p. 114). For information about service-linked roles in general, see Using service-linked roles in the IAM User Guide.

To designate a delegated administrator for Amazon Inspector
Console

Designate a delegated administrator in the console

1. Log in to the AWS Management Console using the AWS Organizations management account.
2. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home, then use the AWS Region selector in the upper right to specify the Region in which you want to designate an administrator.
3. In the **Delegated administrator** pane enter the twelve-digit account ID of the AWS account that you want to designate as the Amazon Inspector delegated administrator for your organization, and choose **Delegate administration**.
4. (Recommended) Repeat the previous steps for each AWS Region.

API

Designate a delegated administrator using the API

- Run the [EnableDelegatedAdminAccount](https://docs.aws.amazon.com/cli/latest/reference/inspector2/enable-delegated-admin-account.html) API operation using the credentials of the AWS account of the Organizations management account. You can also use the AWS Command Line to do this by running the following CLI command. Make sure to specify the account ID of the account you want to make an Amazon Inspector delegated administrator.

```bash
aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 1111111111
```

After you specify the delegated administrator, you need to use the AWS Organizations management account only to change or remove the delegated administrator account.

Activating Amazon Inspector scans for member accounts

As a delegated administrator for your organization, you can activate Amazon EC2 scanning, Amazon ECR scanning, or both, for any member associated with the AWS Organizations management account. When you activate scans for a member account, that account becomes associated to the delegated administrator, Amazon Inspector is automatically activated, and scans of the chosen type are started immediately. For information about what resources can be scanned and configuring scans, see [Scanning resources with Amazon Inspector](p. 57).

Amazon Inspector provides several options for managing and activating scans for member accounts, including allowing member accounts to activate Amazon Inspector. Use one of the following options to start scans for your member accounts.

**To automatically activate scanning for all member accounts**

1. Log in to the delegated administrator account.
2. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home, then use the AWS Region selector in the upper right to specify the Region in which you want to activate scanning for all member accounts.
3. In the navigation pane, under **Settings**, choose **Account management**. The accounts table displays all the member accounts associated with the AWS Organizations management account.
4. Select the check box at the top of the table to select all accounts on this page. Then choose **Activate** and select your preferred scan type option from the menu.

**Note**

Only the accounts currently visible on the page are selected, this means that if you have multiple pages of accounts you must repeat this process on each page. To change the number of accounts displayed on the page select the gear icon.
5. Turn on the **Automatically activate Inspector for new member accounts** setting, and select the scan types to activate for any new members who are added to your organization.

6. (Recommended) Repeat these steps in each Region in which you want to activate scans for all of your members.

The **Automatically activate Inspector for new member accounts** setting activates Amazon Inspector for all future members of your organization. This allows your Amazon Inspector delegated administrator to manage any new members that are added to the organization. When the number of member accounts reaches the limit of 5,000, this setting is automatically turned off. If an account is removed and the total number of members decreases to fewer than 5,000, the setting is automatically reactivated.

**To selectively activate member accounts**

1. Log in to the delegated administrator account.
2. Open the Amazon Inspector console at [https://console.aws.amazon.com/inspector/v2/home](https://console.aws.amazon.com/inspector/v2/home), then use the AWS Region selector in the upper right to specify the Region in which you want to activate scanning for certain member accounts.
3. In the navigation pane, under **Settings**, choose **Account management**. The accounts table displays all the member accounts associated with the AWS Organizations management account.
4. On the **Account management** page, select the check box for each member account that you want to activate scanning for.
5. Select **Activate**.
6. From the **Activate** menu, choose the scan types to activate for the selected accounts. You can choose from the following scan options:
   - **All scanning** to activate all scan types.
   - **EC2 scanning** to activate scans of Amazon EC2 instances
   - **ECR container scanning** to activate scans of Amazon ECR container images
   - **AWS Lambda standard scanning** to activate scans of Lambda functions
7. (Recommended) Repeat these steps in each Region in which you want to activate scans for certain members.

**To activate scanning as a member account**

If your AWS Organizations management account has delegated an administrator for Amazon Inspector, you can activate your own account as a member. This allows you to view scan details for your own account.

1. Log in to your account.
2. Open the Amazon Inspector console at [https://console.aws.amazon.com/inspector/v2/home](https://console.aws.amazon.com/inspector/v2/home), then use the AWS Region selector in the upper right to specify the Region in which you want to activate scanning.
3. In the navigation pane, under **Settings**, choose **Account management**.
4. On the **Account management** page, select the check box for your account.
5. From the **Activate** menu, choose the scan types to activate. You can choose from the following scan options:
   - **All scanning** to activate all scan types.
   - **EC2 scanning** to activate scans of Amazon EC2 instances
   - **ECR container scanning** to activate scans of Amazon ECR container images
   - **AWS Lambda standard scanning** to activate scans of Lambda functions
6. (Recommended) Repeat these steps in each Region in which you want to activate scans.
Disassociating member accounts in Amazon Inspector

The following procedure shows how to disassociate member accounts. Disassociated member accounts remain in your AWS Organizations organization as standalone Amazon Inspector accounts, but the Amazon Inspector delegated administrator no longer has permission to activate and manage Amazon Inspector for these accounts. You can add these accounts as members again later.

**Note**
Disassociating an account does not deactivate Amazon Inspector scans for that account.

**To disassociate member accounts**

1. Log in to the delegated administrator account.
2. Open the Amazon Inspector console at [https://console.aws.amazon.com/inspector/v2/home](https://console.aws.amazon.com/inspector/v2/home), then use the AWS Region selector in the upper right to specify the Region in which you want to disassociate one or more member accounts.
3. In the navigation pane, under **Settings**, choose **Account management**.
4. On the **Account management** page, select the check box for each account that you want to disassociate.
5. From the **Actions** menu, choose **Disassociate account**.
6. (Recommended) Repeat these steps in each Region to ensure that the member account is disassociated in all Regions.

Removing an Amazon Inspector delegated administrator

In the event that you need to assign a new Amazon Inspector delegated administrator, you can remove an existing delegated administrator as the AWS Organizations management account.

When you remove a delegated administrator, it does not deactivate Amazon Inspector in that account or in any organization member accounts. Accounts within your organization are converted to standalone accounts and retain the scan settings they had prior to being managed by a delegated administrator.

**To remove the delegated administrator**

1. Log in to the AWS Management Console using the AWS Organizations management account.
2. Open the Amazon Inspector console at [https://console.aws.amazon.com/inspector/v2/home](https://console.aws.amazon.com/inspector/v2/home), then use the AWS Region selector in the upper right to specify the Region in which you want to remove the delegated administrator.
3. In the navigation pane, under **Settings**, choose **Account management**.
4. In the **Delegated administrator** section, choose **Remove**, and then confirm your action.
5. Repeat these steps in each Region in which you registered this delegated administrator.

**To associate members with a new delegated administrator**

When you add a new Amazon Inspector delegated administrator, you need to manually associate organization members to the new administrator account.

1. Log in to the AWS Management Console using the delegated administrator account.
2. Open the Amazon Inspector console at [https://console.aws.amazon.com/inspector/v2/home](https://console.aws.amazon.com/inspector/v2/home), then use the AWS Region selector in the upper right to specify the Region in which you want to associate members with the new delegated administrator.
3. In the navigation pane, under Settings, choose Account management.
4. Select all of the listed accounts in your organization by using the top check box.
5. From the Actions menu, choose Add member.
6. Repeat these steps in each Region in which you want to associate members with the new delegated administrator.
Monitoring Usage and Cost in Amazon Inspector

You can use the Amazon Inspector console and API operations to project monthly costs of using Amazon Inspector in your environment. If you are the Amazon Inspector administrator for a multiple-account environment, you can view the total cost for your entire environment and cost metrics for each of your member accounts.

Using the usage console

You can assess usage and projected cost for Amazon Inspector from the console.

To access usage statistics

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. By using the AWS Region selector in the upper-right corner of the page, select the Region you want to monitor costs in.
3. In the navigation pane, choose Usage.

In the By account tab you will see the projected total cost based on the 30 day period listed under Account usage. In the table under the Projected cost column select a value to see a breakdown of usage by scan type for that account. In this detail pane you can also see which scan types have a free trial active for that account.

If you are the delegated administrator for an organization you will see a row in the table for each account within your organization. If an account in your organization is disassociated the console shows it's projected cost as a -.

In the By scan type tab you can see a break down of actual usage so far in the current 30 day period by scan type. This is the information used to calculate the projected costs in the By account tab.

If you are the delegated administrator for an organization you can see the usage for each account in your organization.

In this tab, you can expand any of the following panes for usage statistics:

Amazon EC2 scanning

Instances (Avg) — Amazon Inspector uses the coverage hours to calculate the average number of resources for EC2 instance scanning. The average is the total coverage hours divided by 720 hours (the number of hours in a 30 day period).

Coverage hours — for Amazon EC2 scanning this is the sum total number of hours within the last 30 days that Amazon Amazon Inspector provided active coverage for each EC2 instance in an account. For EC2 instances, coverage hours are the hours from when Amazon Inspector discovered the instance until it's terminated or stopped, or excluded from scans by tags. (when you restart a stopped instance or remove an exclusion tag, Amazon Inspector resumes coverage and coverage hours for that instance will continue to accrue).
Amazon ECR scanning

Initial scans — The sum total of first time scans of images in the account within the last 30 days.

Rescans — The sum total of rescans for images in the account within the last 30 days. A rescan is any scan done on an ECR image that Amazon Inspector has previously scanned. If you have configured your ECR repository for continuous scanning, rescans occur automatically when Amazon Inspector adds a new Common Vulnerabilities and Exposures (CVE) to it's database.

Lambda scanning

Instances (Avg) — Amazon Inspector uses the coverage hours to calculate the average number of functions for Lambda function scanning. Average is the total coverage hours divided by 720 hours (the number of hours in a 30 day period).

Coverage hours — For Lambda function scanning this is the sum total number of hours within the last 30 days that Amazon Amazon Inspector provided active coverage for each Lambda function in an account. For AWS Lambda functions the coverage hours are calculated from when Amazon Inspector discovers a function until when it's deleted or excluded from scans. If an excluded function is included again, coverage hours for that function will continue to accrue.

Understanding how Amazon Inspector calculates usage costs

The costs provided by Amazon Inspector are estimates, not actual costs, so they may differ from those in your AWS Billing console.

Note the following about how Amazon Inspector calculates cost on the Usage page:

• The usage cost reflects the current region only. Prices per scan type vary by AWS Region, to review exact prices per region, see the Pricing for Amazon Inspector
• All usage projections are rounded to the nearest US dollar.
• Discounts aren't included in the projected costs.
• The projected cost represent the total cost for the 30 day usage period per scan type. If there has been less than 30 days of usage for an account, Amazon Inspector projects the cost after 30 days as if any currently covered resources will remain covered for the rest of the 30 day period.
• The cost per scan type is calculated based on the following:
  • EC2 scanning: cost reflects the average number of EC2 instances covered by Amazon Inspector in the last 30 days.
  • ECR container scanning: cost reflects the sum of the number of initial image scans + image rescans in the last 30 days.
  • Lambda standard scanning: cost reflects the average number of Lambda functions covered by Amazon Inspector in the last 30 days.
  • Lambda code scanning: cost reflects the average number of Lambda functions covered by Amazon Inspector in the last 30 days.

About the Amazon Inspector free trial

When you Activate an Amazon Inspector scan type you are automatically enrolled in a 15 day free trial for that scan type. Each scan type has an independent free trial, this includes: EC2 scanning, ECR scanning, Lambda standard scanning, and Lambda code scanning.
If you deactivate a scan type during the free trial the free trial will paused for that scan type. If you reactivate that service the free trial will resume and you will get the remaining days of that free trial.
Security in Amazon Inspector

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, 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. The following topics show you how to configure Amazon Inspector 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 resources.

**Topics**
- [Data protection in Amazon Inspector](#) (p. 92)
- [Identity and Access Management for Amazon Inspector](#) (p. 96)
- [Monitoring Amazon Inspector](#) (p. 120)
- [Compliance validation for Amazon Inspector](#) (p. 122)
- [Resilience in Amazon Inspector](#) (p. 122)
- [Infrastructure security in Amazon Inspector](#) (p. 122)
- [Incident response in Amazon Inspector](#) (p. 123)

Data protection in Amazon Inspector

The AWS shared responsibility model applies to data protection in Amazon Inspector. 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. This content includes 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.
• 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 140-2 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) 140-2.

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 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 at rest (p. 93)
• Encryption in transit (p. 95)

Encryption at rest

Amazon Inspector securely stores your data at rest using AWS encryption solutions by default. Amazon
Inspector encrypts data, such as resource inventory collected using AWS Systems Manager, resource
inventory parsed from Amazon ECR images, and generated security findings, using AWS owned
encryption keys from AWS Key Management Service (AWS KMS). You can't view, manage, or use AWS
owned keys, or audit their use. However, you don't have to take any action or change any programs to
protect the keys that encrypt your data. For more information see AWS owned keys.

If you disable Amazon Inspector, it permanently deletes all resources that it stores or maintains for you,
such as collected inventory and security findings.

Encryption at rest for code in your findings

For Amazon Inspector Lambda code scanning, Amazon Inspector partners with CodeGuru to scan your
code for vulnerabilities. When a vulnerability is detected CodeGuru extracts a snippet of your code
containing the vulnerability and stores that code until Amazon Inspector requests access. By default
CodeGuru uses an AWS owned key to encrypt the extracted code, however, you can configure Amazon
Inspector to use your own customer managed AWS KMS key for encryption.

The following work flow explains how Amazon Inspector uses the key you configure to encrypt your
code:

1. You supply a AWS KMS key to Amazon Inspector using the Amazon Inspector UpdateEncryptionKey
   API.
2. Amazon Inspector forwards the information about your AWS KMS key to CodeGuru. CodeGuru stores
   the information for future use.
3. CodeGuru requests a grant from AWS KMS for the key you configured in Amazon Inspector.
4. CodeGuru creates an encrypted data key from your AWS KMS key and stores it. This data key is used to
   encrypt your code data stored by CodeGuru.
5. Whenever Amazon Inspector requests data from code scans CodeGuru uses the grant to decrypt the
   encrypted data key, then uses that key to decrypt the data so it can be retrieved.

When you disable Lambda code scanning CodeGuru retires the grant and deletes the associated data key.
Permissions for code encryption with a customer managed key

To use encryption you need to have a policy that allows access to AWS KMS actions, as well as a statement that grants Amazon Inspector and CodeGuru permissions to use those actions through condition keys.

If you are setting, updating, or resetting the encryption key for your account you will need to use an Amazon Inspector administrator policy, such as AWS managed policy: AmazonInspector2FullAccess (p. 108). You will also need to grant the following permissions to read-only users who need to retrieve code snippets from findings or data about the key chosen for encryption.

For KMS, the policy must allow you to perform the following actions:

- kms:CreateGrant
- kms:Decrypt
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlainText
- kms:Encrypt
- kms:RetireGrant

Once you’ve verified that you have the correct AWS KMS permissions in your policy, you must attach a statement that allows Amazon Inspector and CodeGuru to use your key for encryption. Attach the following policy statement:

**Note**
Replace Region with the AWS Region you have Amazon Inspector Lambda code scanning enabled in.

```json
{
    "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
                "GenerateDataKey",
                "GenerateDataKeyWithoutPlaintext",
                "Encrypt",
                "Decrypt",
                "RetireGrant",
                "DescribeKey"
            ]
        },
        "StringEquals": {
            "kms:ViaService": [
                "codeguru-security.Region.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:RetireGrant",
```
Encryption in transit

AWS encrypts all data in transit between AWS internal systems and other AWS services.

For inventory collection, Systems Manager gathers telemetry data from customer-owned EC2 instances that it sends back to AWS over a Transport Layer Security (TLS)-protected channel for assessment. See Data Protection in Systems Manager to understand how SSM encrypts data in transit.
Likewise, Amazon ECR and AWS Lambda function scan findings that are sent to Security Hub are encrypted using a TLS-protected channel.

Identity and Access Management for Amazon Inspector

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 (p. 96)
- Authenticating with identities (p. 96)
- Managing access using policies (p. 99)
- How Amazon Inspector works with IAM (p. 100)
- Identity-based policy examples for Amazon Inspector (p. 105)
- AWS managed policies for Amazon Inspector (p. 108)
- Using service-linked roles for Amazon Inspector (p. 114)
- Troubleshooting Amazon Inspector identity and access (p. 119)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon Inspector.

Service user – If you use the Amazon Inspector service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Inspector features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Inspector, see Troubleshooting Amazon Inspector identity and access (p. 119).

Service administrator – If you're in charge of Amazon Inspector resources at your company, you probably have full access to Amazon Inspector. It's your job to determine which Amazon Inspector features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Inspector, see How Amazon Inspector works with IAM (p. 100).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Inspector. To view example Amazon Inspector identity-based policies that you can use in IAM, see Identity-based policy examples for Amazon Inspector (p. 105).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.
You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the AWS Sign-In User Guide.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the IAM User Guide.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the AWS IAM Identity Center User Guide and Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

### AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the IAM User Guide.

### Federated identity

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

A federated identity is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see What is IAM Identity Center? in the AWS IAM Identity Center User Guide.

### IAM users and groups

An IAM user is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the IAM User Guide.

An IAM group is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to
manage for large sets of users. For example, you could have a group named IAMAdmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the IAM User Guide.

IAM roles

An IAM role is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the IAM User Guide. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the AWS IAM Identity Center User Guide.

- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.

- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.

- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.

- **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, resources, and condition keys for Amazon Inspector in the Service Authorization Reference.

- **Service role** – 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 Creating a role to delegate permissions to an AWS service in the IAM User Guide.

- **Service-linked role** – 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.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the IAM User Guide.
To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) 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 is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see *Overview of JSON policies* in the *IAM User Guide*.

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

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

### Identity-based policies

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 *Creating IAM policies* in the *IAM User Guide*.

Identity-based policies can be further categorized as **inline policies** or **managed policies**. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see *Choosing 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 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.

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.

### Access control lists (ACLs)

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.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see *Access control list (ACL) overview* in the *Amazon Simple Storage Service Developer Guide*.
Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity’s identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the IAM User Guide.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session’s permissions are the intersection of the user or role’s identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. 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 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

<table>
<thead>
<tr>
<th>IAM feature</th>
<th>Amazon Inspector support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity-based policies (p. 101)</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource-based policies (p. 101)</td>
<td>No</td>
</tr>
<tr>
<td>Policy actions (p. 102)</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy resources (p. 102)</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy condition keys (service-specific) (p. 103)</td>
<td>Yes</td>
</tr>
<tr>
<td>ACLs (p. 103)</td>
<td>No</td>
</tr>
<tr>
<td>ABAC (tags in policies) (p. 103)</td>
<td>Partial</td>
</tr>
</tbody>
</table>
### How Amazon Inspector works with IAM

<table>
<thead>
<tr>
<th>IAM feature</th>
<th>Amazon Inspector support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary credentials (p. 104)</td>
<td>Yes</td>
</tr>
<tr>
<td>Principal permissions (p. 104)</td>
<td>Yes</td>
</tr>
<tr>
<td>Service roles (p. 104)</td>
<td>No</td>
</tr>
<tr>
<td>Service-linked roles (p. 105)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Supports identity-based policies</th>
<th>Yes</th>
</tr>
</thead>
</table>

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 [Creating IAM 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. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. 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](p. 105).

#### Resource-based policies within Amazon Inspector

<table>
<thead>
<tr>
<th>Supports resource-based policies</th>
<th>No</th>
</tr>
</thead>
</table>

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. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see [How IAM roles differ from resource-based policies](#) 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. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as permission-only actions that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called dependent actions.

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 in the Service Authorization Reference.

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

```
inspector2
```

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

```
"Action": [
  "inspector2:action1",
  "inspector2:action2"
]
```

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector (p. 105).

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. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as resource-level permissions.

For actions that don't support resource-level permissions, such as listing operations, 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 in the Service Authorization Reference. To learn with which actions you can specify the ARN of each resource, see Actions defined by Amazon Inspector.

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector (p. 105).

**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 (or Condition block) lets you specify conditions in which a statement is in effect. The Condition element is optional. 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.

If you specify multiple Condition elements in a statement, or multiple keys in a single Condition element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the IAM User Guide.

AWS supports global condition keys and service-specific condition keys. 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 in the Service Authorization Reference. To learn with which actions and resources you can use a condition key, see Actions defined by Amazon Inspector.

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector (p. 105).

**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. In AWS, these attributes are called tags. You can attach tags to IAM entities (users or roles).
and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

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 What is ABAC? 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

<table>
<thead>
<tr>
<th>Supports temporary credentials</th>
<th>Yes</th>
</tr>
</thead>
</table>

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the IAM User Guide.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switching to a role (console) in the IAM User Guide.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Cross-service principal permissions for Amazon Inspector

<table>
<thead>
<tr>
<th>Supports principal permissions</th>
<th>Yes</th>
</tr>
</thead>
</table>

When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, resources, and condition keys for Amazon Inspector in the Service Authorization Reference.

Service roles for Amazon Inspector

<table>
<thead>
<tr>
<th>Supports service roles</th>
<th>No</th>
</tr>
</thead>
</table>

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 Creating 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 service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a Yes in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon Inspector

By default, users and roles don’t have permission to create or modify Amazon Inspector resources. They also can’t perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Creating IAM policies 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 in the Service Authorization Reference.

Topics
- Policy best practices (p. 105)
- Using the Amazon Inspector console (p. 106)
- Allow users to view their own permissions (p. 106)
- **Allow read-only access to all Amazon Inspector resources** (p. 107)
- Allow full access to all Amazon Inspector resources (p. 107)

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 AWS 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 IAM Access Analyzer policy validation 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 Configuring MFA-protected API access 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 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.

```json
{
  "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}"
    }
  ]
}
```
Identity-based policy examples

{  
  "Sid": "NavigateInConsole",
  "Effect": "Allow",
  "Action": [
    "iam:GetGroupPolicy",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:ListAttachedGroupPolicies",
    "iam:ListGroupPolicies",
    "iam:ListPolicyVersions",
    "iam:ListPolicies",
    "iam:ListUsers"
  ],
  "Resource": "*"
}

Allow read-only access to all Amazon Inspector resources

This example shows a policy that allows read-only access to all Amazon Inspector resources.

{  
  "Version": "2012-10-17",
  "Statement": [
    {  
      "Effect": "Allow",
      "Action": [
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:BatchGet*",
        "inspector2:List*"
      ],
      "Resource": "*"
    },
    {  
      "Effect": "Allow",
      "Action": ["organizations:ListDelegatedAdministrators", "organizations:ListAWSServiceAccessForOrganization", "organizations:DescribeOrganizationalUnit", "organizations:DescribeAccount", "organizations:DescribeOrganization"],
      "Resource": "*"
    }
  ]
}

Allow full access to all Amazon Inspector resources

This example shows a policy that allows full access to all Amazon Inspector resources.

{  
  "Version": "2012-10-17",
  "Statement": [
    {  
      "Effect": "Allow",
      "Action": "inspector2:*",
      "Resource": "*"
    },
    {  
      "Effect": "Allow",
      "Action": ["organizations:ListDelegatedAdministrators", "organizations:ListAWSServiceAccessForOrganization", "organizations:DescribeOrganizationalUnit", "organizations:DescribeAccount", "organizations:DescribeOrganization"],
      "Resource": "*"
    }
  ]
}
AWS managed policies for Amazon Inspector

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the IAM User Guide.

AWS managed policy: AmazonInspector2FullAccess

You can attach the AmazonInspector2FullAccess policy to your IAM identities.

This policy grants administrative permissions that allow full access to Amazon Inspector.

Permissions details
This policy includes the following permissions.

- **inspector2** – Allows full access to Amazon Inspector functionality.
- **iam** – Allows Amazon Inspector to create the service-linked role, AWSServiceRoleForAmazonInspector2. This is required so that Amazon Inspector can perform operations such as retrieve information about your Amazon EC2 instances and Amazon ECR repositories and container images, analyze your VPC network, and describe accounts associated with your organization. For more information, see [Using service-linked roles for Amazon Inspector](p. 114).
- **organizations** – Allows administrators to use Amazon Inspector for an organization in AWS Organizations. After activating trusted access for Amazon Inspector in AWS Organizations, members of the delegated administrator account can manage settings and view findings across their organization.
- **codeguru-security** – Allows administrators to use Amazon Inspector to retrieve information code snippets and change encryption settings for code stored by CodeGuru Security. For more information, see [Encryption at rest for code in your findings](p. 93).

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "codeguru-security:BatchGetFindings",
                "codeguru-security:GetAccountConfiguration",
                "codeguru-security:UpdateAccountConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```
AWS managed policy: AmazonInspector2ReadOnlyAccess

You can attach the AmazonInspector2ReadOnlyAccess policy to your IAM identities.

This policy grants permissions that allow read-only access to Amazon Inspector.

Permissions details

This policy includes the following permissions.

- inspector2 – Allows read-only access to Amazon Inspector functionality.
- organizations – Allows details about Amazon Inspector coverage for an organization in AWS Organizations to be viewed.
- codeguru-security – Allows code snippets to be retrieved from CodeGuru Security. Also allows encryption settings for your code stored in CodeGuru Security to be viewed.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource": "*
    }
  ]
}
```

AWS managed policy: AmazonInspector2ServiceRolePolicy

You can't attach the AmazonInspector2ServiceRolePolicy policy to your IAM entities. This policy is attached to a service-linked role that allows Amazon Inspector to perform actions on your behalf. For more information, see Using service-linked roles for Amazon Inspector (p. 114).

Amazon Inspector updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Inspector since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Inspector Document history (p. 141) page.
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AmazonInspector2ReadOnlyAccess (p. 110)</td>
<td>Amazon Inspector has added new permissions that allow read-only users to retrieve vulnerability intelligence details for package vulnerability findings.</td>
<td>September 22, 2023</td>
</tr>
<tr>
<td>AmazonInspector2ServiceRolePolicy (p. 114)</td>
<td>Amazon Inspector has added new permissions that allow Amazon Inspector to scan network configurations of Amazon EC2 instances that are part of Elastic Load Balancing target groups.</td>
<td>August 31, 2023</td>
</tr>
<tr>
<td>AmazonInspector2ReadOnlyAccess (p. 110)</td>
<td>Amazon Inspector has added new permissions that allow read-only users to export Software Bill of Materials (SBOM) for their resources.</td>
<td>June 29, 2023</td>
</tr>
<tr>
<td>AmazonInspector2ReadOnlyAccess (p. 110)</td>
<td>Amazon Inspector has added new permissions that allow read-only users to retrieve details of encryption settings for Lambda code scanning findings for their account.</td>
<td>June 13, 2023</td>
</tr>
<tr>
<td>AmazonInspector2FullAccess (p. 108)</td>
<td>Amazon Inspector has added new permissions that allow users to configure a customer managed KMS key to encrypt code in findings from Lambda code scanning.</td>
<td>June 13, 2023</td>
</tr>
<tr>
<td>AmazonInspector2ReadOnlyAccess (p. 110)</td>
<td>Amazon Inspector has added new permissions that allow read-only users to retrieve details of Lambda code scanning status and findings for their account.</td>
<td>May 02, 2023</td>
</tr>
<tr>
<td>AmazonInspector2ServiceRolePolicy (p. 114)</td>
<td>Amazon Inspector has added new permissions that allow Amazon Inspector to create AWS CloudTrail service-linked channels in your account when you activate Lambda scanning. This allows Amazon Inspector to monitor CloudTrail events in your account.</td>
<td>April 30, 2023</td>
</tr>
<tr>
<td>AmazonInspector2FullAccess (p. 108)</td>
<td>Amazon Inspector has added new permissions that allow users to retrieve details of code</td>
<td>April 21, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>AmazonInspector2ServiceRolePolicy</strong></td>
<td><strong>Amazon Inspector</strong> has added new permissions that allow Amazon Inspector to send information to Amazon EC2 Systems Manager about the custom paths a customer has defined for Amazon EC2 Deep inspection.</td>
<td>April 17, 2023</td>
</tr>
<tr>
<td><strong>AmazonInspector2ServiceRolePolicy</strong></td>
<td><strong>Amazon Inspector</strong> has added new permissions that allow Amazon Inspector to create AWS CloudTrail service-linked channels in your account when you activate Lambda scanning. This allows Amazon Inspector to monitor CloudTrail events in your account.</td>
<td>April 30, 2023</td>
</tr>
<tr>
<td><strong>AmazonInspector2ServiceRolePolicy</strong></td>
<td><strong>Amazon Inspector</strong> has added new permissions that allow Amazon Inspector to request scans of the developer code in AWS Lambda functions, and receive scan data from Amazon CodeGuru Security. Additionally, Amazon Inspector has added permissions to review IAM policies. Amazon Inspector uses this information to scan Lambda functions for code vulnerabilities.</td>
<td>February 28, 2023</td>
</tr>
<tr>
<td><strong>AmazonInspector2ServiceRolePolicy</strong></td>
<td><strong>Amazon Inspector</strong> has added a new statement that allows Amazon Inspector to retrieve information from CloudWatch about when an AWS Lambda function was last invoked. Amazon Inspector uses this information to focus scans on the Lambda functions in your environment that have been active in the last 90 days.</td>
<td>February 20, 2023</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>AmazonInspector2ServiceRolePolicy (p. 114)</strong></td>
<td>Updates to an existing policy</td>
<td>November 28, 2022</td>
</tr>
<tr>
<td><strong>AmazonInspector2FullAccess (p. 108)</strong></td>
<td>New policy</td>
<td>November 29, 2021</td>
</tr>
<tr>
<td><strong>AmazonInspector2ReadOnlyAccess</strong></td>
<td>New policy</td>
<td>January 21, 2022</td>
</tr>
<tr>
<td>Amazon Inspector started tracking changes</td>
<td>Amazon Inspector started tracking changes for its AWS managed policies.</td>
<td>November 29, 2021</td>
</tr>
<tr>
<td>Amazon Inspector added a new action to allow Amazon Inspector to describe SSM association executions. Additionally, Amazon Inspector has added additional resource scoping to allow Amazon Inspector to create, update, delete, and start SSM associations with AmazonInspector2 owned SSM documents.</td>
<td>August 31, 2022</td>
<td></td>
</tr>
<tr>
<td>Amazon Inspector has updated the resource scoping of the policy to allow Amazon Inspector to collect software inventory in other AWS partitions.</td>
<td>August 12, 2022</td>
<td></td>
</tr>
<tr>
<td>Amazon Inspector has restructured the resource scoping of the actions allowing Amazon Inspector to create, delete, and update SSM associations.</td>
<td>August 10, 2022</td>
<td></td>
</tr>
<tr>
<td>Amazon Inspector added a new statement that allows Amazon Inspector to retrieve information about AWS Lambda functions, including each layer version that is associated with each function. Amazon Inspector uses this information to scan Lambda functions for security vulnerabilities.</td>
<td>November 28, 2022</td>
<td></td>
</tr>
<tr>
<td>Amazon Inspector has updated the resource scoping of the policy to allow Amazon Inspector to perform actions in other services on your behalf.</td>
<td>November 29, 2021</td>
<td></td>
</tr>
</tbody>
</table>
Using service-linked roles for Amazon Inspector

Amazon Inspector uses an AWS Identity and Access Management (IAM) service-linked role named AWSServiceRoleForAmazonInspector2. This service-linked role is an IAM role that is linked directly to Amazon Inspector. It is predefined by Amazon Inspector and it includes all the permissions that Amazon Inspector requires to call other AWS services on your behalf.

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

You must configure permissions to allow an IAM entity (such as a 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. You can delete a service-linked role only after deleting its related resources. This protects your Amazon Inspector 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 review the service-linked role documentation for that service.

Service-linked role permissions for Amazon Inspector

Amazon Inspector uses the service-linked role named AWSServiceRoleForAmazonInspector2. This service-linked role trusts the inspector2.amazonaws.com service to assume the role.

The permissions policy for the role, which is named AmazonInspector2ServiceRolePolicy, allows Amazon Inspector to perform tasks such as:

- Use Amazon Elastic Compute Cloud (Amazon EC2) actions to retrieve information about your instances and network paths.
- Use AWS Systems Manager actions to retrieve inventory from your Amazon EC2 instances, and to retrieve information about third-party packages from custom paths.
- Use Amazon Elastic Container Registry actions to retrieve information about your container images.
- Use AWS Lambda actions to retrieve information about your Lambda functions.
- Use AWS Organizations actions to describe associated accounts.
- Use CloudWatch actions to retrieve information about the last time your Lambda functions were invoked.
- Use select IAM actions to retrieve information about your IAM policies that could create security vulnerabilities in your Lambda code.
- Use CodeGuru Security actions to perform scans of the code in your Lambda functions. Amazon Inspector uses the following CodeGuru Security actions:
  - codeguru-security:CreateScan – Grants permission to create CodeGuru Security scan.
  - codeguru-security:GetScan – Grants permission to retrieve CodeGuru Security scan metadata.
  - codeguru-security:DeleteScansByCategory – Grants permission for CodeGuru Security to delete scans initiated by Amazon Inspector.
- Use select Elastic Load Balancing actions to perform network scans of EC2 instances that are part of Elastic Load Balancing target groups.
The role is configured with the following permissions policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TirosPolicy",
      "Effect": "Allow",
      "Action": [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource": ["*"]
    }
  ]
}
```
Amazon Inspector User Guide
Using service-linked roles

},
{
  "Sid": "PackageVulnerabilityScanning",
  "Effect": "Allow",
  "Action": [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
    "ecr:DescribeRegistry",
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
  ],
  "Resource": "*"
},
{
  "Sid": "LambdaPackageVulnerabilityScanning",
  "Effect": "Allow",
  "Action": [
    "lambda:ListFunctions",
    "lambda:GetFunction",
    "lambda:GetLayerVersion",
    "cloudwatch:GetMetricData"
  ],
  "Resource": "*"
},
{
  "Sid": "GatherInventory",
  "Effect": "Allow",
  "Action": [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "ssm:DeleteAssociation",
    "ssm:UpdateAssociation"
  ],
  "Resource": [
    "arn:*:ec2:*:*:instance/*",
    "arn:*:ssm:*:*:document/AmazonInspector2-*",
    "arn:*:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:*:ssm:*:*:managed-instance/",
    "arn:*:ssm:*:*:association/"
  ]
},
{
  "Sid": "DataSyncCleanup",
  "Effect": "Allow",
  "Action": [
    "ssm:CreateResourceDataSync",
    "ssm:DeleteResourceDataSync"
  ],
  "Resource": [
    "arn:*:ssm:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
  ]
}
"Sid": "ManagedRules",
"Effect": "Allow",
"Action": [
  "events:PutRule",
  "events:DeleteRule",
  "events:DescribeRule",
  "events:ListTargetsByRule",
  "events:PutTargets",
  "events:RemoveTargets"
],
"Resource": [
  "arn:*:events::*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
],

"Sid": "LambdaCodeVulnerabilityScanning",
"Effect": "Allow",
"Action": [
  "codeguru-security:CreateScan",
  "codeguru-security:GetAccountConfiguration",
  "codeguru-security:GetFindings",
  "codeguru-security:GetScan",
  "codeguru-security:ListFindings",
  "codeguru-security:BatchGetFindings",
  "codeguru-security:DeleteScansByCategory"
],
"Resource": [
  "*
]
},

"Sid": "CodeGuruCodeVulnerabilityScanning",
"Effect": "Allow",
"Action": [
  "iam:GetRole",
  "iam:GetRolePolicy",
  "iam:GetPolicy",
  "iam:GetPolicyVersion",
  "iam:ListAttachedRolePolicies",
  "iam:ListPolicies",
  "iam:ListPolicyVersions",
  "iam:ListRolePolicies",
  "lambda:listVersionsByFunction"
],
"Resource": [
  "*
]
},

"Condition": {
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": [
      "codeguru-security.amazonaws.com"
    ]
  }
},

"Sid": "Ec2DeepInspection",
"Effect": "Allow",
"Action": [
  "ssm:PutParameter",
  "ssm:GetParameters",
  "ssm:DeleteParameter"
],
"Resource": [
  "arn:*:ssm::*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
]}
Creating a service-linked role for Amazon Inspector

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

Editing a service-linked role for Amazon Inspector

Amazon Inspector does not allow you to edit the AWSServiceRoleForAmazonInspector2 service-linked role. After a service-linked role is created, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role by using IAM. For more information, see Editing a service-linked role in the IAM User Guide.

Deleting a service-linked role for Amazon Inspector

If you no longer need to use Amazon Inspector, we recommend that you delete the AWSServiceRoleForAmazonInspector2 service-linked role. Before you can delete the role, you must deactivate Amazon Inspector in each AWS Region where it's activated. When you deactivate Amazon Inspector, it doesn't delete the role for you. Therefore, if you activate Amazon Inspector again, it can use the existing role. That way you can avoid having 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.

If you delete this service-linked role and then need to create it again, you can use the same process to re-create the role in your account. When you activate Amazon Inspector, Amazon Inspector re-creates the service-linked role for you.

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

You can use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonInspector2 service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.

**Troubleshooting Amazon Inspector 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 (p. 119)
- I am not authorized to perform iam:PassRole (p. 119)
- I want to allow people outside of my AWS account to access my Amazon Inspector resources (p. 120)

**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 inspector2:GetWidget permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: inspector2: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 inspector2: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.
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 works with IAM (p. 100).
- 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 How IAM roles differ from resource-based policies in the IAM User Guide.

Monitoring Amazon Inspector

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Inspector and your other AWS solutions. AWS provides monitoring tools to watch Amazon Inspector, report when something is wrong, and take automatic actions when appropriate:

- Amazon EventBridge is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services and routes that data to targets such as Lambda. This allows you to monitor events that happen in services, and build event-driven architectures. For more information, see the Amazon EventBridge User Guide.
- AWS CloudTrail captures API calls and related events made by or on behalf of your AWS account. CloudTrail then delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Logging Amazon Inspector API calls using AWS CloudTrail

Amazon Inspector is integrated with AWS CloudTrail, a service that provides a record of actions taken by an IAM user or role, or an AWS service, in Amazon Inspector. CloudTrail captures all API calls for Amazon Inspector as events. The calls captured include calls from the Amazon Inspector console and calls to the Amazon Inspector API operations. If you create a trail, you can enable continuous delivery of CloudTrail logs.
CloudTrail logs

Events to an Amazon S3 bucket, including events for Amazon Inspector. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine:

- The request that was made to Amazon Inspector.
- The IP address from which the request was made.
- Who made the request.
- When the request was made.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Amazon Inspector information in CloudTrail

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

For an ongoing record of events in your AWS account, including events for Amazon Inspector, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in 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 topics:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple accounts
- Receiving CloudTrail log files from multiple regions

All Amazon Inspector actions are logged by CloudTrail. All actions that Amazon Inspector can make are documented in the Amazon Inspector API Reference. For example, calls to the CreateFindingsReport, ListCoverage, and UpdateOrganizationConfiguration actions generate entries in the CloudTrail log files.

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

For more information, see the CloudTrail userIdentity element.

Understanding Amazon Inspector log file entries

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

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. 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 AWS services 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 baseline environments on AWS that are security and compliance focused.
- **Architecting for HIPAA Security and Compliance on Amazon Web Services** – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

  **Note**
  Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.

- **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** – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- **AWS Audit Manager** – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in Amazon Inspector

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.

Infrastructure security in Amazon Inspector

As a managed service, Amazon Inspector 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 through the network. Clients must support the following:
Incident response

• 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.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Incident response in Amazon Inspector

Incident response for Amazon Inspector 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.
Amazon Inspector integrations

Amazon Inspector integrates with other AWS services. These services can ingest data from Amazon Inspector to allow you to view your findings in new ways. Review the following integration options to learn more about how that service is set up to work with Amazon Inspector.

Integrating Amazon Inspector with Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) is a fully-managed Docker container registry that makes it easy to store, share, and deploy container images. Amazon ECR private registries host your container images in a highly-available and scalable architecture. You can use Amazon Inspector to scan container images residing in your Amazon ECR repositories for vulnerable operating system packages and programming language packages.

For more information about using Amazon ECR with Amazon Inspector, see Amazon Inspector integration with Amazon Elastic Container Registry (Amazon ECR) (p. 124).

Amazon Inspector integration with AWS Security Hub

AWS Security Hub collects security data from across your AWS accounts, services, and other supported products to assess the security state of your environment according to industry standards and best practices. In addition to evaluating your security posture, Security Hub creates a central location for findings across all your integrated AWS services, and AWS Partner Network products. Activating Security Hub with Amazon Inspector automatically allows Security Hub to ingest Amazon Inspector findings data.

For more information about using Security Hub with Amazon Inspector see Amazon Inspector integration with AWS Security Hub (p. 125).

Amazon Inspector integration with Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR is a fully managed container registry that supports Docker and OCI images and artifacts on AWS. If you are using Amazon ECR, you can activate Enhanced scanning for your registry to allow Amazon Inspector to automatically detect your container images and scan them for vulnerable operating system packages and programming language packages.

This integration allows you to view Amazon Inspector findings for container images within the Amazon ECR console. Additionally, from the Amazon ECR console you can manage scan frequency and refine the scope of scans by creating inclusion filters.

Activating the integration

You can activate the integration by activating Amazon Inspector scanning through the Amazon Inspector console or API, or by configuring your repository to use Enhanced scanning with Amazon Inspector through the Amazon ECR console or API.
Using the integration with a multi-account environment

If you are a member in a multi-account environment, you can activate enhanced scanning through Amazon ECR. However, once activated, it can only be deactivated by your Amazon Inspector delegated administrator. If it is deactivated, it reverts to basic scanning. For more information, see Deactivating Amazon Inspector (p. 137).

Amazon Inspector integration with AWS Security Hub

Security Hub provides a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. Security Hub collects security data from across AWS accounts, services, and additional supported products. You can use the information it provides to analyze your security trends and identify the highest priority security issues.

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

In AWS Security Hub, security issues are tracked as findings. Some findings result from issues that are detected by other AWS services or by third-party products. Security Hub also has a set of rules that it uses to detect security issues and generate findings. Security Hub provides tools to manage findings from across all of these sources. You can view and filter lists of findings and view finding details. For more information about findings in Security Hub, 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 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.

Security Hub will archive Amazon Inspector findings once those findings have been addressed and closed in Amazon Inspector.

Viewing Amazon Inspector findings in AWS Security Hub

The findings from Amazon Inspector Classic and the new Amazon Inspector are available in the same panel in Security Hub. However, you can filter findings from the new Amazon Inspector by adding a "aws/inspector/ProductVersion": "2" to the filter bar. Adding this filter excludes findings from Amazon Inspector Classic from the Security Hub dashboard.

Example finding from Amazon Inspector

```json
{
    "SchemaVersion": "2018-10-08",
```
Viewing Amazon Inspector findings in AWS Security Hub

```
"Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
"ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
"ProductName": "Inspector",
"CompanyName": "Amazon",
"Region": "us-east-1",
"GeneratorId": "AWSInspector",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Vulnerabilities/CVE"
],
"FirstObservedAt": "2023-01-31T20:25:38Z",
"LastObservedAt": "2023-05-04T18:18:43Z",
"CreatedAt": "2023-01-31T20:25:38Z",
"UpdatedAt": "2023-05-04T18:18:43Z",
"Severity": {
  "Label": "HIGH",
  "Normalized": 70
},
"Title": "CVE-2022-34918 - kernel",
"Description": "An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c."
,
"Remediation": {
  "Recommendation": {
    "Text": "Remediation is available. Please refer to the fixed version in the vulnerability details section above. For detailed remediation guidance for each of the affected packages, refer to the vulnerabilities section of the detailed finding JSON."
  }
},
"ProductFields": {
  "aws/inspector/FindingStatus": "ACTIVE",
  "aws/inspector/inspectorScore": "7.8",
  "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform": "AMAZON_LINUX_2",
  "aws/inspector/ProductVersion": "2",
  "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
  "aws/securityhub/ProductName": "Inspector",
  "aws/securityhub/CompanyName": "Amazon"
},
"Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
    "Partition": "aws",
    "Region": "us-east-1",
    "Tags": {
      "Patch Group": "SSM",
      "Name": "High-SEv-Test"
    },
    "Details": {
      "AwsEc2Instance": {
        "Type": "t2.micro",
        "ImageId": "ami-0cfff7528ff583bf9a",
        "Ipv4Addresses": [
          "52.87.229.97",
          "172.31.57.162"
        ],
        "KeyName": "ACloudGuru",
        "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AmazonSSMRoleForInstancesQuickSetup",
        "VpcId": "vpc-a0c2d7c7",
```
"SubnetId": "subnet-9c934cb1",
"LaunchedAt": "2022-07-26T21:49:46Z"
}
}
,"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"Vulnerabilities": [
  {
    "Id": "CVE-2022-34918",
    "VulnerablePackages": [
      {
        "Name": "kernel",
        "Version": "5.10.118",
        "Epoch": "0",
        "Release": "111.515.amzn2",
        "Architecture": "X86_64",
        "PackageManager": "OS",
        "FixedInVersion": "0:5.10.130-50.517.amzn2",
        "Remediation": "yum update kernel"
      }
    ],
    "Cvss": [
      {
        "Version": "2.0",
        "BaseScore": 7.2,
        "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
        "Source": "NVD"
      },
      {
        "Version": "3.1",
        "BaseScore": 7.8,
        "Source": "NVD"
      },
      {
        "Version": "3.1",
        "BaseScore": 7.8,
        "Source": "NVD",
        "Adjustments": []
      }
    ],
    "Vendor": {
      "Name": "NVD",
      "VendorSeverity": "HIGH",
      "VendorCreatedAt": "2022-07-04T21:15:00Z",
      "VendorUpdatedAt": "2022-10-26T17:05:00Z"
    },
    "ReferenceUrls": [
      "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=7e6bc1f6cabcb30a8b0b1219d8e01b952eacbb6",
      "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffbd22-d949-d86f486f452@randorisec.fr/T/",
      "https://www.debian.org/security/2022/dsa-5191"
    ],
    "FixAvailable": "YES"
  }
},
"FindingProviderFields": {
  "Severity": {
    "Value": 7.2
  }
}
Activating and configuring the integration

To use the Amazon Inspector integration with AWS Security Hub, you must activate Security Hub. For information on how to activate Security Hub, see Setting up Security Hub in the AWS Security Hub User Guide.

When you activate both Amazon Inspector and Security Hub, the integration is activated automatically, and Amazon Inspector begins to send findings to Security Hub. Amazon Inspector sends all of the findings it generates to Security Hub using the AWS Security Finding Format (ASFF).

Stopping the publication of findings to AWS Security Hub

How to stop sending findings

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

See Deactivating and activating the flow of findings from an integration (console) or Deactivating the flow of findings from an integration (Security Hub API, AWS CLI) in the AWS Security Hub User Guide.
Operating systems and programming languages supported by Amazon Inspector

Amazon Inspector can scan software applications installed on Amazon Elastic Compute Cloud (Amazon EC2) instances, container images stored in Amazon Elastic Container Registry (Amazon ECR) repositories and AWS Lambda functions. For container images in Amazon ECR, Amazon Inspector can scan for both operating system and programming language package vulnerabilities. For Lambda functions Amazon Inspector can inspect for code vulnerabilities. When Amazon Inspector scans resources, it uses its own purpose-built scanning engine and it sources more than 50 data feeds to generate findings for Common Vulnerabilities and Exposures (CVEs). Sources include vendor security advisories, NVD, MITRE, open-source feeds, internal research, and licensed data feeds.

For Amazon Inspector to scan a resource, the resource must be running a supported operating system or use a supported programming language. The topics in this section list the operating systems, runtimes and programming languages that Amazon Inspector currently supports for different resources and scan types. They also list operating systems that Amazon Inspector previously supported but have since been discontinued by vendors. Amazon Inspector can provide only limited support for an operating system after a vendor discontinues support for the operating system.

Topics
• Supported operating systems: Amazon EC2 scanning (p. 129)
• Supported programming languages: Amazon EC2 Deep inspection (p. 131)
• Supported operating systems: Amazon ECR scanning (p. 131)
• Supported programming languages: Amazon ECR scanning (p. 133)
• Supported runtimes: Amazon Inspector Lambda standard scanning (p. 133)
• Supported runtimes: Amazon Inspector Lambda code scanning (p. 134)
• Discontinued operating systems (p. 134)

Supported operating systems: Amazon EC2 scanning

The following table lists the operating systems that Amazon Inspector currently supports for scans of Amazon Elastic Compute Cloud (Amazon EC2) instances, and the source of the vendor security advisories for each one.

Note
Linux operating system detections are only supported for the default package manager repository and do not include optional repositories, such as Red Hat Application Streams.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Vendor security advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlmaLinux</td>
<td>8</td>
<td>ALSA</td>
</tr>
<tr>
<td>AlmaLinux</td>
<td>9</td>
<td>ALSA</td>
</tr>
<tr>
<td>Amazon Linux (AL2)</td>
<td>AL2</td>
<td>ALAS</td>
</tr>
</tbody>
</table>

129
<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Vendor security advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux 2023 (AL2023)</td>
<td>AL2023</td>
<td>ALAS</td>
</tr>
<tr>
<td>Bottlerocket</td>
<td>1.7.0 and later</td>
<td>GHSA, CVE</td>
</tr>
<tr>
<td>CentOS Linux (CentOS)</td>
<td>7</td>
<td>CESA</td>
</tr>
<tr>
<td>Debian Server (Buster)</td>
<td>10</td>
<td>DSA</td>
</tr>
<tr>
<td>Debian Server (Bullseye)</td>
<td>11</td>
<td>DSA</td>
</tr>
<tr>
<td>Debian Server (Bookworm)</td>
<td>12</td>
<td>DSA</td>
</tr>
<tr>
<td>Fedora</td>
<td>37</td>
<td>CVE</td>
</tr>
<tr>
<td>Fedora</td>
<td>38</td>
<td>CVE</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.4</td>
<td>CVE</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.5</td>
<td>CVE</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>7</td>
<td>ELSA</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>8</td>
<td>ELSA</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>9</td>
<td>ELSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>7</td>
<td>RHSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>8</td>
<td>RHSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>9</td>
<td>RHSA</td>
</tr>
<tr>
<td>Rocky Linux</td>
<td>8</td>
<td>RLSA</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.4</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.5</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.3</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.4</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.5</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>Ubuntu (Trusty)</td>
<td>14.04 (ESM)</td>
<td>USN, Ubuntu Pro</td>
</tr>
<tr>
<td>Ubuntu (Xenial)</td>
<td>16.04 (ESM)</td>
<td>USN, Ubuntu Pro</td>
</tr>
<tr>
<td>Ubuntu (Bionic)</td>
<td>18.04 (ESM)</td>
<td>USN, Ubuntu Pro</td>
</tr>
<tr>
<td>Ubuntu (Focal)</td>
<td>20.04 (LTS)</td>
<td>USN</td>
</tr>
<tr>
<td>Ubuntu (Jammy)</td>
<td>22.04 (LTS)</td>
<td>USN</td>
</tr>
<tr>
<td>Ubuntu (Lunar Lobster)</td>
<td>23.04</td>
<td>USN</td>
</tr>
</tbody>
</table>
Supported programming languages: Amazon EC2 Deep inspection

The following lists the programming languages that Amazon Inspector currently supports when scanning Amazon EC2 Linux instances for vulnerabilities in third-party software packages:

- Java
- JavaScript
- Python

Amazon Inspector uses Systems Manager Distributor to deploy the plugin used for Deep inspection in your Amazon EC2 instance. Systems Manager Distributor supports the operating systems listed as Supported package platforms and architectures in the Systems Manager guide. Your Amazon EC2 instance’s operating system must be supported by Systems Manager Distributor and Amazon Inspector for Amazon Inspector to perform Deep inspection scans.

**Note**
Deep inspection is not supported for Bottlerocket operating systems.

Supported operating systems: Amazon ECR scanning

The following table lists the operating systems that Amazon Inspector currently supports for scans of container images in Amazon Elastic Container Registry (Amazon ECR) repositories, and the source of the vendor security advisories for each one.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Vendor security advisories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.14</td>
<td>Alpine Secdb</td>
</tr>
<tr>
<td>Operating system</td>
<td>Version</td>
<td>Vendor security advisories</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.15</td>
<td>Alpine Secdb</td>
</tr>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.16</td>
<td>Alpine Secdb</td>
</tr>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.17</td>
<td>Alpine Secdb</td>
</tr>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.18</td>
<td>Alpine Secdb</td>
</tr>
<tr>
<td>AlmaLinux</td>
<td>8</td>
<td>ALSA</td>
</tr>
<tr>
<td>AlmaLinux</td>
<td>9</td>
<td>ALSA</td>
</tr>
<tr>
<td>Amazon Linux (AL2)</td>
<td>AL2</td>
<td>ALAS</td>
</tr>
<tr>
<td>Amazon Linux 2023 (AL2023)</td>
<td>AL2023</td>
<td>ALAS</td>
</tr>
<tr>
<td>CentOS Linux (CentOS)</td>
<td>7</td>
<td>CESA</td>
</tr>
<tr>
<td>Debian Server (Buster)</td>
<td>10</td>
<td>DSA</td>
</tr>
<tr>
<td>Debian Server (Bullseye)</td>
<td>11</td>
<td>DSA</td>
</tr>
<tr>
<td>Debian Server (Bookworm)</td>
<td>12</td>
<td>DSA</td>
</tr>
<tr>
<td>Fedora</td>
<td>37</td>
<td>CVE</td>
</tr>
<tr>
<td>Fedora</td>
<td>38</td>
<td>CVE</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.4</td>
<td>CVE</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.5</td>
<td>CVE</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>7</td>
<td>ELSA</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>8</td>
<td>ELSA</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>9</td>
<td>ELSA</td>
</tr>
<tr>
<td>Photon OS</td>
<td>3</td>
<td>PHSA</td>
</tr>
<tr>
<td>Photon OS</td>
<td>4</td>
<td>PHSA</td>
</tr>
<tr>
<td>Photon OS</td>
<td>5</td>
<td>PHSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>7</td>
<td>RHSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>8</td>
<td>RHSA</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>9</td>
<td>RHSA</td>
</tr>
<tr>
<td>Rocky Linux</td>
<td>8</td>
<td>RLSA</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.4</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.5</td>
<td>SUSE CVE</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.3</td>
<td>SUSE CVE</td>
</tr>
</tbody>
</table>
Supported programming languages: Amazon ECR scanning

The following lists the programming languages that Amazon Inspector currently supports when scanning container images in Amazon Elastic Container Registry (Amazon ECR) repositories:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Supported runtimes: Amazon Inspector Lambda standard scanning

The following lists the programming language runtimes that Amazon Inspector Lambda standard scanning currently supports when scanning Lambda functions for vulnerabilities in third-party software packages:

- Java
  - java8
  - java8.al2
  - java11
  - java17
  - NodeJS
  - nodejs12.x
Supported runtimes: Amazon Inspector Lambda code scanning

The following lists the programming language runtimes that Amazon Inspector Lambda code scanning currently supports when scanning Lambda functions for vulnerabilities in code:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- NodeJS
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Discontinued operating systems

Standard vendor support for the operating systems listed in the following tables has been discontinued by the vendor. In the tables, the Discontinued column indicates when the vendor discontinued standard support for an operating system.
Amazon Inspector previously provided full support for these operating systems and will continue to scan Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon Elastic Container Registry (Amazon ECR) container images that are running them. However, in accordance with vendor policy, the operating systems are no longer updated with patches and, in many cases, new security advisories are no longer released for them. In addition, some vendors remove existing security advisories and detections from their feeds when an affected operating system reaches the end of standard support. Consequently, Amazon Inspector might stop generating findings for known CVEs. Any findings that Amazon Inspector does generate for a discontinued operating system should be used for informational purposes only.

As a security best practice and for continued Amazon Inspector coverage, we encourage you to move to a current, supported version of an operating system.

**Discontinued operating systems: Amazon EC2 scanning**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Discontinued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux (AL1)</td>
<td>2012</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>CentOS Linux (CentOS)</td>
<td>8</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>Debian Server (Stretch)</td>
<td>9</td>
<td>June 30, 2022</td>
</tr>
<tr>
<td>Fedora</td>
<td>35</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>Fedora</td>
<td>36</td>
<td>May 16, 2023</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.3</td>
<td>December 1, 2022</td>
</tr>
<tr>
<td>OpenSUSE Leap (SUSE Leap)</td>
<td>15.2</td>
<td>December 1, 2021</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>6</td>
<td>March 1, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12</td>
<td>July 1, 2019</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.1</td>
<td>May 31, 2020</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.2</td>
<td>March 31, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.3</td>
<td>June 30, 2022</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15</td>
<td>December 31, 2019</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.1</td>
<td>January 31, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.2</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>Ubuntu (Groovy)</td>
<td>20.10</td>
<td>July 22, 2021</td>
</tr>
<tr>
<td>Ubuntu (Hirsute)</td>
<td>21.04</td>
<td>January 20, 2022</td>
</tr>
<tr>
<td>Ubuntu (Impish)</td>
<td>21.10</td>
<td>July 31, 2022</td>
</tr>
<tr>
<td>Ubuntu (Kinetic)</td>
<td>22.10</td>
<td>July 20, 2023</td>
</tr>
</tbody>
</table>
## Discontinued operating systems: Amazon ECR scanning

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
<th>Discontinued</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.12</td>
<td>May 1, 2022</td>
</tr>
<tr>
<td>Alpine Linux (Alpine)</td>
<td>3.13</td>
<td>November 1, 2022</td>
</tr>
<tr>
<td>Amazon Linux (AL1)</td>
<td>2012</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>CentOS Linux (CentOS)</td>
<td>8</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>Debian Server (Stretch)</td>
<td>9</td>
<td>June 30, 2022</td>
</tr>
<tr>
<td>Fedora</td>
<td>35</td>
<td>December 13, 2022</td>
</tr>
<tr>
<td>Fedora</td>
<td>36</td>
<td>May 16, 2023</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>15.3</td>
<td>December 1, 2022</td>
</tr>
<tr>
<td>OpenSUSE Leap (SUSE Leap)</td>
<td>15.2</td>
<td>December 1, 2021</td>
</tr>
<tr>
<td>Oracle Linux (Oracle)</td>
<td>6</td>
<td>March 1, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12</td>
<td>July 1, 2019</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.1</td>
<td>May 31, 2020</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.2</td>
<td>March 31, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>12.3</td>
<td>June 30, 2022</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15</td>
<td>December 31, 2019</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.1</td>
<td>January 31, 2021</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>15.2</td>
<td>December 31, 2021</td>
</tr>
<tr>
<td>Ubuntu (Groovy)</td>
<td>20.10</td>
<td>July 22, 2021</td>
</tr>
<tr>
<td>Ubuntu (Hirsute)</td>
<td>21.04</td>
<td>January 20, 2022</td>
</tr>
<tr>
<td>Ubuntu (Impish)</td>
<td>21.10</td>
<td>July 31, 2022</td>
</tr>
<tr>
<td>Ubuntu (Kinetic)</td>
<td>22.10</td>
<td>July 20, 2023</td>
</tr>
</tbody>
</table>
Deactivating Amazon Inspector

You can deactivate Amazon Inspector in any AWS Region by using the Amazon Inspector console or API. Follow the instructions at the end of this topic to deactivate Amazon Inspector. If you deactivate all Amazon Inspector scans for an AWS account, Amazon Inspector is deactivated for this account automatically. For information about deactivating scans types for different resources, see Scanning resources with Amazon Inspector (p. 57).

After Amazon Inspector is deactivated for an account, all scan types are deactivated for that account in that Region. Additionally, all Amazon Inspector scan settings, suppression rules, and filters and findings for the account in that Region are deleted.

You aren’t charged for using Amazon Inspector while it’s deactivated for your account in that Region. After you deactivate Amazon Inspector, you can choose to re-activate it at a later time.

Note
Before you deactivate Amazon Inspector, we recommend that you export your findings. For more information, see Exporting findings reports from Amazon Inspector (p. 24).

When you deactivate Amazon Inspector Amazon EC2 scanning, the following SSM associations used by Amazon Inspector are deleted:

- InspectorDistributor-do-not-delete
- InspectorInventoryCollection-do-not-delete
- InvokeInspectorSsmPlugin-do-not-delete. Additionally, the Amazon Inspector SSM plug-in installed through this association is removed from all of your Windows hosts. For more information, see Scanning Windows instances (p. 64).

Prerequisites

Depending on your account type, you might need to take additional steps before deactivating Amazon Inspector as follows:

- If you have a standalone Amazon Inspector account, you can deactivate it at any time.
- If you are a member account in an Amazon Inspector multi-account environment, you cannot deactivate your own service. You must contact the delegated administrator for your organization to deactivate your service.
- If you are a delegated administrator, you must disassociate all of your member accounts before you can deactivate Amazon Inspector. For more information, see Disassociating member accounts in Amazon Inspector (p. 87).

Note
Disassociating an account does not deactivate Amazon Inspector for that account, instead, a disassociated member account becomes a standalone account.

Note
When you deactivate Amazon Inspector as a delegated administrator, the auto-activate feature is deactivated for your organization.
Deactivate Amazon Inspector

Console

To deactivate Amazon Inspector

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. By using the AWS Region selector in the upper-right corner of the page, choose the Region in which you want to deactivate Amazon Inspector.
3. In the navigation pane, choose General settings.
5. When prompted for confirmation, enter deactivate in the text box, and then choose Deactivate Inspector.
6. (Recommended) Repeat these steps in each Region for which you want to deactivate Amazon Inspector.

API

Run the Disable API operation. In the request, provide the account IDs you are deactivating, and EC2, ECR, LAMBDA for resourceTypes to deactivate all scans, which will deactivate the account.
Quotas for Amazon Inspector

Your AWS account has the following quotas for Amazon Inspector per Region.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppression rules</td>
<td>500</td>
<td>The maximum number of saved suppression rules per AWS account per Region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You cannot request a quota increase.</td>
</tr>
<tr>
<td>Amazon EC2 network findings</td>
<td>10,000</td>
<td>The maximum number of Amazon EC2 network findings per AWS account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You cannot request a quota increase.</td>
</tr>
<tr>
<td>Member accounts</td>
<td>7000</td>
<td>The maximum number of member accounts associated with an Amazon Inspector account. This limit is based on AWS Organizations, see Quotas for AWS Organizations.</td>
</tr>
</tbody>
</table>

For a list of quotas associated with Amazon Inspector Classic, see Amazon Inspector service quotas in the AWS General Reference.

For a list of quotas associated with Organizations, see Organizations service quotas in the AWS General Reference.
Regions and endpoints

To view the AWS Regions where Amazon Inspector is available, see [Amazon Inspector endpoints](amazon-inspector-landing-page) in the Amazon Web Services General Reference.

Region-specific feature availability

This section describes the availability of Amazon Inspector features by AWS Region.

**Lambda code scanning Regions**

The following table shows the AWS Regions where Lambda code scanning is currently available.

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region code</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>us-east-2</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>ap-southeast-2</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>ap-northeast-1</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>eu-central-1</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>eu-west-1</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>eu-west-2</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>eu-north-1</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>ap-southeast-1</td>
</tr>
</tbody>
</table>

**AWS GovCloud (US) Regions**

For the latest information, see [Amazon Inspector](amazon-inspector-landing-page) in the AWS GovCloud (US) User Guide.
Document history for the Amazon Inspector User Guide

The following table describes the important changes to the documentation since the last release of Amazon Inspector. For notification about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New supported resources (p. 141)</td>
<td>Amazon Inspector now supports scanning of MacOS Amazon EC2 instances. See Supported operating systems: Amazon EC2 scanning for supported MacOS versions.</td>
<td>October 5, 2023</td>
</tr>
<tr>
<td>New Regions (p. 141)</td>
<td>Amazon Inspector is now available in Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), and Europe (Zurich).</td>
<td>September 29, 2023</td>
</tr>
<tr>
<td>New feature (p. 141)</td>
<td>You can now exclude EC2 instances from Amazon Inspector scans using exclusion tags.</td>
<td>September 14, 2023</td>
</tr>
<tr>
<td>New feature (p. 141)</td>
<td>Amazon Inspector has added new permissions that allow Amazon Inspector to scan network configurations of Amazon EC2 instances that are part of Elastic Load Balancing target groups.</td>
<td>August 31, 2023</td>
</tr>
<tr>
<td>New feature (p. 141)</td>
<td>Amazon Inspector now provides vulnerability intelligence details for package vulnerability findings.</td>
<td>July 31, 2023</td>
</tr>
<tr>
<td>Updated functionality (p. 141)</td>
<td>Amazon Inspector has added new permissions that allow read-only users to export Software Bill of Materials (SBOM) for their resources.</td>
<td>June 29, 2023</td>
</tr>
<tr>
<td>New feature (p. 141)</td>
<td>You can now export SBOM for resources being scanned by Amazon Inspector.</td>
<td>June 13, 2023</td>
</tr>
<tr>
<td>New feature (p. 141)</td>
<td>Lambda code scanning is now generally available. New features have been added that allow you to encrypt code identified in your Lambda code scanning</td>
<td>June 13, 2023</td>
</tr>
</tbody>
</table>
findings. Additionally Lambda code scanning now provides suggested remediation rewrites of your code.

<table>
<thead>
<tr>
<th>Updated functionality (p. 141)</th>
<th>Amazon Inspector added a new statement to the AmazonInspector2ReadOnlyAccess policy. The new statements allows read-only users to retrieve details of Lambda code scanning status and findings for their account.</th>
<th>May 2, 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>New feature (p. 141)</td>
<td>Amazon Inspector has added Vulnerability database search which allows you to check if Amazon Inspector covers a specific CVE.</td>
<td>May 1, 2023</td>
</tr>
<tr>
<td>Updated functionality (p. 141)</td>
<td>Amazon Inspector has added new permissions to the AmazonInspector2ServiceRolePolicy policy that allow Amazon Inspector to create AWS CloudTrail service-linked channels in your account when you activate Lambda scanning. This allows Amazon Inspector to monitor CloudTrail events in your account.</td>
<td>April 30, 2023</td>
</tr>
<tr>
<td>Updated functionality (p. 141)</td>
<td>Amazon Inspector added a new statement to the AmazonInspector2FullAccess policy. The new statement allows users to retrieve details of code vulnerability findings from Lambda code scanning.</td>
<td>April 17, 2023</td>
</tr>
<tr>
<td>Updated functionality (p. 141)</td>
<td>Amazon Inspector added a new statement to the AmazonInspector2ServiceRolePolicy policy. The new statement allows Amazon Inspector to send information to Amazon EC2 Systems Manager about the custom paths you have defined for Amazon EC2 Deep inspection.</td>
<td>April 17, 2023</td>
</tr>
<tr>
<td>Date</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>April 17, 2023</td>
<td><strong>New feature (p. 141)</strong></td>
<td>Amazon Inspector adds additional support for Linux EC2 instances in the form of Amazon Inspector Deep inspection, which scans your instances for package vulnerabilities in application programming language packages.</td>
</tr>
<tr>
<td>February 28, 2023</td>
<td><strong>Updated functionality (p. 141)</strong></td>
<td>Amazon Inspector added a new statement to the AmazonInspector2ServiceRolePolicy policy. The new statements allows Amazon Inspector to request scans of the developer code in AWS Lambda functions, and receive scan data from Amazon CodeGuru Security. Additionally Amazon Inspector has added permissions to review IAM policies. Amazon Inspector uses this information to scan Lambda functions for code vulnerabilities.</td>
</tr>
<tr>
<td>February 28, 2023</td>
<td><strong>New feature (p. 141)</strong></td>
<td>Amazon Inspector adds additional support for Lambda functions in the form of Lambda code scanning, which scan the developer code of your Lambda functions for security vulnerabilities.</td>
</tr>
<tr>
<td>February 20, 2023</td>
<td><strong>Updated functionality (p. 141)</strong></td>
<td>Amazon Inspector added a new statement to the AmazonInspector2ServiceRolePolicy policy. The new statement allows Amazon Inspector to retrieve information from CloudWatch about when an AWS Lambda function was last invoked. uses this information to focus scans on the Lambda functions in your environment that have been active in the last 90 days.</td>
</tr>
<tr>
<td>November 28, 2022</td>
<td><strong>Updated functionality (p. 141)</strong></td>
<td>Amazon Inspector added a new statement to the AmazonInspector2ServiceRolePolicy policy. The new statement allows Amazon Inspector to retrieve information about your AWS Lambda functions. Amazon Inspector uses this information to scan your Lambda functions for security vulnerabilities.</td>
</tr>
<tr>
<td>Date</td>
<td>New feature (p. 141)</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>November 28, 2022</td>
<td>Amazon Inspector adds support for Scanning AWS Lambda functions.</td>
<td></td>
</tr>
<tr>
<td>October 14, 2022</td>
<td>Updated content (p. 141)</td>
<td></td>
</tr>
<tr>
<td>October 7, 2022</td>
<td>New content (p. 141)</td>
<td></td>
</tr>
<tr>
<td>September 2, 2022</td>
<td>New feature (p. 141)</td>
<td></td>
</tr>
<tr>
<td>August 31, 2022</td>
<td>Updated functionality (p. 141)</td>
<td></td>
</tr>
</tbody>
</table>

- **New feature (p. 141)**: Amazon Inspector adds support for Scanning AWS Lambda functions.
- **Updated content (p. 141)**: Added procedures, policy examples, and tips for exporting findings reports from Amazon Inspector to an Amazon Simple Storage Service (Amazon S3) bucket.
- **New content (p. 141)**: Added information about assessing Amazon Inspector coverage of your AWS environment by using the Amazon Inspector console. The information includes descriptions of Status values for individual resources in your environment.
- **New feature (p. 141)**: Amazon Inspector now provides additional details about how to remediate package vulnerabilities. New fields have been added to finding details. The new fields provide context about whether a fix is available through a package update. If a fix is available, the Suggested remediation section of a finding shows the commands that you can run to make the fix.
- **Updated functionality (p. 141)**: Amazon Inspector added a new action to the AmazonInspector2ServiceRolePolicy policy. The new action allows Amazon Inspector to describe SSM association executions. Amazon Inspector also added additional resource scoping to allow Amazon Inspector to create, update, delete, and start SSM associations with AmazonInspector2 owned SSM documents.
<p>| New feature (p. 141) | Amazon Inspector now supports scans for Windows instances. Amazon Inspector can now scan SSM managed instances running supported Windows operating systems. Scans of Windows hosts are performed by the Amazon Inspector SSM plug-in, which is installed and invoked through new SSM associations automatically created by Amazon Inspector. | August 31, 2022 |
| Updated functionality (p. 141) | Amazon Inspector updated the resource scoping of the AmazonInspector2ServiceRolePolicy policy to allow Amazon Inspector to collect software inventory in other AWS partitions. | August 12, 2022 |
| Updated functionality (p. 141) | In the AmazonInspector2ServiceRolePolicy policy, Amazon Inspector restructured the resource scoping of the actions allowing Amazon Inspector to create, delete, and update SSM associations. | August 10, 2022 |
| New feature (p. 141) | Amazon Inspector now supports changing your ECR automated re-scan duration setting. The Amazon ECR automated re-scan duration setting determines how long Amazon Inspector continuously monitors images pushed into repositories. When an image is older than the scan duration, Amazon Inspector will no longer scan the image and close all existing findings for it. All new accounts will automatically have their ECR automated re-scan duration set to lifetime. Previously created accounts had an ECR automated re-scan duration of 30 days, but you can now choose from 30-day, 180-day, or lifetime durations for scans. | June 25, 2022 |</p>
<table>
<thead>
<tr>
<th><strong>New functionality (p. 141)</strong></th>
<th>Amazon Inspector added a new AWS managed policy, the AmazonInspector2ReadOnlyAccess policy, to allow read-only access to Amazon Inspector functionality.</th>
<th>January 21, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General availability (p. 141)</strong></td>
<td>This is the initial public release of the Amazon Inspector User Guide.</td>
<td>November 29, 2021</td>
</tr>
</tbody>
</table>
AWS Glossary

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