Amazon Inspector

User Guide

Amazon Inspector: User Guide

Table of Contents

What is Amazon Inspector?

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

When a software vulnerability or network issue is discovered, Amazon Inspector creates a finding. A finding describes the vulnerability, identifies the affected resource, rates the severity of the vulnerability, and provides remediation guidance. Details of a finding for your account can be analyzed in multiple ways using the Amazon Inspector console, or you can view and process your findings through other AWS services. For more information, see Understanding findings in Amazon Inspector (p. 8).

Topics

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 and designating an account as the delegated administrator account for Amazon Inspector.

Amazon Inspector can be enabled for your entire organization with a single click. Additionally, you can automate enabling 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, enabling or disabling 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 do not need to manually schedule or configure assessment scans. Amazon Inspector automatically discovers and begins scanning your eligible resources (p. 29). Amazon Inspector continues to assess your environment throughout the lifecycle of your resources by automatically scanning resources whenever you make changes to them.

When vulnerabilities or open network paths are identified, Amazon Inspector produces a finding (p. 8) that you can investigate. The finding includes comprehensive details about the vulnerability, the impacted 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. 34) offers a high-level view of findings from across your environment. From the dashboard, you can access the granular details of a finding. The newly redesigned 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, see findings details, and view 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.

Any Amazon Inspector user 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. 20) 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 enabled AWS Security Hub (p. 69), then Amazon Inspector will also publish findings to Security Hub (p. 68). 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 quick setup method to help you get started with Amazon Inspector.

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

In Step 2, you gain hands-on experience explore your findings in the console.

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

Topics

Before you begin

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

Note the following before you enable 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 enable either EC2 scanning or ECR container image scanning, or both. You can manage the scanning types from the account management page within the Amazon Inspector console or using Amazon Inspector APIs.
- Amazon Inspector can provide common vulnerabilities and exposures (CVE) data for your Amazon EC2 instances only if the Amazon EC2 Systems Manager (SSM) agent is installed and enabled. This agent is preinstalled on many Amazon EC2 instances, but you might need to enable it manually. Regardless of SSM agent status, all of your Amazon EC2 instances are scanned for network reachability issues. For more information about configuring scans for Amazon EC2, see Scanning Amazon EC2 instances (p. 29).
- Any user with administrator permissions in an AWS account can enable Amazon Inspector. However, following the security best practice of least privilege, we recommend that you create an IAM user, role, or group specifically to manage Amazon Inspector. For information on the permissions required to enable Amazon Inspector, see AWS managed policy: AmazonInspector2FullAccess (p. 58).
- When you enable 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 VPC configurations in order to generate vulnerability findings. For more information, see Using service-linked roles for Amazon Inspector (p. 61). For more information about service-linked roles, see Using service-linked roles.

Step 1: Enable Amazon Inspector

The first step to using Amazon Inspector is to enable it in your account. After you enable 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 enable 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 **Enable Amazon Inspector**.

When you enable Amazon Inspector in a standalone account, all scan types are enabled by default. You can manage enabled scan types from the account management page within the Amazon Inspector console or by using Amazon Inspector APIs. After Amazon Inspector is enabled, 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 enabled. This agent is pre-installed on many EC2 instances, but you may need to enable it manually. Regardless of SSM agent status, all of your EC2 instances will be scanned for network reachability issues. For more information on configuring scans for Amazon EC2, see Scanning Amazon EC2 instances with Amazon Inspector (p. 29).

Amazon ECR scanning

When you enable 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 ECR scan setting can be changed at any time. For more information on configuring scans for Amazon ECR, see Scanning Amazon ECR container images with Amazon Inspector (p. 30).

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. 40).

To delegate an administrator for Amazon Inspector

1. Log in to the AWS Organizations management account.
2. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
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 administration**.

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

Amazon Inspector currently offers scans for EC2 instances and scans for ECR container images. After you enable Amazon Inspector, it automatically begins 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 instance, Amazon Inspector requires that the AWS Systems Manager (SSM) agent be installed and enabled. This agent is pre-installed on many Amazon EC2 instances, but you may need to enable it manually. Regardless of SSM agent status, all of your Amazon EC2 instances will be scanned for network reachability issues. For more information on configuring scans for Amazon EC2, see Scanning Amazon EC2 instances with Amazon Inspector (p. 29).

Amazon ECR scanning

When you enable 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 continuous 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 ECR scan setting can be changed by the delegated administrator at any time. For more information on configuring scans for Amazon ECR, see Scanning Amazon ECR container images with Amazon Inspector (p. 30).

To add member accounts

As a delegated administrator you can enable Amazon EC2 scanning, Amazon ECR scanning, or both, for any member associated with the Organizations management account. This workflow enables scans for all member accounts. However, members can also enable Amazon Inspector for their own accounts, or the service can be selectively enabled by the delegated administrator. For more information, see Managing multiple accounts (p. 39).

1. Log in to the delegated administrator account.
2. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
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 **Enable scanning for all accounts** from the top banner to enable both Amazon EC2 instance and Amazon ECR container image 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 **Enable** menu, select **All scanning**.
5. (Optional) Turn on the **Auto-enable** feature and select the scan types to include to enable those scans for any new member accounts that are added to your organization.

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 enabled). 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 on the Amazon Inspector dashboard, see Understanding the dashboard (p. 34).

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 on that item.
3. From the navigation pane, select **Findings**.
4. By default you will see the **All findings** tab, which displays all EC2 instance and ECR container image 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 on 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 Breakdown** tab explaining how the Amazon Inspector score was calculated for that finding. For more details on finding types, see Finding types in Amazon Inspector (p. 8).

Understanding findings in Amazon Inspector

In Amazon Inspector, a finding is a detailed report about a potential vulnerability that affects one of your resources. Amazon Inspector generates a finding whenever it detects a potential vulnerability for an Amazon EC2 instance or a potential software vulnerability in a container image within an Amazon ECR repository. Each finding is titled according to the detected vulnerability and provides a severity rating, information about the affected resource, and additional 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 can be assigned one of the following states:

Active

The finding is identified by Amazon Inspector and has not yet 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, with the exception of the **Suppressed findings** list. For more information about suppressed findings, see Suppressing Amazon Inspector findings with suppression rules (p. 14)

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

Amazon Inspector generates findings for the following AWS resources: Amazon EC2 instances, and container images residing in Amazon ECR repositories.

Following are the finding types identified by Amazon Inspector:

Package vulnerability

Package vulnerability findings identify software packages in your 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://cve.mitre.org/.

Package vulnerability findings are generated for both Amazon EC2 instances and ECR container images.

Network reachability

Network reachability findings indicate that there are allowed 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, ACLs, or IGWs, or that may allow for potentially malicious access.

Network reachability findings are only generated for Amazon EC2 resources.

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

- Amazon EC2 instances
- Application Load Balancers
- Direct Connect
- Elastic Load Balancers
- Elastic Network Interfaces
- Internet Gateways
- Network Access Control Lists
- Route Tables
- Security Groups
- Subnets
- Virtual Private Clouds
- Virtual Private Gateways
- VPC endpoints
- VPC gateway endpoints
- VPC peering connections
- VPN connections

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) You can view the findings grouped by the following categories by selecting that category from the navigation pane or findings table:

   - Vulnerability
   - Account
   - Instance
   - Container image
   - Repository
   - All findings

The details for each finding differ depending on the finding type, resources involved, and the type of vulnerability. For more information on available finding fields, see the following section.

Amazon Inspector Finding summary

In the Amazon Inspector console, you can view finding details in a finding summary section. Finding details vary based on finding type.

Finding details

Choose a row in the findings list to see all occurrences of that finding as well as its details, suggested remediation, and the severity score. See Severity levels for Amazon Inspector findings (p. 10) for information about scoring. Choose the title of a finding to see specific information.

The finding's **Details** tab contains the basic identifying features of the finding, including the following information:

- **Overview** – The ID of the account that owns the impacted resource, the finding severity, vulnerability type, and when the finding was last detected.
- **Affected packages** – The name, version, and package manager for the packages affected by the finding.
- **Vulnerability details** – A link to the Amazon Inspector preferred source for the CVE identified in the finding, such as National Vulnerability Database (NVD), REDHAT or other OS vendors. Additionally you will find the severity score for the finding, and scoring details. See Severity levels for Amazon Inspector findings (p. 10) for more details about severity scoring.
- **Related vulnerabilities** – Other vulnerabilities related to the finding.
- **Resource affected** – Information about the resource affected by this finding such as the Resource ID and type.
- **Tags** – Tags relevant to the resource.
- **Remediation** – A brief description of the recommended action to remediate the finding.

The **Score breakdown** tab contains the finding's scoring details. Here you can see comprehensive metrics on how the finding was assessed and how the Inspector score was calculated.

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 does not imply or otherwise indicate the criticality or importance that an affected resource might have for your organization.

A finding's severity rating is represented as **untriaged**, **informational**, **low**, **medium**, **high**, or **critical**. This rating is driven by a numerical score. The method by which the score is determined is based on whether the vulnerability is found in a software package or through network reachability. See the following sections on these two vulnerability types to learn more about how their severity rating is determined.

Score breakdown

The score breakdown section of a finding explains how the severity rating was assigned based on a combination of the Amazon Inspector score and the Vendor score for the software package.

Amazon Inspector score

The Amazon Inspector risk score is a highly contextualized score that is generated for each finding by correlating common vulnerabilities and exposures (CVE) information with network reachability results and exploitability data. This score allows you to prioritize findings and focus on the most critical findings and vulnerable resources. You can see how the Amazon Inspector score was calculated and which factors influenced the score in the **Score breakdown** tab within the findings details pane.

Amazon Inspector examines the security metrics that compose the National Vulnerability Database (NVD) base score for the vulnerability and adjusts them according your compute environment. For example, the service may lower the Amazon Inspector score of a finding if the vulnerability is exploitable over the network but no open network path to the vulnerable instance is available from the internet. The Amazon Inspector score helps you prioritize your findings by highlighting the most critical vulnerabilities for your specific environment. This score is in CVSS format and is a modification of the base Common Vulnerability Scoring System (CVSS) score provided by NVD.

Software package vulnerability scoring

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. This score is considered a base score because it reflects the severity of a vulnerability according to its intrinsic characteristics, which are constant over time, and assumes the reasonable worst-case impact across different deployed environments. The CVSS v3 standard maps CVSS scores to the following severity ratings:

Score	Rating
0	Informational
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Network reachability scoring

The severity for a network reachability vulnerability is determined by the service, ports, and protocols that are exposed and by the type of open path. The severity ratings are defined in the following table. The value in the **Open path rating** column represents open paths from virtual gateways, peered VPCs, and Direct Connect networks. All other exposed services, ports, and protocols have an Informational severity rating.

Service	TCP ports	UDP ports	Internet path rating	Open path rating
DHCP	67, 68, 546, 547	67, 68, 546, 547	Medium	Informational
Elasticsearch	9300, 9200	NA	Medium	Informational
FTP	21	21	High	Medium

Global catalog LDAP	3268	NA	Medium	Informational
Global catalog LDAP over TLS	3269	NA	Medium	Informational
HTTP	80	80	Low	Informational
HTTPS	443	443	Low	Informational
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Medium	Informational
LDAP	389	389	Medium	Informational
LDAP over TLS	636	NA	Medium	Informational
MongoDB	27017, 27018, 27019, 28017	NA	Medium	Informational
MySQL	3306	NA	Medium	Informational
NetBIOS	137, 139	137, 138	Medium	Informational
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Medium	Informational
Oracle	1521, 1630	NA	Medium	Informational
PostgreSQL	5432	NA	Medium	Informational
Print services	515	NA	High	Medium
RDP	3389	3389	Medium	Low
RPC	111, 135, 530	111, 135, 530	Medium	Informational
SMB	445	445	Medium	Informational
SSH	22	22	Medium	Low
SQL Server	1433	1434	Medium	Informational
Syslog	601	514	Medium	Informational
Telnet	23	23	High	Medium
WINS	1512, 42	1512, 42	Medium	Informational

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 potential vulnerability or 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. 69). Container image findings are also available in the Amazon ECR console, and you can view all findings using the AWS Command Line Interface (AWS CLI) or API.

Topics

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 a tab above the findings list. You can also create a filter on each tab to focus on specific types of findings. For more information about using filters, see Filtering Amazon Inspector findings (p. 14).

Findings can be grouped by the following parameters:

- **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.
- **Vulnerability** – Identifies the most critical vulnerabilities detected in your environment. Choose a vulnerability title from this view to open a details pane with additional information.
- **Account** – Lists your accounts and shows Amazon Inspector coverage and the total number of **Critical** and **High** severity findings for each account. This grouping is only available to delegated administrators.
- **Instance** – Identifies the most vulnerable Amazon EC2 instances in your environment.
- **Container image** – Identifies the most vulnerable Amazon ECR container images in your environment.
- **Repository** – Shows the repositories with the most vulnerabilities.

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. 14).

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. 14).

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.

To apply a filter to the findings view

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
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 criterion 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, but they are not published to Amazon EventBridge.

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.

Creating a suppression rule

You can create suppression rules to filter the list of findings that are shown by default.

To create a suppression rule

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
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

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
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 with Amazon Inspector

Amazon Inspector automatically exports findings to EventBridge and, optionally, to an Amazon S3 bucket.

To export active findings to an Amazon S3 bucket, you need a KMS key that Amazon Inspector can use to encrypt findings and an S3 bucket with permissions that allow Amazon Inspector to upload objects.

You can generate reports in CSV or JSON formats in the Amazon Inspector console or by using the Amazon Inspector API. All users with delegated administrator, member, and standalone accounts can generate and export reports. You can choose to generate either a full report, with all findings in a single report, or a customized report based on view filters that were added in the console.

To produce a customized report, add view filters before generating the report. For example, a user from the delegated administrator account who wants to produce a customized report with only critical findings for an account can apply two filters (account = 'X' and severity = 'critical') before generating the report.

Only one report can be generated at a time. If a report is in progress, new reports cannot be generated until the report in progress is completed and pushed to the S3 bucket.

> **Note**
> You can check the status of an in-progress report with the GetFindingsReportStatus API.

Permissions required to configure findings export

When you configure export options for findings, you select an Amazon S3 bucket to store the findings and a KMS key to use for data encryption. In addition to permissions to Amazon Inspector actions, you must also have permissions to the following actions to successfully configure export options for findings:

- `kms:ListAliases`
- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutBucketPolicy`
- `s3:PutObject`

> **Important**
> If your policy explicitly denies `s3:putObjectAcl`, you will not be able to export findings.

Granting Amazon Inspector permissions to a KMS key

Amazon Inspector encrypts the findings data in your Amazon S3 bucket by using an AWS KMS key. To successfully configure findings export, you must first give Amazon Inspector permissions to use a KMS key. You grant the permissions by changing the key policy for the key you use or by creating a new key.

If you plan to use a new key for Amazon Inspector findings, create a key before proceeding. If you are using a key in another account, you need to log in to the account that owns the key to apply the key policy. You also need the Amazon Resource Name (ARN) for a key from another account when you configure export settings.

To modify or create a key policy to allow Amazon Inspector to use the key

1. Open the AWS KMS console at https://console.aws.amazon.com/kms.
2. To change the AWS Region, use the Region selector in the upper-right corner of the page.
3. Create a new key or choose an existing key that you plan to use to encrypt exported findings. The key must be in the same Region as the Amazon S3 bucket that you export findings to.
4. Select your key, and then make a note of the key ARN from the **General configuration** pane.
5. Under **Key policy**, choose **Edit**. If **Switch to policy view** is displayed, choose that to display the key policy, and then choose **Edit**.
6. Add the following statement granting Amazon Inspector access to your key to the policy. This statement allows Amazon Inspector to use only the key for which you changed the policy. When you edit the key policy, make sure your JSON syntax is valid. In particular, be sure to add a comma before or after your statement, depending on where you add it to the policy.

```
{
    "Sid": "Allow inspector to perform kms actions",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:123456789012:report/*"
        }
    }
}
```

   Note
   If you're using Inspector in a manually-enabled Region, replace the value for the "Service" with the Regional endpoint for that Region. For example, if you're using Inspector in the Middle East (Bahrain) (me-south-1) Region, replace `"Service": "inspector2.amazonaws.com"` with `"Service": "inspector2.me-south-1.amazonaws.com"`.

7. Choose **Save**.
8. (Optional) Make a note of the key ARN for use in later steps. To locate the key ARN, see Finding the key ID and ARN.

Granting Amazon Inspector permissions to an S3 bucket

To export findings to an existing bucket within your account or in a different AWS account, you must grant Amazon Inspector permissions to upload objects to that bucket. You grant these permissions by adding an S3 bucket policy. If you are using an existing bucket, expand the following section for step-by-step instructions on adding a bucket policy.

To add a bucket policy that allows Amazon Inspector to upload objects to your S3 bucket:

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3.
2. Choose the Amazon S3 bucket that you plan to use for exported findings.
3. Choose **Permissions**, and then choose **Bucket Policy**.
4. Copy the following example policy and paste it into the Amazon S3 bucket policy editor.
5. Replace the placeholder values in the example policy with the appropriate values for your environment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow inspector to perform Put and Delete actions on s3",
            "Effect": "Allow",
            "Principal": {
                "Service": "inspector2.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:inspector2:Region:123456789012:report/*"
                }
            }
        }
    ]
}
```

Note
If you're using Amazon Inspector in a manually-enabled Region, replace the value for the service with the Regional endpoint for the Region. For example, if you're using Amazon Inspector in the Middle East (Bahrain) (me-south-1) Region, replace `Service": "inspector2.amazonaws.com` with `inspector2.me-south-1.amazonaws.com`.

Exporting findings to an S3 bucket from the console

When you configure findings export, you must use an existing Amazon S3 bucket with a bucket policy that allows Amazon Inspector to export findings to the S3 bucket.

When you choose an existing S3 bucket in your account, you can specify a prefix that Amazon Inspector will prepend to the name of the resulting report. S3 will automatically generate any folder structure specified in the prefix. To store all Inspector reports sorted by account number and region, use a prefix like `/AWSLogs/111122223333/Amazon Inspector/Region`.

Important
The KMS key and S3 bucket for findings export must be in the same Region.

Before you complete the following steps, makes sure you have configured a KMS key and added a bucket policy to allow Amazon Inspector to create objects.

To configure findings export using an existing S3 bucket

1. Add a policy to the KMS key that Amazon Inspector will use to encrypt findings. For an example policy, see Granting Amazon Inspector permissions to a KMS key (p. 17).
2. Attach a policy granting Amazon Inspector permission to upload objects to an S3 bucket in any AWS account. For an example policy see Granting Amazon Inspector permissions to an S3 bucket (p. 18).
3. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
4. Choose **Findings**.
5. Choose **Export findings**.
6. (Optional) Choose filters for the report.
7. Choose the export file format for the report.
8. Enter the S3 bucket URI of the bucket you attached a policy to in Step 2. If you do not know the URI choose **Browse S3** to search for your bucket.
9. Enter the KMS key ARN or select from KMS keys within your current Region. The bucket and key must be in the same Region.
10. Choose **Export**.

To configure findings export using an existing S3 bucket in another account

1. Add a policy to the KMS key that Amazon Inspector will use to encrypt findings. For an example policy, see Granting Amazon Inspector permissions to a KMS key (p. 17).
2. Attach a policy granting Amazon Inspector permissions to upload objects to the S3 bucket in another account. For an example policy see, Granting Amazon Inspector permissions to an S3 bucket (p. 18).

   Note
   Use the account ID of the account that owns the S3 bucket in the policy.
3. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
4. Choose **Findings**.
5. Choose **Export findings**.
6. (Optional) Choose filters for the report.
7. Choose the export file format for the report.
8. Enter the S3 bucket URI of the bucket you attached a policy to in Step 2.
9. Enter the KMS key ARN. The bucket and key must be in the same Region.
10. Choose **Export**.

Export access error

If Amazon Inspector is not able to export findings after you request a report, an error message is displayed on the *Settings* page. This can happen when Amazon Inspector can no longer access the

target resource because the S3 bucket is deleted or the permissions to the bucket have changed. This can also happen when the KMS key used to encrypt data in the bucket becomes inaccessible.

If you receive this error message, review the information in this topic about how to enable and configure findings export. For example, review the key policy and confirm that the correct policy is applied to the KMS key that you chose for encryption.

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. Events are emitted on a best-effort basis.

> **Note**
> If your account is an Amazon Inspector delegated administrator, EventBridge events are published 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.

In order 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 enables EventBridge to send notifications for findings that Amazon Inspector generates to the target that is specified in the rule. For more information, see Amazon EventBridge rules in the EventBridge User Guide.

Event schema

The following is an example of the Amazon Inspector event format for a finding event.


```
{
  "version": "0",
  "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  "account": "555555555555",
  "time": "2019-10-29T02:36:48Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ecr:us-east-1:555555555555:repository/my-repo/
sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91"
  ],
  "detail": {
    "awsAccountId": "555555555555",
    "description": "Multiple integer overflows in libwebp allows attackers to have
 unspecified impact via unknown vectors.",
    "findingArn": "arn:aws:inspector2:us-east-1:555555555555:finding/FINDING_ID",
    "firstObservedAt": "2021-05-12T19:45:41.343Z",
    "inspectorScore": 3.3,
    "inspectorScoreDetails": {
      "adjustedCvss": {
        "adjustments": [],
        "cvssSource": "NVD",
        "score": 3.3,
        "scoreSource": "NVD",
        "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L",
        "version": "3.1"
```

```
      }
    },
    "lastObservedAt": "2021-05-12T19:45:41.343Z",
    "packageVulnerabilityDetails": {
      "cvss": [
        {
          "baseScore": 3.3,
          "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L",
          "source": "NVD",
          "version": "3.1"
        }
      ],
      "referenceUrls": [
        "https://bugzilla.redhat.com/show_bug.cgi"
      ],
      "source": "NVD",
      "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2016-9085",
      "vendorCreatedAt": "2017-02-03T15:59:00Z",
      "vendorSeverity": "LOW",
      "vulnerabilityId": "CVE-2016-9085",
      "vulnerablePackages": [
        {
          "arch": "AMD64",
          "epoch": 0,
          "name": "libwebp-dev",
          "packageManager": "OS",
          "release": "1",
          "sourceLayerHash": "sha256:hash",
          "version": "0.5.2"
        }
      ]
    },
    "remediation": {
      "recommendation": {
        "text": "Update all packages in the vulnerable packages section to their latest
 versions."
      }
    },
    "resources": [
      {
        "details": {
          "awsEcrContainerImage": {
            "architecture": "amd64",
            "imageHash":
 "sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91",
            "imageTags": [
              "2.0.01"
            ],
            "platform": "AMAZON_LINUX_2",
            "imagePushedAt": "2020-04-09T03:49:22Z",
            "registry": "555555555555",
            "repositoryName": "myrepo"
          }
        },
        "id": "arn:aws:ecr:us-east-1:555555555555:repository/myrepo/
sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91",
        "partition": "N/A",
        "region": "N/A",
        "type": "AWS_ECR_CONTAINER_IMAGE"
      }
    ],
    "severity": "LOW",
    "status": "ACTIVE",
    "title": "CVE-2016-9085 - libwebp-dev",
    "type": "PACKAGE_VULNERABILITY",
    "updatedAt": "2021-06-05T17:30:42.773Z"
```

```
    }
}
```

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.

Creating an EventBridge rule to notify you of Amazon Inspector findings

To increase the visibility of Amazon Inspector findings, you can use EventBridge with Amazon Inspector to set up automated finding alerts that are sent to a messaging hub. This topic shows you how to send findings alerts to email, Slack, or Amazon Chime by setting up an SNS topic and then connecting that topic to an EventBridge event rule.

Step 1. Setup 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

1. Sign in to the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
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_Email`**. Other details are optional.
4. Choose **Create Topic**. The Topic details for your new topic will open.
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

1. Sign in to the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
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_Slack`**. Other details are optional. Choose **Create topic** to finalize endpoint creation.

Configuring an AWS Chatbot client

1. Navigate to the AWS Chatbot console at https://console.aws.amazon.com/chatbot/.
2. From the **Configured clients** pane, select **Configure new client**.
3. Choose **Slack**, and then choose **Configure** to confirm.

   Note
   When choosing Slack, you must confirm permissions for AWS Chatbot to access your channel by selecting **allow**.
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. T
   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**.
   h. 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 Slack channel.
5. Select **Configure**.

Amazon Chime setup

Creating an SNS topic

1. Sign in to the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
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 finalize.

Configuring an AWS Chatbot client

1. Navigate to the AWS Chatbot console at https://console.aws.amazon.com/chatbot/.
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/.
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. Within the **Event source** pane select **AWS events or EventBridge partner events** .
6. In the **Event Pattern** pane for AWS service select `Inspector2`.
7. For **Event type** select `Inspector2 finding`, then select **Next**.

   Note
   You can also choose another option to set up rules for different types of events, for schema and explanations of available event types see Finding types in Amazon Inspector (p. 8).
8. In the **Select targets** page choose **AWS service**, then for **Select a target** choose **SNS topic**.
9. For **Topic**, select the name of the SNS topic you created in step 1. Then choose **Next**.
10. Add optional tags if needed and choose **Next**.
11. Review your rule then choose **Create rule**.

EventBridge for Amazon Inspector multi-account environments

If you are 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 will 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.

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 a resource. Amazon Inspector does not publish events for findings that you archive automatically using

suppression rules. Each event is a JSON object that conforms to the EventBridge schema for AWS events and contains a JSON representation of a finding. Because the findings data is structured as an EventBridge event, you can more easily monitor, process, and act upon findings by using other applications, services, and tools.

Topics

Amazon EventBridge base schema for Amazon Inspector

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

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Amazon Web Services 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 example of the basic schema for an EventBridge event for an Amazon Inspector finding. This event is 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. 20).

The following fields identify this as a **finding** event:

- `detail-type` is set to `Inspector2 Finding`.
- The `detail` section contains a `description` field that describes a finding.

```
{
  "version": "0",
  "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
  "detail-type": "Inspector2 Finding",
  "source": "aws.inspector2",
  "account": "555555555555",
  "time": "2019-10-29T02:36:48Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ecr:us-east-1:555555555555:repository/my-repo/
sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91"
  ],
  "detail": {
    "awsAccountId": "555555555555",
    "description": "Multiple integer overflows in libwebp allows attackers to have
 unspecified impact via unknown vectors.",
    "findingArn": "arn:aws:inspector2:us-east-1:555555555555:finding/FINDING_ID",
    "firstObservedAt": "2021-05-12T19:45:41.343Z",
    "inspectorScore": 3.3,
    "inspectorScoreDetails": {
      "adjustedCvss": {
        "adjustments": [],
        "cvssSource": "NVD",
        "score": 3.3,
        "scoreSource": "NVD",
        "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L",
        "version": "3.1"
      }
    },
    "lastObservedAt": "2021-05-12T19:45:41.343Z",
    "packageVulnerabilityDetails": {
      "cvss": [
        {
          "baseScore": 3.3,
          "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L",
          "source": "NVD",
          "version": "3.1"
        }
      ],
      "referenceUrls": [
        "https://bugzilla.redhat.com/show_bug.cgi"
      ],
      "source": "NVD",
      "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2016-9085",
      "vendorCreatedAt": "2017-02-03T15:59:00Z",
      "vendorSeverity": "LOW",
      "vulnerabilityId": "CVE-2016-9085",
      "vulnerablePackages": [
        {
          "arch": "AMD64",
          "epoch": 0,
          "name": "libwebp-dev",
          "packageManager": "OS",
          "release": "1",
          "sourceLayerHash": "sha256:hash",
          "version": "0.5.2"
        }
      ]
    },
    "remediation": {
      "recommendation": {
        "text": "Update all packages in the vulnerable packages section to their latest
 versions."
      }
    },
    "resources": [
      {
        "details": {
          "awsEcrContainerImage": {
            "architecture": "amd64",
            "imageHash":
 "sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91",
            "imageTags": [
              "2.0.01"
            ],
```

```
            "platform": "AMAZON_LINUX_2",
            "imagePushedAt": "2020-04-09T03:49:22Z",
            "registry": "555555555555",
            "repositoryName": "myrepo"
          }
        },
        "id": "arn:aws:ecr:us-east-1:555555555555:repository/myrepo/
sha256:7308b29228bde15a52a49b2f4a4cf95d5e2610e5ca67cdae32430e4b18effd91",
        "partition": "N/A",
        "region": "N/A",
        "type": "AWS_ECR_CONTAINER_IMAGE"
      }
    ],
    "severity": "LOW",
    "status": "ACTIVE",
    "title": "CVE-2016-9085 - libwebp-dev",
    "type": "PACKAGE_VULNERABILITY",
    "updatedAt": "2021-06-05T17:30:42.773Z"
  }
}
```

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 your resources. the following fields identify an **initial scan complete** event:

- `detail-type` is set to `Inspector2 Scan`.
- The `detail` section contains a `finding-severity-counts` field that details the number of findings in the **CRITICAL**, **HIGH**, and **MEDIUM** severity categories.

```
{
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2019-10-29T02:36:48Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:123456789012:repository/my-repo",
        "i-12345678"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "my-repo",
        "finding-severity-counts": {
           "CRITICAL": 10,
           "HIGH": 2,
           "MEDIUM": 9
         },
        "image-digest":
 "sha256:7f5b2640fe6fb4f46592dfd3410c4a79dac4f89e4782432e0378abcd1234",
        "image-tags": [],
        "instance-id": "i-12345678",
        "tags": {
            "cost-center": "engineering"
        }
```

```
    }
}
```

Scanning resources with Amazon Inspector

Amazon Inspector employs 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. For more information, see Managing findings in Amazon Inspector (p. 13).

When enabled, Amazon Inspector automatically discovers all eligible resources and begins continuous scans of those resources 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 enable Amazon Inspector for the first time, your account is automatically enrolled in all scan types. The following topics cover which resources are scanned, what initiates new scans, and how to configure scans for each resource type.

Topics

Scanning Amazon EC2 instances with Amazon Inspector

Amazon Inspector scans software applications installed on your EC2 instances for software vulnerabilities and network reachability issues. For more information on the types of findings produced for these issues, see Finding types in Amazon Inspector (p. 8).

Amazon Inspector initiates vulnerability scans of EC2 instances in the following situations:

- As soon as the EC2 instance is discovered by Amazon Inspector
- When you launch a new instance
- When you install new software on an existing instance
- When Amazon Inspector adds a new common vulnerabilities and exposures (CVE) item to its database

Network reachability scans for EC2 instances are performed once every 24 hours.

Amazon Inspector uses the AWS 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. For information about supported operating systems, see Supported operating systems and programming languages by Amazon Inspector (p. 74).

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

Configuring the SSM Agent

The SSM Agent is installed by default on EC2 instances created from some Amazon Machine Images (AMIs). For more information, see About SSM Agent. However, even if it is installed, you may need to enable the SSM Agent manually. Use the following procedure to configure the SSM Agent so that Amazon Inspector can discover your EC2 instance resources.

To enable the SSM Agent:

1. If it is not already installed by your operating system vendor, install the SSM Agent as explained in the Systems Manager User Guide.
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. Set up Systems Manager for your environment. For more information, see Setting up Systems Manager.
4. (Optional) Enable 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, see Create a Amazon Virtual Private Cloud endpoint.

Important
Amazon Inspector requires an 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 does not already exist.
Amazon Inspector also requires a resource data sync and automatically creates one called **InspectorResourceDataSync-do-not-delete** if one does not already exist. For more information, see Configuring resource data sync for Inventory.

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 more information, see Finding types in Amazon Inspector (p. 8)

When you enable 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**, provided as a free service by Amazon ECR, with **Enhanced scanning**, 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 view findings discovered using enhanced scanning at the image level, at each layer of the image, and in the Amazon ECR console. Additionally you can view and work with these findings in other services not available for basic scanning findings, including Security Hub, and Amazon EventBridge.

Enhanced scanning gives you a choice between continuous scanning or on-push scanning at the repository level. Continuous scanning includes on-push scans and automated rescans. On-push scanning scans only when you push an image. For both options you can refine the scanning scope through inclusion filters.

Automated rescans are triggered for container images based on whether you use the continuous or on-push option in your **Enhanced scanning** settings. Whenever Amazon Inspector adds a new CVE to its

database, eligible containers images in Amazon ECR repositories configured with continuous scanning are scanned in response.

> **Note**
> When ECR scanning is first enabled Amazon Inspector will begin scanning all images pushed within the last 30 days. To include images older than 30 days in Amazon Inspector ECR scans you must delete and re-push them.

Supported operating systems and media types

For information about supported operating systems, see Supported operating systems and programming languages by Amazon Inspector (p. 74).

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**
> **The following are not supported:**
>
> - Scratch images are not supported.
> - `DockerV2ListMediaType` images are not supported.

Configuring enhanced scanning for Amazon ECR repositories

When Amazon Inspector scans for Amazon ECR are enabled, the default scanning option is **Enhanced scanning** set to **Continuously scan all repositories**. See the previous section for more information about scanning options.

To change your enhanced scanning settings:

You can modify the coverage and scope of your Amazon ECR container image scans through the Amazon ECR console.

1. Open the Amazon ECR console at https://console.aws.amazon.com/ecr/.
2. Select the Region that contains the repositories that you want to scan.
3. From the navigation bar, choose **Private Registry**.
4. Within the **Scanning** pane, choose **Edit**.
5. Under **Scanning configuration**, choose **Enhanced scanning**.
6. Select **Continuously scan all repositories** for complete Amazon Inspector scan coverage for all repositories, or choose **Scan on push all repositories** to run scans only when you push an image.
7. (Optional) Specify which repositories to include in scans for continuous or on-push scans by entering the repository names in the input box and selecting **Add filter**.
   - After you add inclusion filters, you can select **Preview repository matches** to see which repositories will be included.
8. Choose **Save**.
9. (Recommended) Repeat these steps in each Region for which you want to enable Amazon Inspector scans for Amazon ECR repositories.

Changing the ECR automated re-scan duration

The 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 will no longer monitor the image. When Amazon Inspector stops monitoring an image the scan status of the image is changed to `inactive` with a reason code of `expired`, and all associated findings for the image are scheduled to be closed.

You can set the ECR automated re-scan duration in Amazon Inspector to best suit your environment. For example, if you build images frequently a shorter scan duration is sufficient. However, if you continue to use images for long periods of time you can choose a longer scan duration. The following scan duration options are available:

- 30 days
- 180 days
- Lifetime

> **Note**
> The default scan duration for new accounts and new accounts added through organizations is **Lifetime**. This means images are scanned until they are deleted.

To change the ECR automated re-scan duration:

1. Expand **Settings** in the navigation panel and then select **General**.
2. Under **ECR automated re-scan duration** choose a setting.
3. Select **Save**. Your new setting applies immediately.

When you increase the duration from a shorter value to a longer value, such as 30 days to 180 days, Amazon Inspector applies the change to all images actively being scanned in repositories configured for continual scanning. However, images that are already expired remain expired.

When you decrease the duration from a longer value to a shorter value, such as 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.

Disabling Scans

You can disable Amazon ECR container image scanning or EC2 instance scanning at any time. Disabling all scan types for an account disables Amazon Inspector for that account in that Region. For more information see Disabling Amazon Inspector (p. 73).

When you disable Amazon ECR container image scanning for any account the Amazon ECR scan type for that account changes from **Enhanced scanning** with Amazon Inspector to **Basic scanning** with Amazon ECR.

To disable scans

To complete this procedure for a multi-account environment, follow the steps while signed in as the Amazon Inspector delegated administrator. Member accounts cannot disable scans.

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. Use the Region selector in the upper right to specify the Region where you want to disable scans.

3. In the navigation pane, choose **Settings**, and then choose **Account Management**.
4. Choose the **Accounts** tab to see the scan status of an account.
5. Select the check box for the account or accounts for which you want to disable scans.
6. From the **Actions** drop down, select the scan type to disable.

Understanding the Amazon Inspector dashboard

The Amazon Inspector dashboard provides a snapshot of aggregated statistics for your Amazon 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 EC2 instances 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:

1. Open the Amazon Inspector console https://console.aws.amazon.com/inspector/v2/home.
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 Amazon 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 and Amazon ECR images 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 enabled, 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 your Amazon Inspector coverage (p. 37).

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
- Repositories

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. 8).

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:

- Container findings
- EC2 findings
- Network reachability

Risk-based remediations

The **Risk-based remediations** section shows the top five software packages with critical vulnerabilities that impact 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 impacted 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 impacted AMI.

Assessing your Amazon Inspector coverage

You can get statistics on how much of your environment is covered by Amazon Inspector scanning from the **Account Management** page. You can also use this page to manage which resources and accounts are actively scanned by Amazon Inspector.

To view Amazon Inspector coverage for accounts and resources in your environment

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. In the navigation pane, under **Settings**, choose **Account Management**.
3. From the Account Management page, choose from the three different coverage views: **Accounts**, **Instances**, and **Repositories**.

Viewing coverage for accounts

For an individual account that is not part of Organizations or is not a delegated administrator account, the **Accounts** view displays account information and enabled resource scans. From this view, resource scanning can be enabled or disabled. For more information about enabling scans, see Scanning resources with Amazon Inspector (p. 29).

For a delegated administrator account, the **Accounts** view shows organization-level automatic enablement settings, lists all accounts in the organization, and shows which accounts have Amazon Inspector enabled with the resource scanning types enabled for each account. From this view, delegated administrators can change the automatic enablement settings or enable and disable resource scanning for member accounts. For more information about enabling scans, see Scanning resources with Amazon Inspector (p. 29). For information on adding or removing member accounts from the list, see Managing multiple accounts in Amazon Inspector with AWS Organizations (p. 39).

Viewing coverage for instances

The **Instances** view displays all Amazon EC2 instances within your environment and organizes them into groups in the following tabs:

- **All** – Shows all instances in your environment along with AWS account identifier and scan status.
- **Scanning** – Shows instances that Amazon Inspector is actively scanning.
- **Not scanning** – Shows instances in your environment that Amazon Inspector is not actively scanning. Amazon Inspector uses Systems Manager SSM Agents to automatically monitor your EC2 instances for vulnerabilities. If your instances do not have the SSM Agent running, do not have an IAM role supporting Systems Manager, or are not running a supported operating system, then they cannot be monitored. See the **Reason** column in this tab for more information about why an instance is not being scanned.

Viewing coverage for repositories

The **Repositories** view displays all Amazon ECR repositories within your environment and organizes them into groups in the following tabs:

- **All** – Shows all repositories in your environment.
- **Enabled** – Shows repositories which Amazon Inspector is monitoring.
- **Not enabled** – Shows repositories in your environment that Amazon Inspector is not monitoring. See the **Reason** column in this tab for more information about why a repository is not being scanned.

In each view, you can select the repository name to view the scan status of each image in the repository. The resulting view shows the type of scanning enabled for the repository and image tags, date pushed, image digest, scan status, and the number of findings for each image.

Viewing coverage for container images

The **Images** view displays all Amazon ECR container images within your environment and organizes them into groups in the following tabs:

- **All** – Shows all images in your environment along with the Amazon ECR repository they reside in, the AWS account that owns the repository and scan status.
- **Enabled** – Shows images that reside in repositories where Amazon Inspector scans have been enabled.
- **Not enabled** – Shows images in your environment that Amazon Inspector is not actively scanning. These images may reside in repositories where Amazon Inspector scans have not been enabled, or where your filtering rules prevent that repository from being scanned. Additionally the status is **Not enabled** when the image has not been pushed in over 30 days. Container images residing in Amazon ECR repositories that are configured for continuous scanning are scanned for 30 days after they are pushed to the repository.

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 enabling or disabling scans for member accounts, viewing aggregated finding data from the entire organization, and the creation and management of suppression rules.

Topics

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 filters that are applied to member accounts. For more information about suppression filters, see Suppressing Amazon Inspector findings with suppression rules (p. 14).

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

- View and manage the status of Amazon Inspector for associated accounts, including enabling and disabling Amazon Inspector
- Enable or disable 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
- Enable Amazon ECR enhanced scanning for all members of the organization
- View resource coverage for the entire organization
- Defines 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 the member account had set previously. All accounts in the organization share the ECR automated re-scan duration of the delegated administrators and different re-scan durations cannot be set for individual accounts.

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

- Enable 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.

> **Note**
> Once enabled, Amazon Inspector can only be disabled 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 enable 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 disable Amazon Inspector for member accounts.

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

Your AWS Organization must have all features enabled.

All features is the default setting for AWS Organizations. If it is not enabled see Enabling all features in your organization.

Permissions required to designate a delegated administrator

You must have permission to enable 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 enabled for both the Organizations management account and the chosen delegated administrator account.

> **Note**
> Only the Organizations management account can designate a delegated administrator.

Enabling 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. 61). 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:

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 Region selector in the upper right to specify the Region in which you want to designate an administrator.
3. Under **Enable Inspector** enter the twelve-digit AWS account ID of the 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.

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

Enabling Amazon Inspector scans for member accounts

As a delegated administrator for your organization you can enable Amazon EC2 scanning, Amazon ECR scanning, or both, for any member associated with the AWS Organizations management account.

When you enable scans for a member account, that account becomes associated to the delegated administrator, Amazon Inspector is automatically enabled, and scans of the chosen type are started immediately. For information on what resources can be scanned and configuring scans see Scanning resources with Amazon Inspector (p. 29).

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

To automatically enable 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 Region selector in the upper right to specify the Region in which you want to designate an administrator.
3. In the navigation panel, choose **Account Management**. The accounts table displays all of 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 **Enable** and select your preferred scan type option from the list.

   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 **Auto-enable** feature and select the scan types to enable those scans for any new members who are added to your organization.
6. (Recommended) Repeat these steps in each Region in which you want to enable scans for your members.

The auto-enable feature enables 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 5000, the auto-enable feature is automatically turned off. If an account is removed and the total number of members decreases to fewer than 5000, then the auto-enable feature is automatically reactivated.

To selectively enable 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 Region selector in the upper right to specify the desired Region.
3. From the **Account Management** page choose the accounts that you want to add as members by selecting the check box for those accounts.
4. Select **Enable**.
5. From the **Enable** menu, choose the scan types to enable for the selected accounts. You can choose from the following scan options:

   - **All Scanning** to enable both Amazon EC2 and Amazon ECR scans
   - **EC2 Scanning** to enable scans of Amazon EC2 instances
   - **Container Scanning** to enable scans of Amazon ECR container images
6. (Recommended) Repeat these steps in each Region in which you want to enable scans for your members.

To enable scanning as a member account:

If your AWS Organizations management account has delegated an administrator for Amazon Inspector you can enable 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, then use the Region selector in the upper right to specify the desired Region.
3. From the **Account Management** page and choose your account from the table.
4. Select the **Enable** button.
5. From the **Enable** menu choose the scan types to enable. You can choose from the following scan options:
   - **All Scanning** to enable both Amazon EC2 and Amazon ECR scans
   - **EC2 Scanning** to enable scans of Amazon EC2 instances
   - **Container Scanning** to enable scans of Amazon ECR container images
6. (Recommended) Repeat these steps in each Region in which you want to enable 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 enable and manage Amazon Inspector for these accounts. You can add these accounts as members again later.

> **Note**
> Disassociating an account does not disable 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, then use the Region selector in the upper right to specify the desired Region.
3. In the navigation pane, choose **Settings** and then choose **Account Management**.
4. Select the check box for the accounts to disassociate.
5. Select the **Actions** button, then choose **Disassociate account** from the menu.
6. (Recommended) Repeat these steps in each AWS 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 disable 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 a 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, then use the Region selector in the upper right to specify the desired Region.
3. Select **Settings** from the navigation bar.
4. Select **Remove** from the **Delegated administrator** pane and confirm your action on the next pane.
5. Repeat in each Region in which you registered this delegated administrator.

To associate members to 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, then use the Region selector in the upper right to specify the desired Region.
3. Select **Account Management** under **Settings** in the navigation panel.
4. Select all of the listed accounts in your organization using the top check box.
5. Select the **Actions** button, then choose **Add member** from the menu.
6. Repeat in each other Region in which you registered this delegated administrator.

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

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 user accounts with 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 recommend TLS 1.2 or later.
- 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 personal 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 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 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.

Encryption at rest

Amazon Inspector securely stores your data at rest using AWS encryption solutions. 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 an Amazon Inspector-managed key from AWS Key Management Service (AWS KMS).

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 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, AWS Amazon ECR 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

- AWS managed policies for Amazon Inspector (p. 58)
- Using service-linked roles for Amazon Inspector (p. 61)
- Troubleshooting Amazon Inspector identity and access (p. 62)

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. 62).

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 employees 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. 50).

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. 55).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also 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 Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then

securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

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:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.
- **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 IAM 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. 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 what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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 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

IAM feature	Amazon Inspector support
Identity-based policies (p. 51)	Yes
Resource-based policies (p. 51)	No
Policy actions (p. 52)	Yes
Policy resources (p. 52)	Yes
Policy condition keys (p. 53)	Yes
ACLs (p. 53)	No
ABAC (tags in policies) (p. 54)	Partial
Temporary credentials (p. 54)	Yes
Principal permissions (p. 54)	Yes
Service roles (p. 55)	Yes
Service-linked roles (p. 55)	No

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

Identity-based policies for Amazon Inspector

Supports identity-based policies	Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see 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. 55).

Resource-based policies within Amazon Inspector

Supports resource-based policies	No

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

based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. 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:

```
awes
```

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

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

To view examples of Amazon Inspector identity-based policies, see Identity-based policy examples for Amazon Inspector (p. 55).

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. 55).

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. 55).

Access control lists (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.

Attribute-based access control (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.

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

Supports temporary credentials	Yes

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

Supports principal permissions	Yes

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

Supports service roles	Yes

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	No

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 IAM 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, IAM users and roles don't have permission to create or modify Amazon Inspector resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform actions on the resources that they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

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

Topics

Policy best practices

Identity-based policies are very powerful. They 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 using AWS managed policies** – To start using Amazon Inspector quickly, use AWS managed policies to give your employees the permissions they need. These policies are already

available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.

- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition 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 (IAM 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 you're trying to perform.

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

Allow users to view their own permissions

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

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

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow 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": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "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 policies for Amazon Inspector

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions 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 images, analyze your VPC network, and describe accounts associated with your organization. For more information, see Using service-linked roles for Amazon Inspector (p. 61).
- `organizations` – Allows administrators to use IAM Access Analyzer for an organization in AWS Organizations. After enabling trusted access for IAM Access Analyzer in AWS Organizations, members of the delegated administrator account can manage settings and view findings across their organization.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "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 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.

- `organizations` – Allows details about Amazon Inspector coverage for an organization to be viewed.

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

AWS managed policy: AmazonInspector2ServiceRolePolicy

You can't attach `AmazonInspector2ServiceRolePolicy` 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. 61).

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 page.

Change	Description	Date
AmazonInspector2ReadOnlyAccess (p. 59) – New policy	Amazon Inspector added a new policy to allow read-only access to Amazon Inspector functionality.	January 21, 2021
AmazonInspector2FullAccess (p. 58) – New policy	Amazon Inspector added a new policy to allow full access to Amazon Inspector functionality.	November 29, 2021
AmazonInspector2ServiceRolePolicy (p. 61) – New policy	Amazon Inspector added a new policy to allow Amazon Inspector to perform actions in other services on your behalf.	November 29, 2021
Amazon Inspector started tracking changes	Amazon Inspector started tracking changes for its AWS managed policies.	November 29, 2021

Using service-linked roles for Amazon Inspector

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

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

You can delete a service-linked role only after first deleting their 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 Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon Inspector

Amazon Inspector uses the service-linked role named **AWSServiceRoleForAmazonInspector2**.

The AWSServiceRoleForAmazonInspector2 service-linked role trusts the following services to assume the role:

- `inspector2.amazonaws.com`

The permissions policy named AmazonInspector2ServiceRolePolicy allows Amazon Inspector to perform tasks such as:

- Use 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.
- Use Amazon ECR actions to retrieve information about your container images.
- Use AWS Organizations actions to describe associated accounts.

For details about updates to the **AWSServiceRoleForAmazonInspector2** policy, see Amazon Inspector updates to AWS managed policies (p. 60).

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

Creating a service-linked role for Amazon Inspector

You don't need to manually create a service-linked role. When you enable the service 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 you create a service-linked role, you cannot change the name of the role because various

entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a service-linked role for Amazon Inspector

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 disable Amazon Inspector in each AWS Region where it's enabled. When you disable Amazon Inspector, it doesn't delete the role for you. Therefore, if you enable Amazon Inspector again, it can use the existing role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

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 enable Inspector, 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, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To manually delete the service-linked role using IAM

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

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

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 does not have the fictional `awes:`*`GetWidget`* permissions.

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

In this case, Mateo asks his administrator to update his policies to allow him to access the *`my-example-widget`* resource using the `awes:`*`GetWidget`* action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies 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 granted by a service role. Mary does not have permissions to pass the role to the service.

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

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access Amazon Inspector

To allow others to access Amazon Inspector, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon Inspector.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

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. 50).
- 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*.

Compliance validation for Amazon Inspector

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

To learn whether Amazon Inspector or other AWS services are in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

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

Your compliance responsibility when using 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 Whitepaper – 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 that helps you check your compliance with security industry standards and best practices.
- 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 the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Amazon Inspector through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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.

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 the following monitoring tools to watch Amazon Inspector, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and 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 a user, 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 code calls to the Amazon Inspector API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Inspector. If you don't configure a trail, you can still view the most recent events 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 it was made, and additional details.

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:

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

All Amazon Inspector actions are logged by CloudTrail and are documented in the Amazon Inspector API Reference. For example, calls to the `ACTION_1`, `ACTION_2` and `ACTION_3` 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 or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see 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 and includes 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.

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. 68).

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 of your integrated AWS services, and AWS Partner Network products. Enabling Security Hub with Amazon Inspector automatically allows Amazon Inspector findings data to be ingested by Security Hub.

For more information about using Security Hub with Amazon Inspector see Amazon Inspector integration with AWS Security Hub (p. 69).

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 enable **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.

Enabling the integration

You can enable the integration by enabling 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.

For more information on enabling the integration through Amazon Inspector, see Scanning resources with Amazon Inspector (p. 29).

For information on enabling and configuring **Enhanced scanning** in Amazon ECR, see Enhanced Scanning in the Amazon ECR user guide.

Using the integration with a multi-account environment

If you are a member in a multi-account environment, you can enable enhanced scanning through Amazon ECR. However, once enabled, it can only be disabled by your Amazon Inspector delegated administrator. If it is disabled, it reverts to basic scanning. For more information, see Changing the ECR automated re-scan duration (p. 32).

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 enables 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.

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

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector: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": "2021-09-02T19:01:56.725Z",
  "LastObservedAt": "2021-10-13T05:43:34.982Z",
  "CreatedAt": "2021-09-02T19:01:56.725Z",
  "UpdatedAt": "2021-10-13T05:43:34.982Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2019-19882 - passwd, login",
  "Description": "shadow 4.8, in certain circumstances affecting at least Gentoo, Arch
 Linux, and Void Linux, allows local users to obtain root access because setuid programs
 are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-
libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM
 configuration suitable for use with setuid account management tools. This combination
 leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel,
 usermod) that can easily be used by unprivileged local users to escalate privileges to
 root in multiple ways. This issue became much more relevant in approximately December 2019
 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the
 upstream Makefile which is now included in the release version 4.8).",
  "Remediation": {
    "Recommendation": {
      "Text": "Update all packages in the vulnerable packages section to their latest
 versions."
    }
  },
  "ProductFields": {
    "aws/inspector/score": "7.8",
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/scoreDetails/scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/
A:H",
    "aws/inspector/scoreDetails/version": "3.1",
    "aws/inspector/packageVulnerabilityDetails/vulnerablePackages/1/sourceLayerHash":
 "sha256:EXAMPLE_HASH",
    "aws/inspector/scoreDetails/score": "7.8",
    "aws/inspector/scoreDetails/scoreSource": "NVD",
    "aws/inspector/packageVulnerabilityDetails/vulnerablePackages/2/sourceLayerHash":
 "sha256:EXAMPLE_HASH",
    "aws/inspector/resources/1/resourceDetails/awsEcrContainerImageDetails/platform":
 "DEBIAN_10",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEcrContainerImage",
      "Id": "123456789012/account-test/sha256:EXAMPLE_HASH",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsEcrContainerImage": {
          "RegistryId": "123456789012",
          "RepositoryName": "account-test",
          "Architecture": "amd64",
          "ImageDigest": "sha256:EXAMPLE_HASH",
```

```
        "ImageTags": [
          "latest"
        ],
        "ImagePublishedAt": "2021-09-02T19:01:48Z"
      }
    }
  }
],
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"Vulnerabilities": [
  {
    "Id": "CVE-2019-19882",
    "VulnerablePackages": [
      {
        "Name": "passwd",
        "Version": "4.5",
        "Epoch": "1",
        "Release": "1.1",
        "Architecture": "AMD64"
      },
      {
        "Name": "login",
        "Version": "4.5",
        "Epoch": "1",
        "Release": "1.1",
        "Architecture": "AMD64"
      }
    ],
    "Cvss": [
      {
        "Version": "2.0",
        "BaseScore": 6.9,
        "BaseVector": "AV:L/AC:M/Au:N/C:C/I:C/A:C"
      },
      {
        "Version": "3.1",
        "BaseScore": 7.8,
        "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H"
      }
    ],
    "Vendor": {
      "Name": "NVD",
      "Url": "https://nvd.nist.gov/vuln/detail/CVE-2019-19882",
      "VendorSeverity": "HIGH",
      "VendorCreatedAt": "2019-12-18T16:15:00Z",
      "VendorUpdatedAt": "2020-08-25T15:15:00Z"
    },
    "ReferenceUrls": [
      "https://security.gentoo.org/glsa/202008-09",
      "https://bugs.archlinux.org/task/64836",
      "https://bugs.gentoo.org/702252"
    ]
  }
],
"FindingProviderFields": {
  "Severity": {
    "Label": "HIGH"
  },
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ]
}
```

```
}
```

Enabling and configuring the integration

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

When you enable both Amazon Inspector and Security Hub, the integration is enabled 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 Disabling and enabling the flow of findings from an integration (console) or Disabling the flow of findings from an integration (Security Hub API, AWS CLI) in the *AWS Security Hub User Guide*.

Disabling Amazon Inspector

You can disable Amazon Inspector in any Region by using the Amazon Inspector console or API. Amazon Inspector can be disabled either through the process outlined at the end of this topic or whenever all Amazon Inspector scans are disabled for an account. For information about disabling scans, see Scanning resources with Amazon Inspector (p. 29).

After Amazon Inspector is disabled in an account, all scan types are disabled for that account in that AWS Region. Additionally, all Amazon Inspector scan settings, suppression rules, filters and findings for the account in that Region are deleted.

You aren't charged for using Amazon Inspector while it's disabled for your account in that Region. After you disable Amazon Inspector, you can choose to re-enable it at a later time.

> **Note**
> Before you disable Amazon Inspector, we recommend that you export your findings. For more information, see Exporting findings reports with Amazon Inspector (p. 16).

Prerequisites

Depending on your account type, you may need to take additional steps before disabling Amazon Inspector. See the following cases:

- If you have a stand-alone Amazon Inspector account, you can disable it at any time.
- If you are a member account in an Amazon Inspector multi-account environment, you cannot disable your own service. You must contact the delegated administrator for your organization to disable your service.
- If you are a delegate administrator account, you must disassociate all of your member accounts before you can disable Amazon Inspector in your own account. For more information, see Disassociating member accounts in Amazon Inspector (p. 43).

  > **Note**
  > Disassociating an account does not disable Amazon Inspector for that account.

  > **Note**
  > When you disable Amazon Inspector as a delegated administrator, the auto-enable feature is deactivated for your organization.

To disable Amazon Inspector

1. Open the Amazon Inspector console at https://console.aws.amazon.com/inspector/v2/home.
2. Select the Region in which you want to disable Amazon Inspector.
3. In the navigation pane, choose **Settings**.
4. Choose **Disable Inspector**.
5. When prompted for confirmation, select **Disable**, then confirm your decision by selecting **Disable Amazon Inspector**.
6. (Recommended) Repeat these steps in each Region for which you want to disable Amazon Inspector.

Supported operating systems and programming languages by Amazon Inspector

Supported operating systems

Amazon Inspector sources over 50 data-feeds to generate findings for CVEs including **vendor security advisories**, **NVD**, **MITRE**, **other open-source feeds**, **internal research**, and **licensed data feeds**.

The operating systems supported by Amazon Inspector, along with the **vendor security advisories** supported for that system, are listed below:

Amazon EC2 scanning

Operating system	Major version	Minor version	Vendor Advisories
Amazon Linux AMI (AL1)	N/A	N/A	ALAS
Amazon Linux (AL2)	2	N/A	ALAS
CentOS Linux (CentOS)	7	X	CESA
CentOS Linux (CentOS)	8	X	RHSA
Debian Server (Stretch)	9	x	DSA
Debian Server (Buster)	10	X	DSA
Debian Server (Bullseye)	11	X	DSA
Oracle Linux (Oracle)	6	X	ELSA
Oracle Linux (Oracle)	7	X	ELSA
Oracle Linux (Oracle)	8	X	ELSA
Red Hat Enterprise Linux (RHEL)	7	X	RHSA
Red Hat Enterprise Linux (RHEL)	8	X	RHSA
SUSE Linux Enterprise Server (SLES)	12	X	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15	X	SUSE CVE
Ubuntu (Trusty)	14	04 (ESM)	USN
Ubuntu (Xenial)	16	04 (ESM)	USN

Ubuntu (Bionic)	18	04 (LTS)	USN
Ubuntu (Focal)	20	04 (LTS)	USN
Ubuntu (Groovy)	20	10	USN
Ubuntu (Hirsute)	21	04	USN
Ubuntu (Impish)	21	10	USN
Ubuntu (Jammy)	22	04 (LTS)	USN

Amazon ECR scanning

Operating system	Major version	Minor version	Vendor Advisories
Alpine Linux (Alpine)	3	12	Alpine Secdb
Alpine Linux (Alpine)	3	13	Alpine Secdb
Alpine Linux (Alpine)	3	14	Alpine Secdb
Alpine Linux (Alpine)	3	15	Alpine Secdb
Amazon Linux (AL1)	2018.03	N/A	ALAS
Amazon Linux (AL2)	2	N/A	ALAS
CentOS Linux (CentOS)	7	X	CESA
CentOS Linux (CentOS)	8	X	RHSA
Debian Server (Stretch)	9	x	DSA
Debian Server (Buster)	10	X	DSA
Debian Server (Bullseye)	11	X	DSA
Oracle Linux (Oracle)	6	X	ELSA
Oracle Linux (Oracle)	7	X	ELSA
Oracle Linux (Oracle)	8	X	ELSA
Red Hat Enterprise Linux (RHEL)	7	X	RHSA
Red Hat Enterprise Linux (RHEL)	8	X	RHSA
OpenSUSE Leap (SUSE Leap)	15	2	SUSE CVE
OpenSUSE Leap (SUSE Leap)	15	3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12	X	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15	X	SUSE CVE

Ubuntu (Trusty)	14	04 (ESM)	USN
Ubuntu (Xenial)	16	04 (ESM)	USN
Ubuntu (Bionic)	18	04 (LTS)	USN
Ubuntu (Focal)	20	04 (LTS)	USN
Ubuntu (Groovy)	20	10	USN
Ubuntu (Hirsute)	21	04	USN
Ubuntu (Impish)	21	10	USN
Ubuntu (Jammy)	22	04 (LTS)	USN

Supported programming languages

Amazon Inspector supports the following programming languages:

- C#
- Golang
- Java
- Javascript
- PHP
- Python
- Ruby
- Rust

Quotas for Amazon Inspector

Your AWS account has the following quotas for Amazon Inspector per Region.

Resource	Default	Comments
Suppression rules	500	The maximum number of saved suppression rules per AWS account per Region. You cannot request a quota increase.
Amazon EC2 network findings	10,000	The maximum number of Amazon EC2 network findings per AWS account. You cannot request a quota increase.
Member accounts	5000	The maximum number of member accounts associated with an Amazon Inspector account. This limit is based on AWS Organizations, see Quotas for AWS Organizations.

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*.

Document history for the Amazon Inspector User Guide

update-history-change	update-history-description	update-history-date
Amazon Inspector now supports changing your ECR automated re-scan duration setting	The 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.	January 25, 2022
New service and guide (p. 1)	This is the initial release of the *Amazon Inspector User Guide*.	November 29, 2021

AWS glossary

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