What is Amazon Inspector?

Amazon Inspector is an automated security assessment service that helps you test the security state of your applications running on Amazon EC2.

Show less

What can I do with Amazon Inspector?

Amazon Inspector allows you to automate security vulnerability assessments throughout your development and deployment pipeline or against static production systems. This allows you to make security testing a more regular occurrence as part of development and IT operations. Amazon Inspector is agent-based, API-driven, and delivered as a service to make it easy to deploy, manage, and automate.

Show less

What makes up the Amazon Inspector service?

Amazon Inspector consists of an Amazon-developed agent that is installed in the operating system of your Amazon EC2 instances and a security assessment service that uses telemetry from the agent and AWS configuration to assess instances for security exposures and vulnerabilities.

Show less

assessment run, the agent monitors, collects, and analyzes behavioral data (telemetry) within the specified target, such as the use of secure channels, network traffic among running processes, and details of communication with AWS services. Next, the agent analyzes the data and compares it against a set of security rule packages specified in the assessment template used during the assessment run. A completed assessment run produces a list of findings - potential security issues of various severity.

Show less

Is there any performance impact during an Amazon Inspector assessment run?

Amazon Inspector and the Amazon Inspector Agent have been designed for minimal performance impact during the assessment run process.

Show less

What is an assessment target?

An assessment target represents a collection of AWS resources that work together as a unit to help you accomplish your business goal(s). Amazon Inspector evaluates the security state of the resources that constitute the assessment target. You create an assessment target by using Amazon EC2 tags, and you can then define these tagged resources as an assessment target for an assessment run defined by the assessment template.

template and assessment run. Amazon Inspector has many rules packages including common vulnerabilities and exposures (CVE), Center for Internet Security (CIS) Operating System configuration benchmarks, and security best practices. See the Amazon Inspector documentation for a full list of rules packages available.

Show less

Can I define my own rules for assessment templates?

No. Only the pre-defined rules will initially be allowed for assessment runs. However, over time we are exploring the inclusion of both premium rules sets from vendors in the AWS Marketplace and self-developed custom rules.

Show less

Which applications can Inspector analyze for vulnerabilities?

Amazon Inspector finds applications by querying the package manager or software installation system on the operating system where the agent is installed. This means that software that was installed through the package manager is assessed for vulnerabilities. The version and patch level of software that is not installed through these methods is not recognized by Inspector. For example, software installed via apt, yum, or Microsoft Installer will be assessed by Inspector.

packages tested, the rules that generated findings, and detailed information about each of these rules along with the list of instances that failed the check. The full report contains all the information in the findings report, and additionally provides the list of rules that were checked and passed on all instances in the assessment target.

Show less

What happens if some of my targets are unavailable when I run an assessment?

Amazon Inspector will gather vulnerability data for all available targets configured for the assessment template and return any appropriate security findings for the available targets. If there are no available targets for the assessment template when the run is started, the system will report that the assessment could not be run and will return the following notification: “The assessment run could not be executed at this time as there are no targeted instances available for the selected assessment template.”

Show less

How do Targets become unavailable?

Targets in an assessment could be unavailable for a number of reasons, such as: the EC2 instance is down or unresponsive; the Tagged (targeted) instance does not have the Amazon Inspector Agent installed; the installed Amazon Inspector Agent is unavailable or cannot return vulnerability data.

The price of each individual agent-assessment is based on a tiered pricing model. As you move up the volume of agent-assessments in a given billing period, you pay a lower price per agent-assessment. For example, the first two tiers of agent-assessment pricing are:

> First 250 agent-assessments = $0.30 per agent-assessment
> Next 750 agent-assessments = $0.25 per agent-assessment

So for our example above of 331 total agent-assessments in a given billing period, you would be charged $0.30 for the first 250 and $0.25 for the next 81, or $95.25 total for the billing period. See the Amazon Inspector pricing page for the full pricing table.

Show less

Is there a free trial for Amazon Inspector?

Yes. Amazon Inspector offers the first 250 agent-assessments at no cost for the first 90 days of using the service. All AWS accounts new to the Amazon Inspector service are eligible.

Show less

What Operating Systems does Amazon Inspector support?

Please see the Amazon Inspector documentation for a current list of supported operating systems.

Runtime Behavior Analysis rules package, your Linux instance must have a kernel version that is supported for Amazon Inspector. An up-to-date list of Linux kernel versions that are supported for Amazon Inspector assessments is available here.

Show less

Amazon Inspector sounds great, how do I get started?

Simply sign up for Amazon Inspector from the AWS Management Console. Once signed up, you install the appropriate Amazon Inspector Agent on your Amazon EC2 instances, create a new assessment template, select the rules packages you want to use, and schedule an assessment run. Once it completes, the system will generate a findings report on any issues it identified for your environment.

Show less

Does the Amazon Inspector Agent have to be installed on all of the EC2 instances I wish to assess?

Yes. During an assessment run, the Amazon Inspector Agent monitors the behavior of the operating system and applications of the EC2 instance it's installed on, collects configuration and behavioral data, and passes the data to the Amazon Inspector service.

Show less

You can view the status of the Amazon Inspector Agent for all the EC2 instances in your assessment target by using the 'Preview Targets' functionality available in the Inspector console and through the PreviewAgents API query. Agent status includes whether the agent is installed on the EC2 instance and the health of the agent. Along with the Inspector Agent status on the targeted EC2 instance, the instance ID, public hostname, and public IP address (if defined) are also displayed, along with links into the EC2 console for each instance.

Show less

Does Amazon Inspector access other AWS services in my account?

Amazon Inspector needs to enumerate your EC2 instances and tags to identify the instances specified in the assessment target. Amazon Inspector gets access to these through a service-linked role that is created on your behalf when you get started with Inspector as a new customer or in a new region. The Inspector service-linked role is managed by Amazon Inspector, so you don't have to worry about inadvertently revoking permissions required by Amazon Inspector. For some existing customers, an IAM role that was registered while getting started with Inspector might be used for accessing other AWS services until the Inspector service-linked role is created. You can create the Inspector service-linked role through the Inspector console's dashboard page.

Show less

I would like to automate the assessment of my infrastructure on a regular basis. Do you provide an automated way to submit assessments?

Yes. Amazon Inspector provides a full API allowing automatic creation of application environments, creation of assessments, evaluation of policies, creation of policy exceptions, and filters as well as retrieval of the results.

Show less

Can I schedule security assessments to run at certain dates and times?

Yes. Amazon Inspector assessments can be triggered by any Amazon CloudWatch Event. You can set up a recurring Schedule event with either a simple fixed recurring rate or a more detailed Cron expression.

Show less

Can I trigger security assessments to run based on an event?

Yes. You can use Amazon CloudWatch Events to create event patterns which monitor other AWS services for actions to trigger an assessment. For example, you can create an event which monitors AWS Auto Scaling for new Amazon EC2 Instances being launched, or monitors AWS CodeDeploy notifications for when a code deployment has been successfully completed. Once CloudWatch Events have been configured against Amazon Inspector templates, these assessment events will be

Where can I find metrics information on my Amazon Inspector assessments?

Amazon Inspector automatically publishes metrics data on your assessments to Amazon CloudWatch. If you are a CloudWatch user, your Inspector assessment statistics will automatically be populated to CloudWatch. The Inspector metrics that are currently available are: number of assessment runs, agents targeted, and findings generated. For more details, see the Amazon Inspector documentation for details on the assessment metrics published to CloudWatch.

Show less

Can Amazon Inspector be integrated with other AWS services for logging and notifications?

Amazon Inspector integrates with Amazon SNS to provide notification for various events such as monitoring milestones, failures, or expiration of exceptions and integrates with AWS CloudTrail for logging of calls to Amazon Inspector.

Show less

What is the “CIS Operating System Security Configuration Benchmarks” rules package?

CIS Security Benchmarks are provided by the Center for Internet Security and are the only consensus-based, best-practice security configuration guides both developed and accepted by

National Vulnerability Database (NVD). We use the NVD's Common Vulnerability Scoring System (CVSS) as the primary source of severity information. In case a CVE is not scored by NVD but is present in Amazon Linux AMI Security Advisory (ALAS), we use the severity from Amazon Linux advisory. In case neither of these scores is available for a CVE, we do not report that CVE as a finding. We check daily for latest information from NVD and ALAS and update our rules packages accordingly.

Show less

What is the severity of a finding?

Each Amazon Inspector rule has an assigned severity level, which Amazon has classified as High, Medium, Low, or Informational. Severity is intended to help you prioritize your responses to findings.

Show less

How is the severity determined?

Severity of a rule is based on potential impact of the security issue found. Although some rules packages have Severity levels provided as part of the rules they provide, these can often differ by rules set. Amazon Inspector has normalized the severity for findings across all available rules packages by mapping the individual severities to common High, Medium, Low, and Informational classifications. For “High”, “Medium”, and “Low” severity findings, the higher the severity of the

Low	< 2.1 and >= 0.8	Low
Informational	< 0.8	N/A

Show less

When I describe findings via the API (DescribeFindings), each finding has a "numericSeverity" attribute. What does this attribute signify?

The "numericSeverity" attribute is the numeric representation of the severity of a finding. The numeric severity values map to Severity as follows:

> Informational = 0.0
> Low = 3.0
> Medium = 6.0
> High = 9.0

Show less

Does Amazon Inspector work with AWS partner solutions?

Yes, Amazon Inspector has public facing APIs that are available for customers and AWS partners to utilize. Several partners have integrated with Amazon Inspector incorporating findings into email,

Inspector supports SOC 1, SOC 2, SOC 3, ISO 9001, ISO 27001, ISO 27017, ISO 27018, and HIPAA. Inspector meets the controls for FedRAMP and we're waiting for the completion of the audit report. If you want to learn more about the AWS services in scope by compliance program, please visit the AWS Services in Scope Page.

Show less

Learn about Amazon Inspector customers

Visit the customer page

Ready to build?

Get started with Amazon Inspector

Have more questions?

Contact us

AWS CLOUD PRACTITIONER ESSENTIALS

Amazon Inspector

- Overview
- Pricing
- Getting Started
- Resources
- FAQs
- Customers
- Partners

AWS & Cloud Computing

What is Cloud Computing?
What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive

Amazon Inspector

- Overview
- Pricing
- Getting Started
- Resources
- FAQs
- Customers
- Partners

Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method

Amazon Inspector

- Overview
- Pricing
- Getting Started
- Resources
- FAQs
- Customers
- Partners

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy