# Amazon Inspector FAQs

What is Amazon Inspector?

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

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 an API-driven service that uses an optional agent, making it easy to deploy, manage, and automate. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

What makes up the Amazon Inspector service?

Amazon Inspector consists of a technology that analyzes your network configurations in AWS for reachability, 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.

What is an assessment template?

An assessment template is a configuration that you create in Amazon Inspector to define your assessment run. This assessment template includes a rules package against which you want Amazon Inspector to evaluate your assessment target, the duration of the assessment run, Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings, and Amazon Inspector-specific attributes (key/value pairs) that you can assign to findings generated by the assessment run.

What is an assessment run?

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's configuration, installed software, and behavior against specified rule packages. If the network reachability rules package is included, Inspector analyzes your network configurations in AWS to find accessibility of your EC2 instances over the network. If the Inspector agent is installed on the instance, the agent collects and sends on-host software and configuration data. Next, the Inspector service analyzes the data and compares it against the rule packages specified. A completed assessment run produces a list of findings for potential security issues.

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

There is no performance impact to your application when running an agentless assessment with the network reachability rules package. There is a minimal performance impact during the data collection phase of the assessment run when using the Amazon Inspector Agent.

What is an assessment target?

An assessment target represents a collection of Amazon EC2 instances that you want assessed, typically a set of instances that work together as a unit to help you accomplish your business goal(s). Amazon Inspector evaluates the security state of these EC2 instances. You can include all of your instances in an assessment target or specify a subset of instances by using Amazon EC2 tags.

What is a finding?

A finding is a potential security issue discovered during the Amazon Inspector assessment run of the specified target. Findings are displayed in the Amazon Inspector console or retrieved through the API, and contain both a detailed description of the security issue and a recommendation on how to fix it.

What is a rules package?

A rules package is a collection of security checks that can be configured as part of an assessment template and assessment run. Amazon Inspector has two types of rules packages, the network reachability rules package that checks for network accessibility of your Amazon EC2 instances, and host assessment rules packages that check for vulnerabilities and insecure configurations on the Amazon EC2 instance. Host assessment rules packages include Common Vulnerabilities and Exposures (CVE), Center for Internet Security (CIS) Operating System configuration benchmarks, and security best practices. See the [Amazon Inspector documentation](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html) for a full list of rules packages available.

Can I define my own rules for assessment templates?

No. Only the pre-defined rules are currently be allowed for assessment runs.

Which on-host software packages 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. Software installed through make config / make install, or binary files copied directly to the system using automation software such as Puppet or Ansible will not be assessed by Inspector.

What is an assessment report, and what does it include?

An Amazon Inspector assessment report can be generated for an assessment run once it has been successfully completed. An assessment report is a document that details what is tested in the assessment run, and the results of the assessment. The results of your assessment are formatted into a standard report, which can be generated to share results within your team for remediation actions, to enrich compliance audit data, or to store for future reference.

You can select from two types of report for your assessment, a findings report or a full report. The findings report contains an executive summary of the assessment, the instances targeted, the rules 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.

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

Amazon Inspector assessments with the network reachability rules package can be run without an agent for any Amazon EC2 instances. The agent is required for host assessment rules packages. Amazon Inspector will gather vulnerability data from all available agents and return any appropriate security findings for them. Inspector generates Exclusions to notify you of any EC2 instances without the agent installed or having an unhealthy agent.

How do agents become unavailable?

Amazon Inspector Agents could be unavailable for a number of reasons, such as: the EC2 instance is down or unresponsive; the targeted instance does not have the agent installed; the installed agent is unavailable or cannot return vulnerability data.

What is the pricing for Amazon Inspector?

Amazon Inspector pricing is based on number of Amazon EC2 instances included in each assessment, and depends on the rules packages you select for assessments. Inspector assessments can have any combination of host assessment rules packages and the network reachability rules package. Host assessment rules packages include Common Vulnerabilities and Exposures (CVE), Center for Internet Security benchmarks (CIS), Security Best Practices, and Runtime Behavior Analysis. If your assessments include both host rules packages and the network reachability rules package, you will be billed for both separately. The on-demand billing period is one calendar month. See the [Amazon Inspector pricing page](https://aws.amazon.com/inspector/pricing/) for full pricing details.

Pricing example:

Consider a scenario where you run the following assessment runs in a month. In this example, all of your assessment runs include both host assessment rules packages and the network reachability rules package. And all of your EC2 instances have the Inspector Agent on them.

1 assessment run against 1 instance  
1 assessment run against 10 instances  
10 assessment runs against 2 instances each  
30 assessment runs against 10 instances each

If the above represented the Amazon Inspector assessment runs activity in your account for a given billing period, you would be charged for 331 host agent-assessments and 331 network reachability instance-assessments.

The price of each individual host agent-assessment and network reachability instance-assessment is based on a tiered pricing model. For example, as you move up the volume of agent-assessments in a given billing period, you pay a lower price per agent-assessment.

The Amazon Inspector charges for your account for this billing period would be:

For host assessment rules packages -  
First 250 agent-assessments @ $0.30 per agent-assessment  
Next 81 agent-assessments @ $0.25 per agent-assessment

For network reachability rules package  
First 250 instance-assessments @ $0.15 per instance-assessment  
Next 81 instance-assessments @ $0.13 per instance-assessment

Adding up all the above, the Amazon Inspector bill would be $95.25 for host agent-assessments and $48.03 for network reachability instance-assessments, for a total of $143.28.

Is there a free trial for Amazon Inspector?

Yes. Accounts that have never run an Amazon Inspector assessment, you’re eligible for 250 agent-assessments with host rules packages and 250 instance-assessments with the network reachability rules package at no cost during your first 90 days.

What Operating Systems does Amazon Inspector support?

Please see the [Amazon Inspector documentation](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_supported_os_regions.html) for a current list of supported operating systems for the Inspector Agent. Note that the network reachability rules package can be run without an agent for any Amazon EC2 instances regardless of the operating system. If the Inspector Agent is installed, network reachability generates enhanced findings with information that identifies the software processes reachable on your EC2 instances.

In what regions is Amazon Inspector available?

Please see the [Amazon Inspector documentation](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_supported_os_regions.html) for a current list of supported regions.

Which Linux kernel versions are supported for Amazon Inspector assessments?

You can run successful assessments for an EC2 instance with a Linux-based OS using the network reachability, Common Vulnerabilities and Exposures (CVE), Center for Internet Security (CIS) Benchmarks, or Security Best Practices rules packages regardless of the kernel version. However, to run an assessment using the 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.

Amazon Inspector sounds great, how do I get started?

Sign up for Amazon Inspector from the [AWS Management Console](https://console.aws.amazon.com/inspector/). On the welcome page, you can enable scheduled network reachability assessments for your whole account with just one click. You can install the optional Inspector Agent on your EC2 instances to enable host assessment rules packages. You can also customize the EC2 instances to assess, rules package selection, and notifications of findings using the advanced setup option. Once an assessment run completes, Inspector will generate findings for security issues identified in your environment.

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

No, Amazon Inspector assessments with the network reachability rules package can be run without an agent for any Amazon EC2 instances. The agent is required for host assessment rules packages.

How can I install the Amazon Inspector Agent?

There are several ways to install the agent. For simple installations, you can install it manually on each instance or do a one-time load using the [AWS Systems Manager Run Command document](http://docs.aws.amazon.com/inspector/latest/userguide/inspector_installing-uninstalling-agents.html#install-run-command) (AmazonInspector-ManageAWSAgent). For larger deployments, you can [automate agent installations](https://aws.amazon.com/blogs/security/how-to-simplify-security-assessment-setup-using-ec2-systems-manager-and-amazon-inspector/) using the EC2 User Data Function when configuring your instances or you can create automated installs of the agent using AWS Lambda. You can also launch an EC2 instance using the Amazon Linux AMI with the pre-installed Amazon Inspector Agent from the EC2 Console or the [AWS Marketplace](https://aws.amazon.com/marketplace/pp/B077W1VR7G).

How do I check whether the Amazon Inspector Agent is installed and healthy on my EC2 instances?

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.

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 and to read your AWS network configurations. 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.

I use a Network Address Translation (NAT) for my instances. Will Amazon Inspector work with these instances?

Yes. Instances that use a NAT are supported by Amazon Inspector with no action required from you.

I use a Proxy for my instances. Will Amazon Inspector work with these instances?

Yes. The Amazon Inspector Agent supports proxy environments. For Linux instances, we support HTTPS Proxy, and for Windows instances, we support WinHTTP proxy. See the [Amazon Inspector User Guide](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents.html) for instructions to configure Proxy support for the Amazon Inspector Agent.

I would like to automate the assessment of my infrastructure on a regular basis. Do you provide an automated way to set up 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. Amazon Inspector assessments can also be configured and triggered through AWS CloudFormation templates.

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

Yes, you can set up a simple recurring schedule for assessments in your assessment template. And Inspector assessments can be triggered by any Amazon CloudWatch Event. You can set up custom schedules with either a fixed recurring rate or a more detailed Cron expression through CloudWatch Events.

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 displayed in the Inspector console as part of your assessment templates so you can see all of the automated triggers for that assessment.

Can I set up Amazon Inspector assessments through AWS CloudFormation?

Yes, you can create Amazon Inspector resource groups, assessment targets, and assessment templates using AWS CloudFormation templates. This allows you to automatically set up security assessments for your EC2 instances as they are deployed. In your CloudFormation template, you can also bootstrap installation of the Inspector Agent on EC2 instances by using [agent installation commands](http://docs.aws.amazon.com/inspector/latest/userguide/inspector_installing-uninstalling-agents.html) in either [AWS::CloudFormation::Init](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-init.html) or [EC2 user data](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html). Alternatively, you can create EC2 instances in your CloudFormation template using an AMI with the Inspector Agent pre-installed.

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](https://docs.aws.amazon.com/inspector/latest/userguide/using-cloudwatch.html) for details on the assessment metrics published to CloudWatch.

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](https://aws.amazon.com/cloudtrail/) for logging of calls to Amazon Inspector.

What is the network reachability rules package?

The network reachability rules package that identifies ports and services on your Amazon EC2 instances that are reachable from outside your VPC. When you run an assessment with this rules package, Inspector queries AWS APIs to read network configurations in your account such as Amazon Virtual Private Clouds (VPCs), security groups, network access control lists (ACLs), and route tables. then analyzes these network configurations to prove accessibility of ports. Findings show you the network configurations that allow access to a reachable port to help you easily restrict access as needed. The Amazon Inspector agent is not needed for assessments with the network reachability rules package. For instances with the Inspector agent installed, network reachability findings are enhanced with information that identifies which processes are listening on accessible ports.

What is the advantage of using the Inspector Agent for network reachability rules package?

The Amazon Inspector agent is not needed for assessments with the network reachability rules package. For instances with the Inspector agent installed network reachability findings are enhanced with information that identifies which processes are listening on accessible ports.

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

CIS Security Benchmarks are provided by the [Center for Internet Security](https://benchmarks.cisecurity.org/) and are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia. Amazon Web Services is a CIS Security Benchmarks Member company and the list of Amazon Inspector certifications can be [viewed here](https://benchmarks.cisecurity.org/membership/certified/amazon/). CIS benchmark rules are designed to be pass/fail security checks. For every CIS check that fails, Inspector generates a finding with High severity. Additionally, an Informational finding is generated for each instance that lists all the CIS rules that are checked, and the pass/fail result for each rule.

What is the “Common Vulnerabilities and Exposures” rules package?

The Common Vulnerabilities and Exposures or CVE rules check for exposure to publicly known information security vulnerabilities and exposures. CVE rule details are available publicly at the National Vulnerability Database (NVD). We use the [NVD's Common Vulnerability Scoring System (CVSS)](https://nvd.nist.gov/cvss.cfm) 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](https://alas.aws.amazon.com/). 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.

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.

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 finding, the more security impact the underlying issue has. Findings that are classified as “Informational” are provided to advise you of security issues which might not have an immediate security impact.

For AWS supported rules packages, the severity is determined by the AWS security team.

The CIS Benchmarks rules package findings always have severity set to “High”.

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

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

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

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, ticketing systems, pager platforms, or broader security dashboards. For detail on supporting partners, please visit the [Amazon Inspector Partners page](https://aws.amazon.com/inspector/customers/).

Is Amazon Inspector a HIPAA eligible service?

Yes, Amazon Inspector is a [HIPAA eligible service](https://aws.amazon.com/compliance/hipaa-eligible-services-reference/) and has been added to the [AWS Business Associate Addendum (BAA)](https://aws.amazon.com/compliance/hipaa-compliance/). If you have an executed BAA with AWS, you can run Inspector on your EC2 instances that contain protected health information (PHI).

What compliance and assurance programs does Amazon Inspector support?

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](https://aws.amazon.com/compliance/services-in-scope/).