- 中文 (简体)

- AWS Management Console
- My Account
- Billing & Cost Management
- Security Credentials

AWS Vulnerability / Penetration Testing Request Form

In order to request permission to conduct vulnerability and penetration testing originating from any resources in the AWS Cloud, the following information is required. The requesting party must also accept the Terms and Conditions and AWS's policy regarding the Use of Security Assessment Tools and Services. Upon receipt and validation of the information, an authorization email approving the test plan will be sent to the addresses provided below. Testing is not authorized until the requesting party receives that authorization. An asterisk (*) indicates required information:

Contact Information

Please provide the email address and the associated name of the AWS account owner with which you have used to log into this form. The AWS Account ID number of the account used to log into this form will be sent along with your submission. If you would like to request testing for a different account, please log out and log back in with the account for which you want to test.

Customer Information

Your Name:*
Company Name*
Email Address
Additional Email Address
Additional Email Address
Additional Email Address

Do you have an NDA with AWS

☐ Yes ☐ No

Target Data

AWS Targets:

EC2 Resources

Cloudfront Distribution

API Gateway / Lambda

RDS Resources

ELB Name

Non-AWS Targets
IP Addresses

Source Data

IP Address

Is the above IP address located in your offices?

☐ Yes ☐ No

Who owns the IP addresses?
Phone contact for testing team:

Does the testing company have a NDA with AWS?

☐ Yes ☐ No

Testing Details

Expected peak bandwidth (Gbps):*
Expected peak requests per second (RPS):*
Expected peak Queries per second (QPS) for DNS Zone Walking
Start Date and Time (YYYY-MM-DD HH:MM)*
End Date and Time (YYYY-MM-DD HH:MM)*
Additional testing details and why this testing is needed:
What criteria/metrics will you monitor to ensure the success of this test?

Do you have a way to immediately stop the traffic if we/your discover any issue?

☐ Yes ☐ No

Please provide two emergency contacts (email and phone):*

Terms and Conditions

Penetration Testing (the “Testing”):

(a) will be limited to the source and destination IP addresses, network bandwidth, and instance-level resources (such as CPU, memory and input/output) specified in your AWS Vulnerability/Penetration Testing Request Form, and the times and other conditions specified in the authorization email that will be sent to email addresses provided above,
(b) will not involve t2.nano, m1.small or t1.micro instances (as described on the AWS website, located at http://aws.amazon.com),
(c) is subject to the terms of the Amazon Web Services Customer Agreement between AWS and Company (available at http://aws.amazon.com/agreement/) (the “Agreement”),
(d) and will abide by AWS’s policy regarding the use of security assessment tools and services (included below).

Furthermore, Testing is not authorized until AWS validates the information and sends an authorization email to the requesting party containing an authorization number. Authorization can take up to 48 business hours.
Any discoveries of vulnerabilities or other issues that are the direct result of AWS must be conveyed to aws-security@amazon.com within 24 hours of completion of the Testing.

Terms and Conditions Agreement*

○ I agree ○ I do not agree

AWS’s Policy Regarding the Use of Security Assessment Tools and Services

AWS’s policy regarding the use of security assessment tools and services allows significant flexibility for performing security assessments of your AWS assets while protecting other AWS customers and ensuring quality-of-service across AWS.

AWS understands there are a variety of public, private, commercial, and/or open-source tools and services to choose from for the purposes of performing a security assessment of your AWS assets.

The term “security assessment” refers to all activity engaged in for the purposes of determining the efficacy or existence of security controls amongst your AWS assets, eg. port-scanning, vulnerability scanning/checks, penetration testing, exploitation, web application scanning, as well as any injection, forgery, or fuzzing activity, either performed remotely against your AWS assets, amongst/between your AWS assets, or locally within the virtualized assets themselves.

You are NOT limited in your selection of tools or services to perform a security assessment of your AWS assets. However, you ARE prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such against or from ANY AWS asset, yours or otherwise. Prohibited activities include, but may not be limited to:
- Protocol flooding (eg. SYN flooding, ICMP flooding, UDP flooding)
- Resource request flooding (eg. HTTP request flooding, Login request flooding, API request flooding)

A security tool that solely performs a remote query of your AWS asset to determine a software name and version, such as “banner grabbing,” for the purpose of comparison to a list of versions known to be vulnerable to DoS, is NOT in violation of this policy.

Additionally, a security tool or service that solely crashes a running process on your AWS asset, temporary or otherwise, as necessary for remote or local exploitation as part of the security assessment, is NOT in violation of this policy. However, this tool may NOT engage in protocol flooding or resource request flooding, as mentioned above.

A security tool or service that creates, determines the existence of, or demonstrates a DoS condition in ANY other manner, actual or simulated, is expressly forbidden.

Some tools or services include actual DoS capabilities as described, either silently/inherently if used inappropriately or as an explicit test/check or feature of the tool or service. Any security tool or service that has such a DoS capability, must have the explicit ability to DISABLE, DISARM, or otherwise render HARMLESS, that DoS capability. Otherwise, that tool or service may NOT be employed for ANY facet of the security assessment.

It is the sole responsibility of the AWS customer to ensure the tools and services employed for performing a security assessment are properly configured and successfully operate in a manner that does not perform DoS attacks or simulations of such. It is the sole responsibility of the AWS customer to independently validate that the tool or service employed does not perform DoS attacks, or simulations of such, PRIOR to security assessment of any AWS assets. This AWS customer responsibility includes ensuring contracted third-parties perform security assessments in a manner that does not violate this policy.

Furthermore, you are responsible for any damages to AWS or other AWS customers that are caused by your penetration testing activities.

AWS Policy Regarding the Use of Security Assessment Tools and Services Agreement*

I agree I do not agree

Submit

Learn

- Products & Services
- Case Studies
- Economics Center
- Architecture Center
- Security Center
- Whitepapers
- Training & Certification
- Webinars
- Industry Solutions
- Use Case Solutions
- User Groups
- Partners

Developer Resources

- AWS Marketplace
- Sample Code & Libraries
- SDKs & Tools
- Documentation
- Articles & Tutorials
- Management Console
- Flexible Payments Service

Developer Centers

- Java
- JavaScript
- Mobile