AWS Web Application Firewall (WAF) AWS Service Delivery Program

Consulting Partner Validation Checklist

December 2019
Version 2.2

aws partner network

Introduction

The goal of the AWS Service Delivery Program is to recognize APN Partners who demonstrate successful customer delivery and experience in specific AWS services. The AWS Service Delivery Validation Checklist is intended to prepare APN Partners who are interested in applying for AWS Service Delivery. This checklist provides the criteria necessary to achieve the designation(s) under the AWS Service Delivery Program.

Expectations of Parties

Once APN Partners have applied to a designation within AWS Service Delivery, APN Partners undergo a validation of their capabilities known as the technical validation upon applying for any AWS Service Delivery designation, and every 12 months thereafter. AWS leverages in-house expertise and may leverage a third-party firm to facilitate the review.

AWS reserves the right to make changes to this document at any time. **It is expected that APN Partners will review this document in detail *before* submitting an AWS Service Delivery application, even if pre-requisites are met.** If items in this document are unclear and require further explanation, please contact your Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Program Office if further assistance is required.

In order to begin the validation process, please follow the steps outlined below:

- Step #1: Review the Partner Validation Checklist and ensure all requirements are met
- Step #2: Submit an AWS Service Delivery Application through the APN Partner Central
  - Login to the APN Partner Central
  - Click "View My APN Account" in left navigation
  - On this page, first submit the following:
    - Your AWS Service Specific AWS Customer Case Study (2) with attached Architecture Diagrams
    - Your AWS Service Specific Consulting Practice
  - Next, scroll to AWS Service Deliveries and select the AWS service you want to apply for
  - Complete the Service Delivery Application
- Step #3: Email completed Self-Assessment to aws-service-delivery@amazon.com

Incomplete applications will not be considered and will be declined until all requirements are met.

Once your firm's application has been submitted through the APN Partner Central, the APN Team will review for completeness and for compliance with the prerequisites. Next, we send applications to in-house or third-party experts to complete a Technical Validation.

AWS recommends that APN Partners have individuals who are able to 1) provide evidence of compliance and 2) speak in-depth to the technical requirements about the AWS Service during the validation process.

Upon completion of the Technical Validation, APN Partners will receive a final status for the submitted application either confirming or not confirming the APN Partners' acceptance into the Service Delivery Designation. APN Partners may attain one or more AWS Service Delivery Designations. Attaining one designation does not guarantee approval into additional Service Delivery Designations.

AWS Service Delivery Program Prerequisites

AWS Service Delivery Partners have demonstrated success helping customers evaluate and use AWS services productively, at varying levels of complexity, and at scale by completing the below requirements.

The following items must be met before a Technical Validation review will be scheduled. These items will be validated by the AWS Service Delivery Program Manager; any deficiencies must be addressed prior to scheduling a validation review.

1.0 APN Program Requirements		Met Y/N
1.1 Program Guidelines	The APN Partner must read the Program guidelines and Definitions before submitting the application. Click here for Program details.	
1.2 Program Requirements	APN Partner is Select, Advanced, or Premier APN Consulting Partner (view requirements)	
2.0 AWS Customer Case Studies		
2.1 AWS Customer Case Studies	APN Partner has two (2) case studies demonstrating successful delivery of the AWS service(s). **Case studies must be for projects that are in production, rather than in pilot or proof of concept stage. Projects that are still in development stage will not be accepted. AWS will not accept case studies in which the partner's customer is an internal or affiliate company.** ***Note**: Public-facing case studies are encouraged over private case studies, as they may be used by AWS for marketing purposes. Evidence of a publicly referenceable case study must be provided in the form of a case study, white paper, blog post, or equivalent, and must be easily discoverable on the APN Partner's website. For best practice on how to write a Public Case Study See Here*	
	APN Partner provides for each case study: ▪ Name of the customer (Internal or affiliate case studies will not be accepted) ▪ AWS Account ID (Will be used to verify AWS service usage) ▪ Problem statement/definition ▪ What you proposed ▪ How AWS services were used as part of the solution ▪ Third party applications or solutions used ▪ Start and end dates of project (Case studies must be for projects started within the past 24 months, and must be for projects that are in production) ▪ Outcome(s)/results ▪ Lessons Learned	
2.2 Architecture Diagrams	Submitted case studies must include architecture diagrams. ▪ Architecture diagrams must detail how the solution interacts with the AWS Cloud; specifically, what AWS tools and services are used in the solution ▪ Diagrams must also include evidence of AWS best practices for architecture and security **Note:** *For best practice on how to build an accepted Architecture Diagram See Here*	
2.3 Partner Practice Microsite	APN Partner must have an AWS-branded microsite that is related to or specific to AWS service. ▪ APN Partner microsite must be accessible from APN Partner home page; Home page is not acceptable as a microsite. **Note:** *For best practice on how to build an accepted Microsite See Here*	
3.0 APN Partner Self-Assessment		
3.1 Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment against designation requirements using the AWS Service Delivery Validation Checklist. ▪ APN Partner must complete all sections of the checklist.	

	▪ Completed self-assessment must be emailed to aws-service-delivery@amazon.com, using the following convention for the email subject line: "[APN Partner Name], Service Delivery Partner Completed Self-Assessment."	

AWS Service Delivery Program Requirements

In preparation for the validation process, Partners should become familiar with the items outlined in this document, and prepare objective evidence, including but not limited to: prepared demonstration to show capabilities, process documentation, and/or actual customer examples.

AWS WAF Approval Criteria

The AWS Service Delivery Program is guided by AWS best practices and Well Architected Framework.

AWS WAF Validation Checklist		Detailed Description of Evidence	Met Y/N
1.0 Case Study Requirements	**Each Case Study includes the following details regarding AWS WAF:** ▪ AWS Web Application Firewall (WAF) use case, e.g., application vulnerability protection, PCI compliance, DDoS protection, or other security and monitoring ▪ Request volume ▪ Details of the rule set implemented, including how it was defined, and what ongoing monitoring and maintenance is being performed, and monitoring details. e.g., implemented publicly available bad IP reputation list and integrated Lambda to trigger updates to rule sets based on traffic patterns	Customer implementation description or documentation	
2.0 AWS Service Requirements	**2.1 Each customer case study will demonstrate at least one of the following:** ▪ Compliance - Achieving a third-party compliance certification, such as PCI DSS, where compliance relies on deployment of WAF rules customized by the partner for the specific application ▪ Custom Application - Deployment of WAF rules for a custom application, where the WAF rules are developed in conjunction with the application development team as part of their defense-in-depth strategy, with a well-defined set of security goals, e.g. addressing OWASP Top 10, with WAF rules tailored to the application and deployed as part of the application ▪ DDoS - Protection for an application that is subject to targeted DDoS attacks, and has successfully deployed WAF, Shield and Shield Advanced to mitigate these attacks ▪ Dedicated Research Team - Use WAF as a platform for their own threat research team to deploy mitigations for emerging threats on an ongoing basis Enhancement of Templatized Rulesets– Building of enhanced maintenance, monitoring, alerting, mitigation and/or rule updates around Managed Rules purchased from AWS Marketplace, AWS WAF Security Automations and/or AWS WAF Preconfigured Rules.		
	Each submitted customer case study includes one of the following, depending on the type:		

	▪ Compliance – Details on the compliance certification achieved, and the rules that were implemented to achieve it. ▪ Custom Application – Details on the security properties targeted, how rules are developed with the application development team, and how they are deployed and updated in production. Deployment of rules must be automated and a part of the application deployment process. ▪ Monitoring – Details on the WAF monitoring solution deployed, how it was implemented and what products, tool or development work was done. Monitoring deployments must also include the net result achieved. ▪ DDoS – Description of the WAF rules implemented, and how they fit into the overall DDoS mitigation strategy. Must implement BP1-7 from "AWS Best Practices for DDoS Resiliency Whitepaper", or have subscribed to Shield Advanced and successfully mitigated three incidents tracked in Shield Advanced. Dedicated Research Team – Must have a team of at least 3 security researchers dedicated full time to security research, where the output of their research is embodied in the WAF rules.		

AWS Resources

Title	Description
How to Build a Practice Microsite	Provides guidance how to build a Practice/solution page that will meet the prerequisites of the Program.
How to Write a Public Case Study	Provides guidance how to build a Public Customer Case Study that will meet the prerequisites of the Program.
How to Build an Architecture Diagram	Provides guidance how to build a architecture diagrams that will meet the prerequisites of the Program.
What is AWS WAF	What is AWS Web Application Firewall and how to get started
Access Control Developer Guide	AWS WAF Authorization and Access Control developer Guide

AWS reserves the right to make changes to the AWS Service Delivery Program at any time and has sole discretion over whether APN Partners qualify for the Program.