AWS IoT Competency

Technology Partner Validation Checklist

May 2017
Version 2.0

Table of Contents

Introduction

The Competency Partner Validation Checklist is intended for APN Partners who are interested in applying for AWS Competency. This checklist provides the criteria necessary to achieve the designation under the AWS Competency Program.

The goal of the AWS Competency Program is to recognize APN Partners who demonstrate technical proficiency and proven customer success in specialized solution areas.

APN Partners undergo a validation of their capabilities upon applying for the specific Competency, and every 12 months thereafter. AWS leverages in-house expertise 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 a Competency application, even if all of the pre-requisites are met.** If items in this document are unclear and require further explanation, please contact your AWS Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Competency Program Team if further assistance is required.

Competency Application and Audit Process

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

- Step #1: Review the Partner Validation Checklist
- Step #2: Submit a Competency Application through the APN Portal
  - Login to the APN Portal
  - Click “View My APN Account” in left navigation
  - Scroll to AWS Competencies and select the appropriate Competency
  - Complete the Competency Application

Incomplete applications will not be considered and will be rejected.

Once your firm’s application has been submitted through the APN Portal, the APN Team will review for compliance.

AWS recommends that APN Partners have individuals who are able to provide evidence of compliance and to speak in-depth to the requirements available during the validation process.

Upon completion of the review, a recommendation is given to the APN Team regarding APN Partner acceptance into the Competency. The final decision regarding acceptance is made by the APN Team; APN Partners will be notified of their status by AWS.

Program Policies

An APN Partner's application to the Competency may be rejected at the discretion of the Global Segment Business or Technical Lead. Rejections may be made due to estimated ability to consistently implement technical solutions, lack of current required APN Partner certifications, judgment of the technical or business merit of the proposed solution, perceived lack of solution delivery capabilities, or any other business or technical criteria deemed critical.

Competency status can be revoked at the discretion of the Global Segment Business or Technical Lead. Revocations may be issued due to loss of required APN Partner certifications, lack of progress toward billing or win goals, repeated violations of AWS PR guidelines, evidence of poor customer experience, including cost vectors, when using the solution, or any other business/technical factors that would indicate that the practice or solution may not meet current requirements, or is projected not to meet future requirements.

Competency status must be renewed annually on a calendar year basis. Requirements for renewal may change from year to year, subject to the business and technical needs of AWS and its customers.

AWS IoT Technology Competency Categories

Please review the IoT category/categories your firm wishes to apply for: Edge, Gateway, Platform Providers, or Connectivity; please note that you may apply for more than one category but must provide separate customer references for each category.

Category	Characteristics
Technology for Edge	Technology that provides: ▪ Hardware or software components and systems used to design and build edge devices ▪ Off-the-shelf edge hardware products in the IoT/M2M space ▪ Connectivity related hardware components used on edge and gateway devices
Technology for Gateway	Technology that provides: • Gateway hardware or software components and systems used to design, build, and manage gateway systems • Off-the-shelf gateway products in the IoT/M2M space
Technology for Platform Providers	Technology that provides: • Tools to create, manage, and extend IoT applications • Secure ingestion, processing, storage, or visualization of data from edge devices and gateways • Configuration and management of edge devices or gateways
Technology for Connectivity	Technology that provides: • Carrier-related services such as network connectivity, billing, rating, fleet visualization, cost optimization, or integration with other connectivity partners • Device and subscription management capabilities

AWS IoT Competency Program Prerequisites

IoT Competency Partners provide deep technical and consulting expertise helping enterprises adopt, develop and deploy complex IoT projects. IoT Partners guide customers though all phases of IoT project development. Deep working knowledge architecting IoT solutions and applications leveraging AWS services is mandatory.

AWS IoT Competency – Technology Partner Prerequsites	
APN Membership	APN Partner must meet Advanced tier+ APN Technology Partner (view requirements)
AWS Support	APN Partner must have Business level+ Support plan (view Support plans)
AWS Customer References	APN Partner must provide ≥ 4 AWS customer references specific to completed IoT projects: • 2 of the 4 AWS customer references must be public (i.e., documented in a case study, white paper, or blog post). Public references must mention AWS, the end customer, and the APN Partner. • References must be for projects started within the past 12 months, and must be for projects that are in production, rather than in pilot or proof of concept stage • All customer references submitted must have supporting documentation providing evidence of compliance to the requirements of this checklist
IoT Product or Solution	APN Partner must have a IoT product or solution on AWS, including: • Availability of product or solution in 3 or more AWS regions • Qualifying for and posting an AWS public support statement on APN Partner's website detailing the APN Partner's IoT practice on AWS and including public reference to the APN Partner's solution, practice, or guidance on IoT. For example, an acceptable public support statement is a landing page on the APN Partner's website that contains various elements, including the AWS solutions and competency use cases, reference architecture, technology partnerships, customer references, sample TCO pricing, and any other relevant information supporting the APN Partner's expertise related to IoT and highlighting the partnership with AWS through the APN. • A reference architecture for an IoT use case which is optimized for security, reliability, performance, cost optimization, and operational excellence • If required, provide licensing model which allows for utility consumption

AWS IoT Technology Partner Validation Checklist

In preparation for the validation process, APN Partners should become familiar with the requirements of this checklist. Supporting documentation (e.g., design and architectural documents) for the submitted customer references must be provided, in order to demonstrate compliance to the below requirements.

Technology for Edge

This classification includes APN Partners providing hardware or software components and systems used to design and build edge devices, component hardware that connects directly to the cloud, component hardware that connects to the cloud via gateway devices, as well as APN Partners providing product-ready devices. Examples include wireless sensors, microcontrollers, low-power battery operated devices and related hardware kits.

APN Partners providing device connectivity related hardware components used in both edge and gateway devices are also included in this category. Examples include but are not limited to 802.15.4, LoRa, Sigfox, Ingenu, Bluetooth, Bluetooth Low Energy, 802.11, GSM, and CDMA.

1.0 AWS Customer References – Technology for Edge		Met	Not Met
1.1 Customer References	APN Partner has four (4) AWS customer references of completed IoT projects. APN Partner must provide for each reference: ▪ Name of the customer ▪ 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 ▪ Outcome(s)/results ▪ Lessons learned		
1.2 Public References	2 of the above 4 references are publicly endorsed by the customer. Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum: ▪ Reference to customer name, APN Partner name, and AWS ▪ Customer problem that was solved ▪ How AWS was used as part of the solution ▪ Outcome(s)/results Public references must be easily discoverable on the APN Partner's website.		
1.3 Security Best Practices	References must show how the solution was deployed in accordance with AWS Security Best Practices.		

2.0 Technology Components – Technology for Edge		Met	Not Met
2.1 General Requirements	General Requirements listed in Appendix A must be met.		
2.2 Reference Architecture	APN Partner must provide a reference architecture showing how the Edge technology fits into the IoT stack (See Appendix C). The Edge offering does not need to be specific to a market segment or vertical; however it must highlight how the Edge technology solves a specific IoT stack problem and/or accelerates the customer's time to production.		
2.3 Project Evidence	For each of the four (4) customer references provided in Section 1, APN Partner must demonstrate a successful integration of the cloud into their hardware, software, or development system. Solutions may: ▪ Communicate securely, directly to the cloud from a standalone device ▪ Integrate AWS IoT device setup/provisioning into the development system ▪ Integrate the AWS IoT device SDK onto a hardware device		

	APN Partner must alternately highlight projects using and integrating the Edge technology with a gateway providing a secure ingest of data into the AWS Cloud. Referenced projects must be reviewed by the IoT Partner Solutions Architect and must follow Hardware Best Practices in Appendix B.		
2.4 Alternate Protocols	For protocols used other than AWS IoT TLS 1.2: ▪ APN Partner must demonstrate how the hardware and protocols are used to provision devices securely ▪ Documentation must demonstrate how the hardware and protocols prevent rogue devices from joining, disrupting, and impersonating the network. Note: For certain communication legacy protocols it may not be possible to meet the above requirements. For these protocols clear documentation of the risks and mitigations are required to ensure the customer understands them before choosing a solution.		
2.5 Hardware Kits	For hardware kits, APN Partner must provide evidence of two (2) well documented applications purpose built for the kit: ▪ Application #1 must demonstrate that AWS IoT or gateway connectivity is functional: o Publish to a known topic that indicates the device is online o Update the thing shadow to indicate that the device is online o Subscribe to a topic and demonstrate that the subscription was successful ▪ Application #2 must demonstrate that all components of the kits are accessed and functional: o For all advertised sensors or components publish readings to a known topic or update them in the thing shadow at a fixed interval		

Technology for Gateway

This classification includes APN Partners that provide gateway hardware or software components and systems that are used to design, build, and manage gateway systems, as well as APN Partners that provide off-the-shelf gateway products in the IoT space. Hardware and software must communicate with the cloud and provide cloud connectivity to edge devices.

1.0 AWS Customer References – Technology for Gateway		Met	Not Met
1.1 Customer References	APN Partner has four (4) AWS customer references of completed IoT projects. APN Partner must provide for each reference: ▪ Name of the customer ▪ 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 ▪ Outcome(s)/results ▪ Lessons learned		
1.2 Public References	2 of the above 4 references are publicly endorsed by the customer. Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum: ▪ Reference to customer name, APN Partner name, and AWS ▪ Customer problem that was solved ▪ How AWS was used as part of the solution ▪ Outcome(s)/results Public references must be easily discoverable on the APN Partner's website.		
1.3 Security Best Practices	References must show how the solution was deployed in accordance with AWS Security Best Practices.		

2.0 Technology Components – Technology for Gateway		Met	Not Met
2.1 General Requirements	General Requirements listed in Appendix A must be met.		
2.2 Reference architecture	APN Partner must provide a reference architecture highlighting how the product or solution fits into the IoT space not specific to a segment or vertical. Technology solutions may: ▪ Ingest data on behalf of edge devices and send it securely to the cloud ▪ Send messages to edge devices that originate from the cloud ▪ Process data offline and provide local functionality (e.g. rules, buffering, alerts, integration with local legacy systems) ▪ Manage topics and thing shadows on behalf of edge devices ▪ Aggregate multiple sensors into logical groups or larger virtual sensors		
2.3 Project Evidence	For each of the four (4) customer references provided in Section 1, APN Partner must demonstrate an IoT solution. Solution may: ▪ Aggregate data from edge devices ▪ Provide services to configure gateway and edge devices ▪ Provide services to manage gateway and edge devices Referenced projects must be reviewed by the IoT Partner Solutions Architect and must follow Hardware Best Practices in Appendix B.		
2.4 Alternate Protocols	For protocols used other than AWS IoT TLS 1.2: ▪ APN Partner must demonstrate how the hardware and protocols are used to provision devices securely ▪ Documentation must demonstrate how the hardware and protocols prevent rogue devices from joining, disrupting, and impersonating the network. Note: For certain communication legacy protocols it may not be possible to meet the above requirements. For these protocols clear documentation of the risks and mitigations are required to ensure the customer understands them before choosing a solution.		

Technology for Platform Providers

This classification includes Platforms that provide customers the ability to build, develop, and manage IoT applications. A Platform must have the ability to collect or act upon the data from edge devices and gateways. Platforms may also provide configuration and management of edge devices or gateways, offer application hosting and deployment environments, and other services.

1.0 AWS Customer References – Technology for Platform Providers		Met	Not Met
1.1 Customer References	APN Partner has four (4) AWS customer references of completed IoT projects. APN Partner must provide for each reference: ▪ Name of the customer ▪ 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 ▪ Outcome(s)/results ▪ Lessons learned		
1.2 Public References	2 of the above 4 references are publicly endorsed by the customer. Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum: ▪ Reference to customer name, APN Partner name, and AWS ▪ Customer problem that was solved ▪ How AWS was used as part of the solution ▪ Outcome(s)/results		

	Public references must be easily discoverable on the APN Partner's website.		
1.3 Security Best Practices	References must show how the solution was deployed in accordance with AWS Security Best Practices.		

2.0 Technology Components – Technology for Platform Providers		Met	Not Met
2.1 General Requirements	General Requirements listed in Appendix A must be met.		
2.2 Reference Architecture	APN Partner must provide a reference architecture highlighting how the platform fits into the IoT space not specific to a segment or vertical as well as how the platform accelerates building of customer applications. Solution must include integration of a minimum of 3 AWS services. Solution may: ▪ Demonstrate the ability to ingest, process, or store data at scale from IoT devices ▪ Integrate with the AWS IoT rules engine to perform scalable message routing, transformation, and condition testing ▪ Leverage AWS managed services (Amazon DynamoDB, AWS Lambda, Amazon SQS, Amazon SNS)		
2.3 Project Evidence	For each of the four (4) customer references provided in Section 1, APN Partner must demonstrate how the IoT platform accelerated the customer's project time-to-market.		
2.4 Platform Integration	APN Partner must demonstrate how their platform contributes to the overall APN ecosystem by highlighting how the platform can be integrated with other Partner solutions. Evidence of integration may include: ▪ Utilization of common open data formats ▪ Showcasing of existing APN partner integrations ▪ Describing how data from the platform would be utilized by a new Partner directly or via documented APIs		
2.5 Platform Access	The platform must provide role-based access and governance to the platform to control what end users can see, access, and modify.		

Technology for Connectivity

This classification includes APN Partners that are carriers or virtual carriers (MNO/MVNO/MVNE/MVNA), as well as APN Partners that provide carrier related services such as billing, rating, fleet visualization, cost optimization, or integration with other connectivity APN Partners. The focus here is on the successful integration of AWS IoT to support initial device discovery and credential authentication.

1.0 AWS Customer References – Technology for Connectivity		Met	Not Met
1.1 Customer References	APN Partner has four (4) AWS customer references of completed IoT projects. APN Partner must provide the following for each reference: ▪ Name of the customer ▪ 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 ▪ Outcome(s)/results ▪ Lessons learned		
1.2 Public References	2 of the above 4 references are publicly endorsed by the customer. Evidence must be in the form of a publicly available case study, white paper, blog post, or equivalent that includes, as a minimum: ▪ Reference to customer name, APN Partner name, and AWS ▪ Customer problem that was solved ▪ How AWS was used as part of the solution ▪ Outcome(s)/results		

	Public references must be easily discoverable on the APN Partner's website.		
1.3 Security Best Practices	References must show how the solution was deployed in accordance with AWS Security Best Practices.		

2.0 Technology Components – Technology for Connectivity		Met	Not Met
2.1 General Requirements	General Requirements listed in Appendix A must be met.		
2.2 Reference Architecture	APN Partner will provide a reference architecture highlighting how their offering fits into the IoT space not specific to a segment or vertical.		
2.3 Project Evidence	APN Partners utilizing SIM cards to provide connectivity, subscription based or pre-paid, must support over the air configuration and management. Acceptable evidence may include: ▪ Demonstration of how devices are remotely provided credentials to access cloud services ▪ Demonstration of how credentials are remotely revoked from devices ▪ Demonstration of how devices are remotely monitored and managed ▪ Demonstration of how data allocations/plans are configured		
2.2 Management Tools	2.2.1 APN Partner must have management tools or dashboard deployable on AWS. Acceptable evidence may include demonstration of the ability to: ▪ Visualize an entire fleet in the field ▪ Drill down to investigate issues for a single device, group of devices, or fleet based on possible configuration issues, connectivity issues, or network outages ▪ Enable provisioning as well as de-provisioning of devices ▪ Integrate provisioning and de-provisioning flows into AWS IoT (e.g., deactivating certificates, updating device registry attributes) ▪ Integrate thing types into management tools to allow grouping by thing types for visualization, configuration, provisioning, and de-provisioning purposes		
	2.2.2 APN Partner must provide evidence of a device and subscription management portal.		

Appendix A – General Requirements

Requirements applicable to all solutions (hardware and software)
▪ Must only use cross-account roles when accessing AWS data/services in another account. Shared IAM credentials are not allowed. ▪ Must have one clearly defined use case it is best suited for (shared with customers) ▪ Must have one clearly defined use case it is not suited for ▪ Must have a clearly defined, differentiated, value proposition (shared with customers) ▪ Capabilities/compliance to be validated yearly by third party auditors
Requirements applicable to software solutions only

▪ All systems must be deployable in at least two regions
▪ All systems must be multi-AZ and demonstrate how they remain highly available in the event of AZ failure
▪ For systems that ingest data through mechanisms other than AWS IoT and AWS managed services the APN Partner must document and demonstrate its ability to scale to meet any size of workload across the following dimensions: number of connected devices (e.g., could it support 1M devices), rate of ingested data per device (e.g., could it support 1 MB / sec from a single device), overall volume of ingested data (e.g., could it support ingesting 1 PB of data)
▪ For systems that durably store data they must do so in an AWS managed service (Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift)
▪ For systems that durably store data with S3 they must enable versioning and MFA delete by default to prevent accidental deletion of critical data
▪ Multi-tenant SaaS solutions must go through a technical assessment by an AWS SA
▪ Non-SaaS (AMI/BYOL/other) solutions must either go through a technical assessment by an AWS SA or be added to the Marketplace
▪ APN Partner must be able to demonstrate that their solution works with AWS for IoT workloads and are not specific to a customer requirement. They should also be able to demonstrate that the solution can scale to meet any size of the workload. Evidence must be in the form of either of the following components:
  ▪ Product documentation of solutions available to public on how it helps customer with IoT workloads
  ▪ For solutions offered as a product to deploy - Product documentation specific to AWS with clear guidelines on how to implement/use the solution on AWS
  ▪ For solutions offered as a service to use - Architectural details of the SaaS solution implemented on AWS. Details of the performance and availability to help customers optimize IoT workloads on AWS.
▪ The product must provide customers with IoT solutions that are aligned with AWS architecture best practices and reference architectures.
▪ APN Partner must be able to provide an architectural overview that provides the following details on the use of AWS services like Amazon Virtual Private Cloud (VPC) and patterns like Multi-AZ deployments to provide highly available and reliable infrastructure.
▪ If APN Partner leverages AWS services, the APN Partner must be able to demonstrate integration/usage of AWS services following best practices. Acceptable evidence is listed below, and includes but is not limited to:
• Amazon S3
  ○ Use of multi-part uploads for upload large objects on Amazon S3
  ○ Capability to process large data sets in parallel
  ○ Support for access control measure either by IAM or a custom integration
• Amazon EC2
  ○ Use of network isolation via Amazon VPC, Subnet and Security groups
  ○ Use of Spot Instances for products which have failure recovery built-in

- Amazon RDS
  - Use of bulk load capabilities for large data upload/download instead of ODBC/JDBC
  - Use a Read-replica for offloading analytical workloads
- Amazon EMR
  - Use of transient and permanent clusters as necessary for the workload
  - Use of IAM roles for launching clusters and for access to AWS resources like Amazon Kinesis, Amazon S3 and Amazon DynamoDB.
- Amazon Redshift
  - Loading from S3 in parallel using Copy from S3 command, and not over ODBC/JDBC
  - Usage pattern aligned with the best practices outlined here - http://docs.aws.amazon.com/redshift/latest/dg/best-practices.html
- Amazon Kinesis
  - Best practices around building real-time application in general with focus on data delivery at low latency with a reliable data backup strategy independent from the processing.
- Amazon DynamoDB
  - Usage pattern aligned with the best practices outline here - http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/BestPractices.html

Appendix B – Hardware Best Practices

AWS IoT hardware best practices - preliminary list of BPs. This list will continue to evolve.
Last updated: 8/8/2016
Author: Tim Mattison

- Do not re-implement the AWS IoT device SDK (*)
- Do not use the REST APIs to publish data (*)
- Do not include hard coded credentials
- Do not include hard coded, direct URLs to services, resources, or credentials
- Do not include URLs to services, resources, or credentials using URL shorteners that your company does not control
- Do not include hard coded Cognito configurations
- Do not allow the device to be configured with credentials other than TLS certificates
- Do not re-use certificates between devices
- All URLs to documentation must be easily modified in the event that documentation needs to be updated
- Keep in-package documentation to a minimum. Where possible link to online documentation.
- Distribute all documentation in PDF format, HTML single page, and HTML multi-page formats

*(*) For devices that are **not** capable enough to include the official AWS IoT device SDK:*

- They must use TLS 1.2
- They must use certificate based authentication
- They may use REST APIs if they only need to publish data, otherwise they must use MQTT
- The device must pass a validation test if it needs to make use of the thing shadow
- The documentation must clearly enumerate which AWS IoT features it supports

Appendix C – IoT Stack Elements