aws partner network | competency

AWS Networking Competency

Technology Partner Validation Checklist

May 2019
Version 2.0

aws partner network

Table of Contents

Introduction

The goal of the AWS Competency Program is to recognize AWS Partner Network Partners ("APN Partners") who demonstrate technical proficiency and proven customer success in specialized solution areas. The Technology Partner Validation Checklist ("Checklist") is intended for APN Partners who are interested in applying for AWS Competency. This Checklist provides the criteria necessary to achieve the AWS Networking Competency designation under the AWS Competency Program. APN Partners undergo an audit of their capabilities upon applying for the specific Competency. AWS leverages in-house expertise and may also utilize a third-party firm to facilitate the audit. AWS reserves the right to make changes to this document at any time and in its sole discretion.

Expectations of Parties

It is expected that APN Partners will review this document in detail before submitting an application for the AWS Competency Program, even if all of the prerequisites 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 Program Office if further assistance is required.

When ready to submit a program application, APN Partners should complete the APN Partner Self-Assessment column of the AWS Competency Program Validation Checklist set forth below in this document.

To submit your application:

1. Log in to the APN Partner Central (https://partnercentral.awspartner.com/), as Alliance Lead
2. Select "View My APN Account" from the left side of the page
3. Scroll to "Program Details" section
4. Select "Update" next to AWS Competency you wish to apply for
5. Fill out Program Application and Click "Submit"
6. Email completed Self-Assessment to competency-checklist@amazon.com

If you have any questions regarding the above instructions, please contact your PDR or PDM.

AWS will review and aim to respond back with any questions within 5 business days to initiate scheduling of your audit or to request additional information.

APN Partners should prepare for the audit by reading the Checklist, completing a self-assessment using the Checklist, and gathering and organizing objective evidence to share with the auditor on the day of the audit.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the audit. The best practice is for the APN Partner to make the following personnel available for the audit: one or more highly technical AWS certified engineers/architects, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation. APN Partners should ensure that they have the necessary consents to share with the auditor (whether AWS or a third-party) all information contained within the objective evidence or any demonstrations prior to scheduling the audit.

AWS Networking Competency and Categories

AWS Networking Competency Partners provide network solutions that assist enterprises adopt, develop, and deploy networks on in AWS. AWS Networking Competency Partners provide a set of specialized solutions for making connectivity easier and extending customer capabilities. Deep working knowledge architecting networking solutions and applications leveraging AWS services is mandatory.

APN Partners must also identify the Segment Category that their solution fits into:

1.) **Networking Connectivity:** Technology that provides network connectivity to AWS, is capable of acting as a router that intelligently forwards packets, manages availability between different network paths, and provides Virtual Private Network (VPN) or Software-Defined Wide Area Networking (SD WAN) services.

2.) **AWS Direct Connect Integrated Partners:** APN Partners that help AWS customers establish network connectivity between AWS Direct Connect locations and the customer. APN Partners who directly integrate with the hosted connection model in addition to supporting customers to access the dedicated connection model are eligible.

    If you directly integrate with the hosted virtual interface (VIF) model, you are still eligible to renew this competency as long as you meet all of the following criteria:

    - You must have implemented the hosted VIF model prior to AWS closing this model to new APN partner integrations
    - You must also support the dedicated connection model

    The APN Partner also includes greater integration and interaction with AWS services. Partners that have developed software-defined networking (SDN) functions to automate end user services.

3.) **AWS Direct Connect Infrastructure Partners:** APN Partners that help AWS customers establish network connectivity between AWS Direct Connect locations and the customer. APN Partners who support the dedicated connection model are eligible. These APN Partners may provide network connectivity and infrastructure such as fiber or AWS Direct Connect interconnections.

4.) **Load Balancers:** Technology that distributes network and application traffic across multiple IP based devices for a service, maintains health status of target services, and supports security services such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

5.) **Network Management:** Technology that provides network health information, network visualization, and capability to alert and notify on network issues.

AWS Networking Competency Program Prerequisites

The following items will be validated by the AWS Competency Program Manager; missing or incomplete information must be addressed prior to scheduling of the AWS Technical Validation Review.

1.0 APN Program Membership		Met Y/N
1.1 Program Guidelines	The APN Partner must read the Program Guidelines and Definitions before applying to the AWS Competency Program. Click here for Program details	
1.1 Technology APN Partner Tier	APN Partner must be an Advanced Tier APN Technology Partner before applying to the Networking Competency Program.	
1.2 Solution Category	APN Partner to identify the Segment Category for their solution: ☐ **Network Connectivity** ☐ **Direct Connect Integrated Partners** ☐ **Direct Connect Infrastructure Partners** ☐ **Load Balancers** ☐ **Network Management** Deployment Model: ☐ **SaaS on AWS** ☐ **SaaS outside AWS** ☐ **BYOL on AWS** ☐ **BYOL On-premises**	
1.3 Customer Adoption	APN Partner to describe total number of customers leveraging their solution.	
2.0 AWS Customer Case Studies		**Met Y/N**
2.1 Networking - Specific Case Studies	APN Partner must have 4 unique AWS customer Case Studies specific to a Networking solution under review. It is acceptable for an APN Partner solution to be comprised of multiple products to address a category use case. Each of the 4 Case Studies must relate to an example of the Partner solution being used in one of the three Segment Categories. For each Case Study, the APN Partner must provide the following information: ▪ Name of the customer ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ Third party applications or solutions used ▪ Date the reference entered production ▪ Outcome(s)/results ▪ Specific architecture diagrams, deployment guides and other materials depending on the type of solution, as described in the next section. This information will be requested as part of the Program Application process in APN Partner Central. The information provided as part of this Case Study can be private and will not be made public. All 4 of the Case Studies provided will be examined in the Documentation Review of the Technical Validation. The Case Study will be removed from consideration for inclusion in the Competency if the APN Partner cannot provide the documentation necessary to assess the Case Study against each checklist item, or if there were any of the checklist items are not met.	

	Case Studies must describe deployments that have been performed within the past 18 months, and must be for projects that are in production with customers, rather than in a 'pilot' or proof of concept stage.	
2.2 Publicly Available Case Studies	Publicly available case studies are used by AWS upon approval into the Competency to showcase the APN Partner has demonstrated success based on measurable KPIs with the solution and provide customers with confidence that the APN Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives. 2 of the four 4 customer deployments associated with the Case Studies must be publicized by the APN Partner as publicly available Case Studies. These publicly available Case Studies may be presented in the form of formal Case Studies, white papers, videos, or blog posts.	
	Publicly available AWS Case Studies must be easily discoverable from the APN Partner's website, e.g. it must be possible to navigate to the publicly available Case Study from the APN Partner's home page, and the APN Partner must provide links to these publicly available Case Studies in their application.	
	Publicly available AWS Case Studies must include the following: ▪ References to the customer name, APN Partner name, and AWS ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ How AWS services were used as part of the solution ▪ Outcome(s)/results	
3.0 AWS Networking Web Presence and Thought Leadership		**Met Y/N**
3.1 APN Partner AWS Landing Page	An APN Partner's internet presence specific to their AWS Networking Solutions provides customers with confidence about the APN Partner's capabilities and experience. APN Partner must have an AWS landing page that describes their AWS Networking solution, links to their publicly available Case Studies, lists technology partnerships, and provides any other relevant information supporting the AWS Partner's expertise related to AWS Networking Competency and highlighting the collaboration with AWS. This AWS-specific Networking page must be accessible from the APN Partner's home page. The home page itself is not acceptable as an AWS landing page unless APN Partner is a dedicated Networking company and home page reflects APN Partner's focus on AWS Networking Competency.	
3.2 Networking Thought Leadership	AWS Networking Competency Partners are viewed as having deep domain expertise in AWS Networking, having developed innovative solutions that leverage or help manage AWS services. APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner's focus on and expertise in AWS Networking. Links must be provided to examples of materials published within the last 12 months.	
4.0 Business Requirements		**Met Y/N**
4.1 Field-Ready Toolkits	APN Partner has field-ready documentation and seller toolkits including a clear product value proposition that can be articulated to the AWS sales organization with all relevant information needed to determine fit for a customer opportunity (e.g., sales collateral, presentation, and customer use cases). Evidence must be in the form of sales collateral including a presentation, one-pager, and use-case checklist.	

4.2 Product Support/Help Desk	APN Partner offers product support via web chat, phone, or email support to customers. Evidence must be in the form of description of support offered to customers for their product or solution.	
4.3 Product is listed on AWS Marketplace	APN Partner makes solution available via AWS Marketplace. ☐ Yes ☐ No If "yes", APN Partner must provide a link to the AWS Marketplace listing. If "no", no further information is required. Note, AWS Marketplace is not mandatory to achieve the competency	
5.0 APN Partner Self-Assessment		**Met Y/N**
5.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance to the requirements of the Checklist. ▪ APN Partner must complete all sections of the Checklist. ▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com**, using the following convention for the email subject line: "[APN Partner Name], Networking Competency Technology Partner Completed Self-Assessment." ▪ It is recommended that APN Partner has their PDR, or PDM review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the APN Partner's AWS team is engaged and working to provide recommendations prior to the review and to help ensure a productive review experience.	

AWS Networking Competency Technology Partner Validation Checklist

The following items will be validated by a third-party auditors and/or AWS Partner Solutions Architects; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

Networking Category Specific Technical Requirements		Met Y/N
Required Solution Features Documentation describing how the APN Partner solution meets the requirements must be submitted as part of the competency self-assessment		
Network Connectivity	*The APM Partner solution must support AWS Auto Scaling for handling additional network connectivity. This design can include Amazon Route 53 or Elastic Load Balancing. The design must be able to auto-scale horizontally without manual intervention.* *The AWS Auto Scaling use case must:* • *Include an AWS CloudFormation template of the deployment, including any load balancing or monitoring dependencies. This can be for a new or existing VPC.* • *Public documentation must provide all steps for deploying the environment, focusing on simplicity whenever possible.*	
	AWS Integration - The routing solution must have these AWS capabilities: ▪ *All components of the solution must be deployed across multiple availability zones such that the solution is resilient to a single AZ failure without manual intervention.*	

	Examples of automated failover mechanisms include: ○ *Leveraging Elastic Load Balancing* ○ *Moving a elastic network interface on failure* ○ *Altering a route table entry or subnet association on failureNative support for the virtual private gateway (or transit gateway via VPN attachment) and providing an up to date VPN template download for the AWS Management Console* ▪ *The solution must provide native support for the virtual private gateway or transit gateway via VPN attachment.* ○ *Must support Border Gateway Protocol (BGP) with the virtual private gateway or transit gateway VPN attachment* ▪ *Native bootstrapping using the user data field* ○ *May involve secondary data sources such as Amazon Simple Storage Service (Amazon S3)* *Support for enhanced networking with the ixgbevf driver and elastic network adapter (ENA) driver.*	
Direct Connect for Integrated Partners	*APN Partner has 6 AWS customer references of completed networking projects.*	
	APN Partner must provide regular (monthly or quarterly) business data for their AWS Direct Connect business to AWS. This will enable AWS to provide better services to AWS customers. It should include: ▪ *Quantity of unique customers* ▪ *Quantity of customer facing ports and interface speeds* ▪ *Quantity of ports and interface speeds facing AWS for the dedicated connection model only* ▪ *Data should be broken out by geography* ▪ *Packet loss percentages peaks and averages per port or location.* ▪ *The time to provision the circuit when requested by the customer, the SLA time, and SLA breaches.* ▪ *Other AWS revenue, e.g. reseller revenue*	
	APN Partner must have a user portal accessible to users. This portal must be able to: ▪ *Allow customers to provision hosted connections and/or hosted virtual interfaces* ▪ *Adjust network capacity allocated to a circuit, if the capability exists* *Provide user-facing visibility of network health. This should involve real-time metrics.*	
	Customers must have a self-service mechanism for provisioning and managing connections and VIFs. This must require no manual intervention from partner operations staff.	
	APN Partner must detail what network infrastructure and services they offer to customers on an AWS landing page (e.g. www.awspartner.com/aws). This landing page should state: ▪ *What models of AWS Direct Connect they support* ▪ *Describe their resiliency offerings and link to AWS Resiliency Recommendations web page (https://aws.amazon.com/directconnect/resiliency-recommendation/)* ▪ *For each supported model: the end to end provisioning process and responsible party for each step* ▪ *What circuit types are available (e.g. Layer 2 - VPLS, Dedicated Fiber, Layer 3 - MPLS, etc)* ▪ *Which AWS Direct Connect locations are supported* *If resiliency is included in the offering*	
	▪ *APN Partner has 6 AWS customer references of completed networking projects mid-*	

	market or enterprise customers.	
Direct Connect Infrastructure Partners	*APN Partner has 6 AWS customer references of completed networking projects.*	
	APN Partner must provide regular (monthly or quarterly) business data for their AWS Direct Connect business to AWS. This will enable AWS to provide better services to AWS customers. It should include: ▪ *Quantity of unique customers* ▪ *Quantity of customer facing ports and interface speeds* ▪ *Quantity of ports and interface speeds facing AWS for the dedicated connection model only* ▪ *Data should be broken out by geography* ▪ *The time to provision the circuit when requested by the customer, the SLA time, and SLA breaches.* ▪ *Other AWS revenue, e.g. reseller revenue*	
	For each of the 6 customer references provided in Section 1, APN Partner must demonstrate a successful integration of their offering with a customer deployment.	
	APN Partner must detail what network infrastructure they offer to customers on an AWS landing page (e.g. www.awspartner.com/aws). This landing page should state: ▪ *What models of AWS Direct Connect they support* ▪ *Describe their resiliency offerings and link to AWS Resiliency Recommendations web page (https://aws.amazon.com/directconnect/resiliency-recommendation/)* ▪ *For the dedicated connection model: the end to end provisioning process and responsible party for each step* ▪ *What circuit types are available (e.g. Layer 2 - VPLS, Dedicated Fiber, Layer 3 - MPLS, etc)* *Which AWS Direct Connect locations are supported*	
	▪	
Load Balancers	*For each of the 4 customer references provided in Section 1, APN Partner must demonstrate a successful integration of their software into a customer deployment.* ▪ *At least 1 customer reference must be utilizing an auto-scaling design where the load balancer instances are in an auto-scaling group*	
	The solution must be able to auto scale for handling additional network connectivity. This design can include Amazon Route 53 or Elastic Load Balancing. The design must be able to auto-scale horizontally without manual intervention. AWS Auto Scaling must be supported without on-premises components.	
	The load balancing solution must provide a highly available deployment option. *In the high availability configuration the solution must use DNS or Elastic Load Balancing to distribute inbound requests to multiple partner load balancer instances deployed in multiple availability zones.* *In the high availability configuration the load balancing solution must be able to send downstream traffic to an Elastic Load Balancing load balancer.* *Native bootstrapping using the user data field* ▪ *May involve secondary data sources such as Amazon S3*	

	Support for at least 3 custom Amazon CloudWatch metrics, such as 3/4/5xx error messages, connections per second, and open sessions *Support for enhanced networking with the ixgbevf driver and elastic network adapter (ENA) driver*	
Network Management	*For each of the 4 customer references provided in Section 1, APN Partner must demonstrate a successful integration of their software into a customer deployment.*	
	The network management solution must provide all of the AWS capabilities from one of the following feature lists. *Either the network management solution must have all of the following AWS capabilities:* ▪ *Support for ingesting flow logs. The solution must provide visualization or reporting on the Flow Logs data.* ▪ *Provide visualization of customer's VPCs* ▪ *Support for ingesting Amazon CloudWatch metrics* ▪ *Provide alerts on Amazon Cloudwatch metrics, traffic patterns, usage, or events such as VPCs created with overlapping addresses* *OR* *The network management solution must have all of the following AWS capabilities:* ▪ *Ability to provide raw network packets to another AWS location or instance* ▪ *Ability to account for the performance of packet replication* ▪ *Support for Amazon Linux* ▪ *Ability to automatically audit the instances or resources in the AWS account that are running the relevant software* ▪ *Publicly available automation (e.g. AWS CloudFormation template) to deploy the solution.*	
	If the management portal runs in the user's account, it must have a public reference designs or automation to maintain high availability in multiple AZs.	

Technical Validation		Applies to: SaaS	Applies to: Customer-Deployed on AWS	Met Y/N
Required Documentation All of the following documentation must be submitted as part of the Competency Self-Assessment.				
Architecture Diagram	Depending on the deployment category, one or more architecture diagrams are required. Each architecture diagram must show: ☐ The major elements of the architecture, and how they combine to provide the APN Partner Solution to customers ☐ All of the AWS services used, using the appropriate AWS service icons. ☐ How the AWS services are deployed, including, VPCs, AZs, subnets, and connections to systems outside of AWS. ☐ Includes elements deployed outside of AWS, e.g. on-premises components, or hardware devices.	Yes – one for the whole solution and one for each Case Study.	Yes – one for each Case Study.	
Deployment Guide	The deployment guide must provide best practices for deploying the APN Partner Solution on AWS, and include all of the sections outlined in "Baseline Requirements for Deployment Guides"	No	Yes – one for the solution.	
Completed Validation Checklist	For each of the 4 AWS Case Studies provided for the APN Partner Solution, the APN Partner must provide a completed version of the following checklist indicating which checklist items are met.	Yes	Yes	
1.0 Security **The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.**				
1.1 AWS account root user is not used for routine activities	The AWS account root user must not be used for routine activities. Following the creation of your AWS account, you should immediately create IAM user accounts, and use these IAM user accounts for all routine activities. Once your IAM users accounts have been created, you should securely store the AWS root account credentials and use them only to perform the few account and service management tasks that require the AWS account root user. For further information on how to set up an IAM user accounts and groups for daily use, see Creating Your First IAM Admin User and Group.	Yes	No	
1.2 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user	MFA must be enabled for your AWS account root user. Because your AWS account root user can perform sensitive operations in your AWS account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available, including virtual MFA and hardware MFA.	Yes	No	
1.3 IAM user accounts used for all routine activities	The AWS account root user must not be used for any task where it is not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an administrators group to which you attach the administrator access managed policy. Thereafter, the users in the administrator's group should set up the groups, users, and so on, for the AWS account. All future interaction should be through the AWS account's users and their own keys instead of the root user. However, to perform some account and service management tasks, you must log in using the root user credentials.	Yes	No	

1.4 Multi-Factor Authentication (MFA) is enabled for all interactive IAM users	You must enable MFA for all interactive IAM users. With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).	Yes	No	
1.5 IAM credentials are rotated regularly	You must change your passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords, and you can choose how often they must do so. For more information about rotating access keys for IAM users, see Rotating Access Keys.	Yes	Yes (for credentials used to integrate with AWS)	
1.7 Strong password policy is in place for IAM users	You must configure a strong password policy for your IAM users. If you allow users to change their own passwords, require that they create strong passwords and that they rotate their passwords periodically. On the Account Settings page of the IAM console, you can create a password policy for your account. You can use the password policy to define password requirements, such as minimum length, whether it requires non-alphabetic characters, how frequently it must be rotated, and so on. For more information, see Setting an Account Password Policy for IAM Users.	Yes	Yes (for credentials used to integrate with AWS)	
1.8 IAM credentials are not shared among multiple users	You must create an individual IAM user account for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative privileges, and use that IAM user for all your work. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)	Yes	No	
1.9 IAM policies are scoped down to least privilege	You must follow the standard security advice of granting least privilege. This means granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.	Yes	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	
1.10 Hard-coded credentials (e.g. access keys) are not used	You must follow best practices for managing AWS access keys and avoid the use of hard-coded credentials. When you access AWS programmatically, you use an access key to verify your identity and the identity of your applications. Anyone who has your access key has the same level of access to your AWS resources that you do. Consequently, AWS goes to significant lengths to protect your access keys, and, in keeping with our shared responsibility model, you should as well.	Yes	Yes (credentials used to integration with AWS should be easily changed and not hard coded)	

1.11 All credentials are encrypted at rest	The baseline requirement is to ensure the encryption of any credentials at rest.	Yes	Yes (credentials stored in APN Partner solution used to integrate with AWS should be encrypted)	
1.12 AWS Access Keys only used by interactive users	No AWS access keys should be in use, except in the following cases: 1. Used by humans to access AWS services, and stored securely on a device controlled by that human. 2. Used by a service to access AWS services, but only in cases where: a) It is not feasible to use an Amazon Elastic Compute Cloud (Amazon EC2) instance role, Amazon Elastic Container Service (Amazon ECS) Task Role or similar mechanism, b) The AWS access keys are rotated at least weekly, and c) The IAM Policy is tightly scoped so that it: i) allows only access to only specific methods and targets and ii) restricts access to the subnets on from which the resources will be accessed.	Yes	No	
1.13 CloudTrail is enabled for all AWS accounts in every region	AWS CloudTrail must be enabled on all AWS accounts and in every region. Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.	Yes	No	
1.14 CloudTrail logs are stored in an Amazon S3 bucket owned by another AWS account	CloudTrail logs must be emplaced in a bucket owned by another AWS account configured for extremely limited access, such as audit and recovery only.	Yes	No	
1.15 CloudTrail Amazon S3 log bucket has Versioning or MFA Delete enabled	CloudTrail log bucket contents must be protected with versioning or MFA Delete.	Yes	No	
1.16 Amazon EC2 security groups are tightly scoped	All Amazon EC2 security groups should restrict access to the greatest degree possible. This includes at least 1. Implementing AWS security groups to restrict traffic between Internet and VPC, 2. Implementing AWS security groups to restrict traffic within the VPC, and 3. In all cases, allow only the most restrictive possible settings.	Yes	Yes	
1.17 S3 buckets within your account have appropriate levels of access	You must ensure that the appropriate controls are in place to control access to each S3 bucket. When using AWS, it's best practice to restrict access to your resources to the people that absolutely need it (the principle of least privilege).	Yes	No (unless APN Partner solution running on AWS requires the S3 service)	
1.18 S3 buckets have not been misconfigured to allow public access.	You must ensure that buckets that should not allow public access are properly configured to prevent public access. By default, all S3 buckets are private, and can only be accessed by users that have been explicitly granted access. Most use cases won't require broad-ranging public access to read files from your	Yes	No (unless APN Partner solution running on AWS requires	

	S3 buckets, unless you're using S3 to host public assets (for example, to host images for use on a public website), and it's best practice to never open access to the public.		the S3 service)	
1.19 A monitoring mechanism is in place to detect when S3 buckets or objects become public	You must have monitoring or alerting in place to identify when S3 buckets become public. One option for this is to use AWS Trusted Advisor. Trusted Advisor checks buckets in Amazon S3 that have open access permissions. Bucket permissions that grant access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant upload/delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. The Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.	Yes	No (unless APN Partner solution running on AWS requires the S3 service)	
1.20 A monitoring mechanism is in place to detect changes in AMAZON EC2 instances and Containers	Any changes to your Amazon EC2 instances or Containers may indicate unauthorized activity, and must at a minimum be logged to a durable location to allow for future forensic investigation. The mechanism employed for this purpose must at least: 1. Detect any changes to the OS or application files in the Amazon EC2 instances or Containers used in the solution. 2 Store data recording these changes in a durable location, external to the Amazon EC2 instance or Container. Examples of suitable mechanisms include: a. Deployment of file integrity checking via scheduled configuration management (e.g. Chef, Puppet, etc.) or a specialized tool (e.g. OSSEC, Tripwire or similar), or b. Extending configuration management tooling to validate Amazon EC2 host configuration, and alert on updates to key configuration files or packages with 'canary' (logged no-op) events configured to ensure the service remains operational on all in-scope hosts during runtime, or c. Deploying a Host Intrusion Detection System such as an open source solution like OSSEC with Amazon Elasticsearch Service and Kibana or using a APN Partner solution. Note that the following mechanism does not meet this requirement: a. Frequently cycling Amazon EC2 instances or Containers.	Yes	No	
1.21 All data is classified	All customer data processed and stored in the workload is considered and classified to determine its sensitivity and the appropriate methods to use when handling it.	Yes	No	
1.22 All sensitive data is encrypted	All customer data classified as sensitive is encrypted in transit and at rest.	Yes	No	
1.23 Cryptographic keys are managed securely	All cryptographic keys are encrypted at rest and in transit, and access to use the keys is controlled using an AWS solution such as AWS Key Management Service (AWS KMS) or an APN Partner solution such as HashiCorp Vault.	Yes	Yes	
1.24 All data in transit is encrypted	All data in transit across a VPC boundary is encrypted.	Yes	Yes	
1.25 Security incident response process is defined and rehearsed	A security incident response process must be defined for handling incidents such as AWS account compromises. This process must be tested by implementing procedures to rehearse the incident response process, e.g. by completing a security game day exercise. A rehearsal must have been held within the last 12 months to confirm that: a. The appropriate people have access to the environment. b. The appropriate tools are available. c. The appropriate people know what to do to respond	Yes	No	

	to the various security incidents outlined in the plan.			
2.0 Reliability The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.				
2.1 Network connectivity is highly available	Network connectivity to the solution must be highly available. If using VPN or AWS Direct Connect to connect to customer networks, the solution must support redundant connections, even if the customers do not always implement this.	Yes	Yes	
2.2 Infrastructure scaling mechanisms align with business requirements	Infrastructure scaling mechanisms must align with business requirements, either by: 1. Implementing auto-scaling mechanisms at each layer of the architecture, by 2. Confirming that current business requirements, including cost requirements and anticipated user growth, do not require auto-scaling mechanisms AND manual scaling procedures are fully documented and frequently tested.	Yes	Yes	
2.3 AWS and Application logs are managed centrally	All log information from the application, and from the AWS infrastructure, should be consolidated into a single system.	Yes	No	
2.4 AWS and Application monitoring and alarms are managed centrally	The application and the AWS infrastructure must be monitored centrally, with alarms generated and sent to the appropriate operations staff.	Yes	No	
2.5 Infrastructure provisioning and management is automated	The solution must use an automated tool such as AWS CloudFormation or Terraform to provision and manage the AWS infrastructure. The AWS Management Console must not be used to make routine changes to the production AWS infrastructure.	Yes	No	
2.6 Regular data backups are being performed	You must perform regular backups to a durable storage service. Backups ensure that you have the ability to recover from administrative, logical, or physical error scenarios. Amazon S3 and Amazon Simple Storage Service Glacier are ideal services for backup and archival. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. The pay-for-what- you-use model and low cost per GB/month make these services a good fit for data protection use cases.	Yes	No	
2.7 Recovery mechanisms are being tested on a regular schedule and after significant architectural changes	You must test recovery mechanisms and procedures, both on a periodic basis and after making significant changes to your cloud environment. AWS provides substantial resources to help you manage backup and restore of your data.	Yes	No	
2.8 Solution is resilient to availability zone disruption	The solution must continue to operate in the case where all of the services within a single AZ have been disrupted.	Yes	Yes	
2.9 Resiliency of the solution has been tested	The resiliency of the infrastructure to disruption of a single AZ has been tested in production, e.g. through a game day exercise, within the last 12 months.	Yes	Yes	
2.10 Disaster Recovery (DR)	A well-defined disaster recovery (DR) plan includes a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO). You must define an RPO and an RTO for all in-scope services, and the	Yes	No	

plan has been defined	RPO and RTO must align with the SLA you offer to your customers			
2.11 Recovery Time Objective (RTO) is less than 24 hours	The baseline requirement is for the RTO to be less than 24 hours for core services.	Yes	No	
2.12 Disaster Recovery (DR) plan is adequately tested	Your DR plan must be tested against your RPO and RTO, both periodically and after major updates. At least one DR test must be completed prior to approval of your AWS APN Advanced Tier application.	Yes	No	
2.13 Disaster Recovery (DR) plan includes recovery to another AWS account	Your DR plan must include a strategy for recovering to another AWS account, and your periodic recovery testing must test this scenario. You must have completed at least one full test of the DR plan, including at least recovery to another AWS account, within the last 12 months. Note: Although processes restoring data into test environments or exporting data for users are useful ways to verify backups, these processes do not fulfill the requirement to perform a full restore test to another AWS account.	Yes	No	
3.0 Operational Excellence The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.				
3.1 Deployment of code changes is automated	The solution must use an automated method of deploying code to the AWS infrastructure. Interactive Secure Shell (SSH) or Remote Desktop Protocol (RDP) sessions must not be used to deploy updates in the AWS infrastructure.	Yes	No	
3.2 Runbooks and escalation process are defined	Runbooks must be developed to define the standard procedures used in response to different application and AWS events. An escalation process must be defined to deal with alerts and alarms generated by the system, and to respond to customer-reported incidents. The escalation process must also include escalating to AWS Support where appropriate.	Yes	No	
3.3 AWS Business Support is enabled for the AWS Account	Business Support must be enabled. Business Support (or greater) is an AWS Partner Network requirement for Advanced Tier Technology APN Partners. To qualify for Advanced Tier, you must enable Business Support on at least one of your AWS accounts.	Yes	No	

AWS Resources

Title	Description
How to Build a Practice Landing Page	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 an architecture diagrams that will meet the prerequisites of the Program.
APN Partner Readiness Doc	Provides guidance and best practice examples of the Program perquisites.
Well Architected Website	Learn about the Well Architected Framework and it's approach.

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