aws partner network | competency

AWS 소매 컴피턴시
기술 파트너 검증 체크리스트

2019 년 12 월
버전 1.0

목차

서론

AWS 컴피턴시 프로그램의 목표는 전문 솔루션 영역에서 기술적 숙련도와 고객 성과를 입증한 AWS 파트너 네트워크 파트너('APN 파트너')를 인증하는 것입니다. 컴피턴시 파트너 검증 체크리스트(이하 "체크리스트")는 AWS 컴피턴시에 지원할 의사가 있는 APN 파트너를 대상으로 제공되는 것입니다. 이 체크리스트에는 AWS 컴피턴시 프로그램에 선정되기 위해 준비해야 할 요건이 설명되어 있습니다. 특정 컴피턴시에 지원하는 APN 파트너는 구체적인 역량에 대한 감사를 받게 됩니다. AWS 에서는 원활한 감사 진행을 위해 사내 전문가 및 타사를 활용합니다. AWS 는 언제든지 이 문서의 내용을 변경할 권리가 있습니다.

기대 사항

모든 전제 조건이 충족되어도 AWS 컴피턴시 프로그램 참여를 신청하기 전에 APN 파트너는 이 문서를 상세히 검토하시기 바랍니다. 항목별 내용이 명확하지 않고 자세한 설명이 필요한 경우, 먼저 AWS 파트너 개발 담당자("PDR") 또는 AWS 파트너 개발 관리자("PDM")에게 문의하십시오. 추가 지원이 필요한 경우 PDR/PDM 이 프로그램 사무실에 연락할 것입니다.

프로그램 신청서 제출이 준비되면 APN 파트너는 이 문서에서 아래에 설명된 체크리스트의 Partner Self-Assessment(파트너 자체 평가) 항목을 작성해야 합니다.

다음과 같이 신청서를 제출하십시오.

1. APN 파트너 센트럴(https://partnercentral.awspartner.com/)에 Alliance Lead 로 로그인합니다.
2. 페이지 왼쪽에서 [View My APN Account]를 선택합니다.
3. "Program Details" 섹션으로 스크롤을 이동합니다.
4. AWS Competency 옆에 있는 "Update"를 선택하여 신청합니다.
5. 프로그램 신청서를 작성하고 "Submit"을 클릭합니다.
6. 작성한 자체 평가를 competency-checklist@amazon.com 으로 보냅니다.
    - 자체 평가 필수 기재 사항:
        - 솔루션 카테고리(고객 참여, 기업 머천다이징 및 계획, 공급망 및 유통, 물리적, 디지털 및 가상 스토어, 고급 소매 데이터 과학, 핵심 소매 비즈니스 애플리케이션)
        - 배포 유형(SaaS 또는 고객이 AWS 에 배포)
        - AWS 사례 연구에 대한 문서(아래 정의 참조)

위 지침과 관련하여 질문이 있으면 PDR/PDM 에게 문의하십시오.
AWS 는 5 일(영업일 기준) 이내에 질문을 검토하고 회신하여 감사 일정을 잡거나 필요한 추가 정보를 요청하도록 최선을 다합니다.

APN 파트너는 이 체크리스트를 읽고, 체크리스트를 사용하여 자체 평가를 완료한 후, 감사 당일에 감사자와 공유할 객관적 증거를 수집 및 정리해서 감사에 대비해야 합니다.

감사 기간에 AWS 의 요구 기준에 대하여 자세한 설명이 가능한 담당자를 둘 것을 권장합니다. 모범 사례는 APN 파트너가 고급 기술을 보유한 AWS 공인 엔지니어/아키텍트 한 명 이상, 운영 및 지원 부분을 담당하는 운영 관리자, 회사 전반에 대한 프레젠테이션을 진행할 비즈니스 개발 책임자가 감사를 지원할 수 있도록 하는 것입니다. APN 파트너는 감사 일정을 잡기 전에 객관적 입증 자료 또는 기술 데모에 포함된 모든 정보를 감사자(AWS 또는 타사)와 공유하는 데 필요한 동의서에 동의해야 합니다.

AWS 소매 컴피턴시 프로그램

AWS 소매 컴피턴시 파트너는 고객 참여, 기업 머천다이징 및 계획, 소매 공급망 및 유통, 물리적, 디지털 및 가상 스토어, 고급 소매 데이터 과학, 핵심 소매 비즈니스 애플리케이션 부문에서 소매 솔루션을 구축합니다.

소매 컴피턴시 카테고리

APN 파트너는 자사의 솔루션에 해당하는 세그먼트 카테고리도 파악해야 합니다.

- **고객 참여:** 충성도, 소셜 채널 관리, 고객 관계 관리(CRM), 콜 센터, 광고(디지털 및 다이렉트 메일), SEO 그리고 소매 마케팅 책임자가 구매 전 및 후에 고객을 사전에 확보 및 유지할 수 있게 해 주는 대상 참여 솔루션.

- **기업 머천다이징 및 계획:** 머천다이징, 보급, 분류 계획, 상품 진열도/공간 계획, 프로모션 및 가격 최적화, 카테고리 관리 그리고 기업 머천다이징 및 계획 팀에서 사용하는 공급업체 협업 솔루션.

- **공급망 및 유통:** 웨어하우스 관리 시스템(WMS), 엔터프라이즈 리소스 계획(ERP), 웨어하우스 자동화, 가져오기/내보내기, 운송 및 물류를 아우르는 공급망 및 유통 솔루션.

- **물리적, 디지털 및 가상 스토어:** POS, 주문 관리 시스템(OMS), 통합 상거래, 전자 상거래, 라스트 마일 배송, 무경계(무마찰) 스토어 환경, 디지털 혁신(AR/VR, ESL, IoT, 비컨, 음성, 인식, 디지털 키오스크, 스마트 미러, 대화형 디스플레이), 디지털 자산 관리(DAM), 결제를 아우르는 온라인 또는 오프라인 쇼핑 환경을 혁신하는 솔루션.

- **고급 소매 데이터 과학:** 운영 효율성과 고객의 통찰력 및 참여를 개선하는 소매 데이터 레이크, AI/ML 및 분석 솔루션.

- **핵심 소매 비즈니스 애플리케이션:** 경영진, 재무, 조달, 인사, 직원 관리, 법무 및 IT 부문용 핵심 소매 엔터프라이즈 솔루션.

APN 파트너는 또한 자사 솔루션에 적용되는 딜리버리 카테고리를 식별해야 합니다.

1. **SaaS:** 공유 AWS 인프라에서 여러 고객에게 서비스를 제공합니다. 모든 AWS 계정이 APN 파트너에 의해 관리됩니다.

2. **고객 배포:** 고객 AWS 환경에 배포됩니다. 모든 AWS 계정이 고객에 의해 관리됩니다.

AWS 소매 컴피턴시 프로그램 사전 조건

다음 항목은 AWS 컴피턴시 프로그램 관리자가 확인해야 합니다. 누락되거나 불완전한 정보는 기술 검증 검토 일정을 정하기 전에 해결해야 합니다.

1.0 APN 프로그램 멤버십		**해당 여부(예/아니요)**
1.1 기술 파트너 티어	APN 파트너는 소매 컴피턴시 프로그램에 지원하기 전에 프로그램 가이드라인과 정의를 읽어야 합니다. 여기를 클릭하여 프로그램 세부 정보를 확인하십시오.	
1.2 기술 파트너 티어	APN 파트너는 AWS 소매 컴피턴시 프로그램에 지원하기 전에 어드밴스 티어 APN 기술 파트너여야 합니다.	
1.3 솔루션 카테고리	APN 파트너가 자사 솔루션에 대한 세그먼트 카테고리를 파악: □ **고객 참여** □ **기업 머천다이징 및 계획** □ **공급망 및 유통** □ **물리적, 디지털 및 가상 스토어** □ **고급 소매 데이터 과학** □ **핵심 소매 비즈니스 애플리케이션** APN 파트너가 자사 솔루션에 대한 딜리버리 카테고리를 파악: □ **SaaS** □ **고객 배포**	
1.4 고객 도입	APN 파트너가 자사 솔루션을 활용하는 총 고객 수에 대해 설명.	
2.0 사례 연구		**해당 여부(예/아니요)**
2.1 소매 관련 사례 연구	APN 파트너는 검토 대상 소매 솔루션별로 4건의 사례 연구가 있어야 합니다. 4건의 각 사례 연구는 6가지 세그먼트 카테고리(고객 참여, 기업 머천다이징 및 계획, 공급망 및 유통, 물리적, 디지털 및 가상 스토어, 고급 소매 데이터 과학, 핵심 소매 비즈니스 애플리케이션) 중 하나에서 사용되는 APN 파트너 솔루션의 예와 관련이 있어야 합니다. AWS 디지털 고객 경험(DCX), 데이터 및 분석, IoT, 마이그레이션 및/또는 기계 학습 컴피턴시를 보유한 APN 파트너는 고유한 세그먼트 영역 지식을 제공하는 컨설팅 활동과 업계 관련 과제에 대한 대상이 세분화된 솔루션과 함께 제공되는 프로젝트에 대해 최대 4건의 고객 사례 연구를 다시 사용할 수 있습니다. APN 파트너는 각 사례 연구에 대하여 다음 정보를 제공해야 합니다. ▪ 고객의 이름 ▪ 고객의 웹사이트 ▪ 고객 당면 과제 ▪ 솔루션이 배포되어 문제를 해결한 과정 ▪ 사용한 타사 애플리케이션 또는 솔루션 ▪ 레퍼런스가 프로덕션에 투입된 날짜 ▪ 성과/결과 ▪ 솔루션 유형에 따라 특정 아키텍처 다이어그램, 배포 안내서 및 기타 자료(다음 섹션에 설명되어 있음).	

	이 정보는 APN 파트너 센트럴의 프로그램 신청 프로세스의 일부로 요청됩니다. 이 사례 연구의 일부로 제공된 정보는 개인 정보일 수 있으며 공개되지 않습니다. 제공된 4건의 사례 연구는 모두 기술 검증 중 문서 검토 단계에서 검토됩니다. APN 파트너가 각 체크리스트 항목에 대한 사례 연구를 평가하는 데 필요한 문서를 제공할 수 없거나 체크리스트 항목 중 충족되지 않은 항목이 있는 경우, 해당 사례 연구는 컴피턴시 고려 대상에서 제외됩니다. 사례 연구에서는 지난 18 개월 이내에 수행된 배포를 설명해야 하며, '파일럿' 또는 개념 증명 단계가 아니라 고객과 진행한 프로덕션 단계의 프로젝트에 대한 것이어야 합니다.	
2.2 공개 사례 연구	컴피턴시가 승인되면 AWS 는 솔루션에서 측정 가능한 KPI 를 기반으로 입증된 APN 파트너의 성공 사례를 소개하고 고객에게 APN 파트너가 고객의 목표를 달성하기 위한 솔루션을 개발 및 공급하는 데 필요한 경험과 지식을 보유하고 있다는 확신을 주는 데 공개 사례 연구를 사용합니다. APN 파트너는 사례 연구와 관련된 고객 배포 4 건 중 2 건을 공개 사례 연구로 알려야 합니다. 이러한 공개 사례 연구는 공식 사례 연구, 백서 또는 블로그 게시물의 형식이 될 수 있습니다.	
	공개 사례 연구는 APN 파트너의 웹 사이트에서 쉽게 검색할 수 있어야 하며(예: APN 파트너의 홈페이지에서 공개 사례 연구로 이동할 수 있어야 함), APN 파트너는 애플리케이션에서 이러한 공개 사례 연구에 대한 링크를 제공해야 합니다.	
	공개 사례 연구는 다음 사항을 포함해야 합니다. ▪ 고객 이름, APN 파트너 이름 및 AWS에 대한 언급 ▪ 고객 당면 과제 ▪ 솔루션이 배포되어 문제를 해결한 과정 ▪ AWS 서비스가 솔루션의 일부로 사용된 방법 ▪ 성과/결과	
3.0 AWS 소매 웹 보유 및 사고 리더십		**해당 여부(예/아니요)**
3.1 APN 파트너 AWS 랜딩 페이지	고객이 인터넷상에서 APN 파트너의 AWS 소매 솔루션 관련 입지와 존재감을 확인하면 APN 파트너의 소매 역량 및 경험을 손쉽게 신뢰하게 됩니다. APN 파트너에는 AWS 소매 솔루션에 대해 설명하고, 공개적으로 사용 가능한 사례 연구에 연결하며, 소매와 관련된 APN 파트너의 전문 지식을 지원하고 AWS와의 협력 관계를 강조하는 기타 관련 정보를 제공하는 AWS 랜딩 페이지가 있어야 합니다. 이 AWS 관련 소매 페이지는 APN 파트너의 홈 페이지에서 액세스할 수 있어야 합니다. APN 파트너가 소매 기술만 제공하는 전문 회사이고 홈 페이지가 APN 파트너가 소매 분야에 주력하고 있음을 반영하는 경우가 아니면 홈 페이지 자체는 AWS 랜딩 페이지로 허용되지 않습니다.	
3.2 소매 사고 리더십	AWS 소매 컴피턴시 파트너는 AWS 를 활용한 혁신적인 솔루션을 개발하여 소매 분야의 전문 지식을 보유하고 있는 것으로 인정받은 업체입니다. APN 파트너는 소매에 중점을 두고 있으며 전문성을 보유하고 있음을 보여주는 공개 자료(예: 블로그 게시물, 언론 기사, 동영상 등)를 보유해야 합니다. 최근 12개월 이내에 발행된 자료의 예제에 대한 링크를 제공해야 합니다.	

4.0 비즈니스 요구 기준		
4.1 현장에서 사용 가능한 도구 키트	APN 파트너는 고객 기회에 적합한지 여부를 판단하는 데 필요한 모든 관련 정보(예: 영업 자료, 프레젠테이션, 고객 사용 사례)와 더불어 AWS 영업 조직에 설명할 수 있는 분명한 제품 가치 제안을 비롯하여 현장에서 사용 가능한 문서 및 판매자 도구 키트를 보유하고 있습니다. 증거 자료는 프레젠테이션, 원페이저, 사용 사례 체크리스트를 비롯한 판매 자료의 형태여야 합니다.	
4.2 제품 지원/도움말 센터	APN 파트너는 고객에게 웹 채팅, 전화 또는 이메일 지원을 통해 제품 지원을 제공합니다. 증거 자료는 제품 또는 솔루션과 관련하여 고객에게 제공되는 지원에 대한 설명의 형태여야 합니다.	
4.3 AWS Marketplace에 제품 등재	APN 파트너가 AWS Marketplace 를 통해 솔루션을 제공합니다. □ 예 □ 아니요 '예'인 경우 APN 파트너는 AWS Marketplace 등재 링크를 제공해야 합니다. '아니요'인 경우 추가 정보가 필요하지 않습니다.	
4.4 공동 AWS 딜에 대한 영업 보상	APN 파트너는 AW 와의 공동 영업기회에 대해 판매자를 위한 영업 보상 계획을 갖추고 있습니다. □ 예 □ 아니요 □ 설명: _____ 증거 자료는 APN 파트너의 판매자를 위한 보상 계획에 대한 간략한 설명 형식이어야 합니다.	
4.5 AWS/APN 파트너 상호 윈윈 전략	APN 파트너가 상호 윈윈 전략을 문서화하고 공개하는 프로세스를 갖추고 있습니다. 증거 자료는 프로세스에 대한 구두 설명의 형식입니다.	
5.0 APN 파트너 자체 평가		**해당 여부(예/아니요)**
5.1 AWS 컴피턴시 파트너 프로그램 검증 체크리스트 자체 평가	APN 파트너는 AWS 소매 기술 파트너 검증 체크리스트 요구 기준 준수 여부에 대한 자체 평가를 수행해야 합니다. ▪ APN 파트너는 체크리스트의 모든 섹션을 작성해야 합니다. ▪ 작성된 자체 평가는 제목란에 "[APN Partner Name], Retail Competency Technology Partner Completed Self-Assessment"라고 쓴 다음 **competency-checklist@amazon.com**으로 보내야 합니다. ▪ APN 파트너는 이를 AWS에 제출하기 전에 파트너 솔루션스 아키텍트, 파트너 개발 담당자(PDR) 또는 파트너 개발 관리자(PDM)가 작성된 자체 평가를 검토하도록 하는 것이 좋습니다. 이는 APN 파트너의 AWS 팀이 업무 협조를 잘해나가고 있는지 확인하고, 감사 전에 파트너에게 필요한 내용을 조언함으로써 검토 결과가 긍정적으로 나올 수 있도록 하기 위함입니다.	

소매 컴피턴시 기술 파트너 검증 체크리스트

다음 항목은 타사 감사자 및/또는 AWS 파트너 솔루션스 아키텍트가 확인해야 합니다. 누락되거나 불완전한 정보는 기술 검증 검토 일정을 정하기 전에 처리되어야 합니다.

		적용 대상:		
기술 검증		SaaS	고객이 AWS 에 배포	충족 예/아니요
아키텍처 다이어그램	배포 카테고리에 따라 하나 이상의 아키텍처 다이어그램이 필요합니다. 각 아키텍처 다이어그램에는 다음이 표시되어야 합니다. □ 아키텍처의 주요 요소와 이러한 요소가 결합되어 고객에게 파트너 솔루션을 제공하는 방식 □ 사용되는 모든 AWS 서비스를 적절한 AWS 서비스 아이콘을 사용하여 표시. □ Amazon Virtual Private Cloud(VPC), 가용 영역(AZ), 서브넷, AWS 외부의 시스템 연결을 비롯하여 AWS 서비스가 배포되는 방식 □ 온프레미스 구성 요소 또는 하드웨어 디바이스와 같이 AWS 외부에 배포되는 요소를 포함.	예 – 전체 솔루션에 대해 1 개 및 각 사례 연구에 대해 1 개.	예 – 각 사례 연구에 대해 1 개.	
배포 안내서	배포 가이드는 AWS 에 파트너 솔루션을 배포하는 모범 사례를 제공하고, "배포 안내서의 기본 요구 사항"에 설명된 모든 섹션을 포함해야 함	아니요	예 – 솔루션에 대해 1 개.	
작성된 검증 체크리스트	파트너 솔루션에 제공된 4 건의 사례 연구 각각에 대해 APN 파트너는 어떤 체크리스트 항목이 충족되었는지 나타내는 다음 체크리스트의 완성된 버전을 제공해야 합니다.	예	예	
1.0 보안 **보안 원칙은 정보 및 시스템을 보호하는 데 중점을 둡니다. 주요 주제로는 데이터의 기밀성 및 무결성, 권한 관리를 통해 누가 무엇을 할 수 있는지를 파악 및 관리, 시스템 보호, 보안 이벤트를 탐지하기 위한 제어 기능 구축 등을 들 수 있습니다.**				
1.1 AWS 계정 루트 사용자를 일상적인 작업에 사용하지 않음	AWS 계정 루트 사용자를 일상 작업에 사용해서는 안 됩니다. AWS 계정을 생성한 후 즉시 AWS Identity and Access Management(IAM) 사용자 계정을 생성하고 모든 일상적인 작업에 이러한 IAM 사용자 계정을 사용해야 합니다. IAM 사용자 계정이 생성되면 AWS 루트 계정 자격 증명을 안전하게 저장하고 AWS 계정 루트 사용자가 필요한 소수의 계정 및 서비스 관리 작업을 수행하는 데에만 이를 사용해야 합니다. 일상적인 용도로 IAM 사용자 계정 및 그룹을 설정하는 방법에 대한 자세한 내용은 첫 번째 IAM 관리자 및 그룹 생성 섹션을 참조하십시오.	예	아니요	
1.2 AWS 계정 루트 사용자에 대해 Multi-Factor Authentication(MFA) 활성화	AWS 계정 루트 사용자에 대해 Multi-Factor Authentication(MFA)을 활성화해야 합니다. AWS 계정 루트 사용자는 AWS 계정에서 민감한 작업을 수행할 수 있으므로 인증 계층을 추가하면 계정 보호를 강화하는 데 도움이 됩니다. MFA는 가상 MFA 및 하드웨어 MFA 등 다양한 유형으로 제공됩니다.	예	아니요	
1.3 모든 일상 작업에 IAM 사용자 계정 사용	AWS 계정 루트 사용자는 이 사용자가 필요하지 않은 작업에 사용해서는 안 됩니다. 대신, 관리자 액세스 권한이 필요한 각 사용자에 대해 새 IAM 사용자를 생성합니다. 그런 다음 사용자를 관리자 액세스 관리 정책에 연결되는 관리자 그룹에 배치하여 해당 사용자를 관리자로 만듭니다. 이후로 관리자 그룹에 속한	예	아니요	

	사용자가 AWS 계정에 대해 그룹, 사용자, 등을 설정해야 합니다. 앞으로 모든 상호 작용은 루트 사용자 대신 AWS 계정의 사용자 및 해당 사용자의 키를 통해 이루어져야 합니다. 하지만 일부 계정 및 서비스 관리 작업을 수행하려면 루트 사용자 자격 증명을 사용하여 로그인해야 합니다.			
1.4 모든 대화형 IAM 사용자에 대해 Multi-Factor Authentication(MFA) 활성화	모든 대화형 IAM 사용자에 대해 MFA를 활성화해야 합니다. MFA를 사용하면 사용자가 고유한 인증 코드(일회용 암호 또는 OTP)를 생성하는 디바이스를 갖게 됩니다. 사용자는 일반 자격 증명(사용자 이름 및 암호)과 OTP를 모두 제공해야 합니다. MFA 디바이스는 하드웨어일 수도 있고 가상 디바이스일 수도 있습니다(예를 들어, 스마트폰의 앱에서 실행될 수 있음).	예	아니요	
1.5 정기적으로 IAM 자격 증명 교체	암호 및 액세스 키를 정기적으로 교체하고, 계정의 모든 IAM 사용자도 이와 같이 수행하도록 합니다. 그러면 자신도 모르게 암호 또는 액세스 키가 손상되어도 해당 자격 증명을 사용하여 리소스에 액세스할 수 있는 기간을 제한할 수 있습니다. 암호 정책을 계정에 적용하여 모든 IAM 사용자가 암호를 교체하도록 하고, 교체 빈도를 선택할 수 있습니다. IAM 사용자의 액세스 키 교체에 대한 자세한 내용은 액세스 키 교체 섹션을 참조하십시오.	예	아니요	
1.6 IAM 사용자에 강력한 암호 정책 적용	IAM 사용자에 대한 강력한 암호 정책을 구성해야 합니다. 사용자가 직접 암호를 변경하도록 허용할 경우 강력한 암호를 만들고 정기적으로 암호를 교체하도록 해야 합니다. IAM 콘솔의 계정 설정 페이지에서 계정에 대한 암호 정책을 만들 수 있습니다. 암호 정책을 사용하여 최소 길이, 알파벳 이외 문자 포함 여부, 교체 주기 등과 같은 암호 요구 사항을 정의할 수 있습니다. 자세한 내용은 IAM 사용자의 계정 암호 정책 설정 섹션을 참조하십시오.	예	아니요	
1.7 IAM 자격 증명이 여러 사용자 간에 공유되지 않음	AWS에 액세스해야 하는 모든 사용자에 대해 개별 IAM 사용자 계정을 만들어야 합니다. 관리자 자신에 대해서도 IAM 사용자를 만들어 관리 권한을 부여한 후 모든 관리 작업에 대해 이 IAM 사용자를 사용합니다. 계정에 액세스하는 사용자에 대해 개별 IAM 사용자를 만들면 각 IAM 사용자에게 고유한 보안 자격 증명 세트를 부여할 수 있습니다. 또한, 각 IAM 사용자에게 서로 다른 권한을 부여할 수 있으며, 필요한 경우 언제든지 IAM 사용자의 권한을 변경하거나 취소할 수 있습니다. (루트 사용자 자격 증명을 부여하면 취소하기 어려울 수 있으며 권한을 제한할 수 없습니다.)	예	아니요	
1.8 IAM 정책을 최소 권한으로 축소	최소 권한 부여라는 표준 보안 지침을 따라야 합니다. 이는 작업 수행에 필요한 최소한의 권한만 부여하는 것을 의미합니다. 사용자들이 수행해야 하는 작업을 파악한 후 사용자들이 해당 작업만 수행하도록 사용자에 대한 정책을 작성합니다. 최소한의 권한 세트로 시작하여 필요에 따라 추가 권한을 부여합니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 안전합니다. 적절한 권한 세트를 정의하려면 약간의 조사가 필요합니다. 먼저 특정 작업에 필요한 사항이 무엇이고, 특정 서비스에서 어떤 작업을 지원하며, 해당 작업을 수행하는 데 필요한 권한은 무엇인지 확인합니다.	예	아니요	
1.9 하드 코딩된 자격 증명(예: 액세스 키)을 사용하지 않음	AWS 액세스 키 관리 모범 사례를 따르고 하드 코딩된 자격 증명을 사용하지 않아야 합니다. AWS에 프로그래밍 방식으로 액세스하는 경우 액세스 키를 사용하여 사용자의 자격 증명과 애플리케이션의 자격 증명을 확인합니다. 액세스 키를 보유한 사람은 누구든지 AWS 리소스에 대해 사용자와 동일한 수준의 액세스 권한을 가집니다. 따라서 AWS에서는 사용자의 액세스 키를 보호하기	예	예	

	위해 최선을 다하며, 사용자도 AWS의 공동 책임 모델을 준수하도록 노력을 해야 합니다.			
1.10 저장 중인 모든 자격 증명 암호화	기준 요구 사항은 저장 중인 모든 자격 증명을 암호화하는 것입니다.	예	예	
1.11 AWS 액세스 키는 대화형 사용자만 사용	다음 경우 이외에는 AWS 액세스 키를 사용해서는 안 됩니다. 1. 사람이 AWS 서비스에 액세스하는 데 사용하고, 그 사람이 제어하는 디바이스에 안전하게 저장되는 경우. 2. 서비스가 AWS 서비스에 액세스하기 위해 사용하는 경우. 그러나 다음을 충족해야 함: a) Amazon EC2 인스턴스 역할, Amazon Elastic Container Service(Amazon ECS) 작업 역할 또는 유사한 메커니즘을 사용할 수 없음, b) AWS 액세스 키를 최소한 매주 교체, c) IAM 정책이 다음과 같이 엄격하게 제한됨: i) 특정 방법 및 대상에 대한 액세스만 허용 및 ii) 리소스에 액세스하는 서브넷에 대한 액세스 제한	예	예	
1.12 모든 리전의 모든 AWS 계정에 대해 AWS CloudTrail 활성화	모든 리전의 모든 AWS 계정에 대해 AWS CloudTrail이 활성화되어야 합니다. AWS 계정 활동에 대한 가시성이 보안 및 운영 모범 사례의 핵심 측면 중 하나입니다. AWS CloudTrail을 사용하여 AWS 인프라 전반에서 계정 활동을 보고, 검색하고, 다운로드하고, 아카이브하고, 분석하고, 대응할 수 있습니다. AWS 계정에서의 활동을 분석하고 대응하는 데 도움이 되도록 누가 어떤 작업을 수행했는지, 어떤 리소스가 사용되었는지, 언제 이벤트가 발생했는지 등의 세부 정보를 식별할 수 있습니다.	예	아니요	
1.13 CloudTrail 로그는 다른 AWS 계정이 소유한 S3 버킷에 저장됨	AWS CloudTrail 로그는 감사 및 복구 전용과 같이 액세스가 매우 제한되도록 구성된 다른 AWS 계정이 소유한 S3 버킷에 배치해야 합니다.	예	아니요	
1.14 CloudTrail S3 로그 버킷에서 버전 관리 또는 MFA Delete 활성화	AWS CloudTrail 로그 버킷 콘텐츠는 버전 관리 또는 MFA Delete를 사용하여 보호되어야 합니다.	예	아니요	
1.15 Amazon EC2 보안 그룹의 범위를 엄격하게 제한	모든 Amazon EC2 보안 그룹은 최대한 액세스를 제한해야 합니다. 즉, 최소한 1. 인터넷과 Amazon VPC 간 트래픽을 제한하는 보안 그룹을 구현하고, 2. Amazon VPC 내부 트래픽을 제한하는 보안 그룹을 구현하고, 3. 모든 경우에 최대한 제한적인 설정만 허용합니다.	예	예	
1.16 계정 내 Amazon S3 버킷의 적절한 액세스 수준	각 Amazon S3 버킷에 대한 액세스를 제어할 수 있는 적절한 제어 항목을 적용해야 합니다. AWS를 사용할 때 절대적으로 필요한 사람으로 리소스에 대한 액세스를 제한하는 것이 모범 사례입니다(최소 권한의 원칙).	예	예	
1.17 Amazon S3 버킷이 공개 액세스를 허용하도록 잘못 구성되지 않음	공개 액세스를 허용하면 안 되는 버킷은 공개 액세스가 되지 않도록 적절히 구성해야 합니다. 기본적으로 모든 Amazon S3 버킷은 비공개 버킷이며 명시적으로 액세스 권한이 부여된 사용자만 액세스할 수 있습니다. 대부분의 사용 사례는 Amazon S3를 사용하여 공개 자산을 호스팅하는 경우(예를 들어, 퍼블릭 웹 사이트에 사용할 이미지를 호스트)가 아니면, Amazon S3 버킷에서 파일을 읽기 위해 광범위한 공개 액세스가 필요하지 않으며, 공개 액세스를 제공하지 않는 것이 모범 사례입니다.	예	예	
1.18 S3 버킷 또는 객체 공개 여부를 탐지하는 모니터링 메커니즘 구현	Amazon S3 버킷이 공개될 때 이를 파악할 수 있도록 모니터링 또는 알림 기능이 마련되어 있어야 합니다. 이에 대한 한 가지 옵션은 AWS Trusted Advisor를 사용하는 것입니다. AWS Trusted Advisor는 Amazon S3에서 공개 액세스 권한이 있는 버킷이 있는지 점검합니다. 모든 사용자에게 List 액세스 권한을 부여하는	예	아니요	

	버킷 권한은 의도하지 않은 사용자가 버킷의 객체를 자주 나열할 경우 예상보다 높은 요금으로 이어질 수 있습니다. 모든 사용자에게 Upload/Delete 액세스 권한을 부여하는 버킷 권한은 사용자가 버킷 항목을 추가하거나, 수정하거나, 제거할 수 있기 때문에 잠재적 보안 취약점이 발생하는 원인이 됩니다. Trusted Advisor 점검 항목은 명시적인 버킷 권한뿐 아니라 버킷 권한을 재정의할 수 있는 관련 버킷 정책도 확인합니다.			
1.19 Amazon EC2 인스턴스 및 컨테이너의 변경 사항을 탐지하는 모니터링 메커니즘 구현	Amazon S3 인스턴스 또는 컨테이너의 변경 사항은 무단 활동을 의미할 수 있으며, 최소한 향후 포렌식 조사가 가능하도록 안정적인 위치에 기록해야 합니다. 이 목적을 위해 사용되는 메커니즘은 적어도 다음 요구 사항을 충족해야 합니다. 1. 솔루션에 사용되는 Amazon S3 인스턴스 또는 컨테이너에서 OS 또는 애플리케이션 파일에 대한 모든 변경 사항을 탐지하고, 2. 이러한 변경 사항을 기록한 데이터를 Amazon S3 인스턴스 또는 컨테이너의 외부에 있는 안정적인 위치에 저장해야 합니다. 적절한 메커니즘의 예: a. 예정된 구성 관리(예: Chef, Puppet 등) 또는 전문 도구(예: OSSEC, Tripwire 등)를 통한 파일 무결성 점검 배포, b. 구성 관리 도구를 확장하여 Amazon S3 호스트 구성을 검증하고, 런타임 중에 서비스가 모든 범위 내 호스트에서 작동 가능한 상태로 유지되도록 구성된 'canary'(기록된 no-op) 이벤트를 통해 주요 구성 파일 또는 패키지에 대한 업데이트를 알림, 또는 c. ElasticSearch 및 Kibana를 사용한 OSSEC 등의 오픈 소스 솔루션과 같은 호스트 침입 탐지 시스템을 배포하거나 파트너 솔루션을 사용. 다음 메커니즘은 이 요구 사항을 충족하지 않습니다. a. 자주 순환되는 Amazon S3 인스턴스 또는 컨테이너.	예	아니요	
1.20 모든 데이터 분류	워크로드에서 처리 및 저장되는 모든 고객 데이터를 고려하고 분류하여 민감도와 처리 시 사용할 적절한 방법을 결정합니다.	예	예	
1.21 모든 민감한 데이터를 암호화	민감한 데이터로 분류된 모든 고객 데이터를 전송 및 저장 중 암호화합니다.	예	예	
1.22 안전하게 암호화 키 관리	모든 암호화 키는 저장 및 전송 중 암호화되며, 키를 사용하기 위한 액세스 권한은 AWS Key Management Service(KMS) 같은 AWS 솔루션 또는 HashiCorp Vault 같은 파트너 솔루션을 사용하여 제어됩니다.	예	예	
1.23 모든 전송 중 데이터 암호화	Amazon Virtual Private Cloud 경계에서 전송 중인 모든 데이터는 암호화됩니다.	예	예	
1.24 보안 인시던트 대응 프로세스 정의 및 리허설	AWS 계정 침해와 같은 인시던트를 처리하기 위한 보안 인시던트 대응 프로세스가 정의되어 있어야 합니다. 이 프로세스는 예를 들어 보안 실전 훈련을 하는 등 인시던트 대응 프로세스를 리허설하는 절차를 구현하여 테스트해야 합니다. 직전 12개월 이내에 연습을 실시하여 다음 사항을 확인한 상태여야 합니다. a. 적절한 사람들이 환경에 대한 액세스 권한을 보유하고 있고, b. 적절한 도구를 사용 가능하며, c. 적절한 사람들이 계획에 정의된 다양한 보안 인시던트에 대응하는 방법을 알고 있는 확인해야 합니다.	예	아니요	
1.25 결제 카드 업계(PCI) 데이터 보안 표준(DSS) - 인증 또는 SAQ	카드 소유자 데이터가 있는 전자 상거래, 통합 상거래 및 판매 시점 애플리케이션의 경우, 워크로드에 대한 결제 카드 업계(PCI) 데이터 보안 표준(DSS) 범위를 매년 평가하는 프로세스가 마련되어 있습니다. 범위 평가를 기반으로 필요에 따라 PCI DSS 인증 또는 SAQ 가 수행됩니다. 증거 자료는 PCI DSS 인증에 대한 규정 준수 보고서 또는 작성한 자체 평가 질문서(SAQ)의 형식이어야 합니다.	예	예	

1.26 PCI 데이터의 엔드 투 엔드 암호화	카드 소유자 데이터가 있는 전자 상거래, 통합 상거래 및 판매 시점 애플리케이션의 경우 Amazon VPC 내에서도 데이터가 전송 중에 암호화됩니다.	예	예	
1.27 DDoS(분산 서비스 거부) 공격에 대비한 보호 조치	Open Systems Interconnection(OSI) 모델의 모든 계층에서 DDoS(분산 서비스 거부) 공격을 완화하는 인프라 및 서비스를 제공합니다.	예	아니요	
1.28 10 가지 주요 Open Web Application Security Project(OWASP) 공격을 완화하기 위한 메커니즘	Open Web Application Security Project(OWASP) 취약성을 완화하는 인프라 및 서비스를 제공합니다.	예	아니요	
2.0 안정성 안정성 원칙은 비즈니스 및 고객 요구를 충족하기 위해 장애를 예방하고 신속하게 복구할 수 있는 기능에 중점을 둡니다. 주요 주제로는 설정을 중심으로 하는 기본 요소, 교차 프로젝트 요구 사항, 복구 계획 및 변경 처리 방법을 들 수 있습니다.				
2.1 네트워크 연결 가용성 우수	솔루션에 대한 네트워크 연결 가용성이 뛰어나야 합니다. VPN 또는 AWS Direct Connect를 사용하여 고객 네트워크와 연결하는 경우, 고객이 항상 중복 연결을 구현하지 않더라도 솔루션은 이를 지원해야 합니다.	예	예	
2.2 비즈니스 요구 사항에 맞는 인프라 규모 조정 메커니즘	인프라 규모 조정 메커니즘은 1. 각 아키텍처 계층에서 Auto Scaling 메커니즘을 구현하거나, 2. 비용 요구 사항 및 예상 사용자 증가율을 비롯한 현재 비즈니스 요구 사항에 Auto Scaling 메커니즘이 필요하지 않음을 확인하고 수동 규모 조정 절차가 완전히 문서화되고 수시로 테스트되는지 확인하여 비즈니스 요구 사항에 부합해야 합니다.	예	예	
2.3 중앙에서 AWS 및 애플리케이션 로그 관리	애플리케이션 및 AWS 인프라의 모든 로그 정보는 단일 시스템으로 통합되어야 합니다.	예	아니요	
2.4 중앙에서 AWS 및 애플리케이션의 모니터링과 경보 관리	애플리케이션 및 AWS 인프라는 중앙에서 모니터링하고, 생성된 경보는 담당 운영 직원에게 전송해야 합니다.	예	아니요	
2.5 인프라 프로비저닝 및 관리 자동화	솔루션이 AWS CloudFormation 또는 Terraform과 같은 자동화된 도구를 사용하여 AWS 인프라를 프로비저닝하고 관리해야 합니다. 프로덕션 AWS 인프라에 대한 일상적 변경을 수행하는 데 AWS 콘솔을 사용해서는 안 됩니다.	예	예	
2.6 정기적으로 데이터 백업 수행	내구성이 뛰어난 스토리지 서비스에 정기적으로 백업해야 합니다. 백업을 통해 관리, 논리적 또는 물리적 오류 시나리오에서 복구할 수 있습니다. Amazon S3 및 Amazon Glacier는 백업 및 아카이브에 적합한 서비스입니다. 두 서비스 모두 내구성이 뛰어나고 저렴한 스토리지 플랫폼입니다. 또한, 무제한 용량을 제공하므로 백업 데이터 세트가 증가하더라도 볼륨 또는 미디어 관리가 필요하지 않습니다. 사용량에 따라 지불하는 요금 모델과 저렴한 월별 GB당 사용 요금 덕분에 이 서비스는 데이터 보호 사용 사례에 적합합니다.	예	예	
2.7 정기적으로 그리고 주요 아키텍처 변경 후 복구 메커니즘 테스트	정기적으로 그리고 클라우드 환경을 크게 변경한 후에는 복구 메커니즘 및 절차를 테스트해야 합니다. AWS는 데이터 백업 및 복구를 관리하는 데 도움이 되는 실질적인 리소스를 제공합니다.	예	아니요	

2.8 솔루션이 가용 영역 중단에 대해 복원력 유지	단일 가용 영역 내 모든 서비스가 중단된 경우에도 솔루션은 계속 작동해야 합니다.	예	예	
2.9 솔루션의 복원력 테스트	지난 12개월 이내에 프로덕션 환경에서 단일 가용 영역 중단에 대한 인프라의 복원력을 테스트했습니다(예: 실전 연습을 통해).	예	아니요	
2.10 재해 복구(DR) 계획 정의	잘 정의된 재해 복구 계획은 복구 시점 목표(RPO) 및 복구 시간 목표(RTO)를 포함합니다. 모든 범위 내 서비스에 대해 RPO 및 RTO를 정의해야 하며, RPO 및 RTO는 고객에게 제공되는 SLA와 일치해야 합니다.	예	예	
2.11 24 시간 미만의 복구 시간 목표(RTO)	기준 요구 사항은 핵심 서비스에서 RTO가 24시간 미만이어야 합니다.	예	아니요	
2.12 재해 복구(DR) 계획을 적절하게 테스트	DR 계획은 정기적으로 그리고 주요 업데이트 후에 복구 시점 목표(RPO) 및 복구 시간(RTO) 에 대해 테스트해야 합니다. AWS APN 어드밴스드 티어를 승인하기 전에 DR 테스트를 최소한 한 번은 완료해야 합니다.	예	아니요	
2.13 다른 리전으로의 복구가 포함된 재해 복구(DR) 계획	DR 계획은 다른 AWS 리전으로의 복구를 위한 전략을 포함해야 하며, 정기 복구 테스트에서 이 시나리오를 테스트해야 합니다. 지난 12개월 이내에 다른 AWS 리전으로의 복구를 비롯하여 DR 계획에 대한 전체 테스트를 최소한 한 번은 완료했어야 합니다. 참고: 테스트 환경으로 데이터 복구 또는 사용자를 위해 데이터 내보내기 프로세스가 백업을 확인하는 유용한 방법이지만, 이러한 프로세스는 다른 AWS 리전으로의 전체 복원 테스트를 수행해야 하는 요구 기준을 충족하지 못합니다.	예	아니요	
3.0 운영 우수성 운영 우수성 원칙은 비즈니스 가치를 제공하기 위해 시스템을 실행 및 모니터링하고 지속적으로 프로세스와 절차를 개선하는 데 중점을 둡니다. 주요 주제로는 변경 관리 및 변경 자동화, 이벤트에 대한 응답, 일상적인 작업을 성공적으로 관리하기 위한 표준 정의 등이 있습니다.				
3.1 코드 변경 배포 자동화	솔루션은 자동화된 방법을 사용하여 AWS 인프라에 코드를 배포해야 합니다. AWS 인프라에 업데이트를 배포하는 데 대화형 Secure Shell(SSH) 또는 Remote Desktop Protocol(RDP) 세션을 사용하면 안 됩니다.	예	아니요	
3.2 런북 및 에스컬레이션 프로세스 정의	다양한 애플리케이션 및 AWS 이벤트에 대응하는 데 사용되는 표준 절차를 정의하는 런북을 개발해야 합니다. 시스템에서 생성한 알림 및 경보를 처리하고 고객이 보고한 인시던트에 대응할 수 있도록 에스컬레이션 프로세스를 정의해야 합니다. 에스컬레이션 프로세스에는 필요한 경우 AWS Support로 애스컬레이션하는 내용이 포함되어야 합니다.	예	아니요	
3.3 AWS 계정에 대해 AWS Business Support 활성화	Business Support가 활성화되어야 합니다. Business Support(또는 그 이상)는 어드밴스드 티어 기술 파트너의 APN 파트너 네트워크 요구 사항 중 하나입니다. 어드밴스드 티어 자격을 갖추려면 하나 이상의 AWS 계정에서 Business Support를 활성화해야 합니다.	예	아니요	
4.0 성능 효율성 성능 효율성 기반은 IT 및 컴퓨팅 리소스를 효율적으로 사용하는 데 중점을 둡니다. 주요 주제에는 워크로드 요구 사항을 기반으로 적합한 리소스 유형 및 크기 선택, 성능 모니터링, 그리고 비즈니스 요구 사항 변화에 따라 효율성을 유지할 수 있도록 정보에 근거한 의사 결정이 포함됩니다.				
4.1 배포 후 활성화되는 성능 테스트	측정 가능한 성능 목표를 정의하고, 프로덕션 단계에 릴리스하기 전에 성능 테스트를 통해 이러한 성능 목표를 충족하는지 확인합니다.	예	예	
4.2 임계값 모니터링 적용	애플리케이션 성능을 모니터링하고, 임계값을 위반할 경우 경보를 트리거하도록 하는 메커니즘을 적용합니다.	예	예	

AWS 리소스:

제목	설명
활동 랜딩 페이지를 작성하는 방법	프로그램의 사전 조건을 충족하는 활동/솔루션 페이지를 작성하는 방법에 대한 지침을 제공합니다.
공개 사례 연구 작성 방법	프로그램의 사전 조건을 충족하는 공개 고객 사례 연구를 작성하는 방법을 안내합니다.
아키텍처 다이어그램 구축 방법	프로그램의 사전 조건을 충족하는 아키텍처 다이어그램을 생성하는 방법을 안내합니다.
파트너 준비 문서	프로그램 사전 조건의 지침 및 모범 사례 예를 제공합니다.
AWS Well Architected 웹 사이트	Well Architected 모범 사례를 설명합니다.