SaaS 제품 AWS 용의 네트워킹 연결 옵션

AWS 권장 가이드

AWS 권장 가이드: SaaS 제품 AWS 용의 네트워킹 연결 옵션

Table of Contents

SaaS 제품 AWS 용의 네트워킹 연결 옵션

Tomas Sykora 및 Luca Schumann, Amazon Web Services

2025년 9월(문서 기록)

이 가이드에서는 소비자 애플리케이션을 서비스형 소프트웨어(SaaS) 공급자에 연결하는 일반적인 시나리오를 살펴봅니다. 온프레미스, , 다른 클라우드 서비스 제공업체(CSP) 클라우드 또는 하이브리드 아키텍처에 있는 리소스 AWS 클라우드에 연결하는 방법을 설명합니다. 이러한 시나리오에는 다음이 포함됩니다.

- HTTPS를 통한 웹 서비스 노출
- TCP 기반 서비스 노출
- AWS AppSync를 사용하여 게시-구독(Pub/Sub) 및 GraphQL APIs 구현
- AWS 리소스를 사용하여 실시간 애플리케이션용 WebSockets 노출
- 대화형 서비스 통신을 위한 양방향 액세스 활성화

SaaS 공급자는이 가이드에서 다루는 모범 사례에 따라 고객의 신뢰를 높이고 SaaS 제품에 대한 확장 가능하고 안전하며 탄력적인 액세스를 지원할 수 있습니다.

이 가이드에는 SaaS 제품의 소비자 네트워킹 요구 사항을 얼마나 성공적으로 충족하는지 평가하는 데 도움이 되는 자체 평가 기준도 포함되어 있습니다. 연결 패턴 외에도 AWS 네트워킹 서비스의 포괄적인 비교, 다양한 배포 시나리오를 위한 상위 수준 아키텍처 다이어그램, 특정 비즈니스 컨텍스트에 따라 올바른 접근 방식을 선택하는 방법에 대한 실용적인 지침을 확인할 수 있습니다. 이 가이드에서는 각 네트워킹 옵션의 보안 고려 사항을 살펴보고, 피해야 할 일반적인 위험에 대해 설명하고, 기술 요구 사항과 운영 효율성의 균형을 맞추는 구현 권장 사항을 제공합니다. 또한 네트워킹 결정을 비즈니스 모델, 성장 목표 및 규정 준수 요구 사항에 맞게 조정하기 위한 전략적 프레임워크를 찾을 수 있습니다.

대상 독자

이 가이드는 SaaS 공급자를 대상으로 합니다. 에서 SaaS 제품의 네트워크 연결을 설계, 구현 및 최적화하는 클라우드 아키텍트, 제품 관리자 및 네트워크 엔지니어에게 도움이 됩니다 AWS 클라우드. 이 가이드의 개념과 권장 사항을 이해하려면 AWS 기본 사항, 핵심 SaaS 개념 및 상위 수준 네트워킹 원칙을 숙지해야 합니다.

목표

이 가이드에서는 소비자가 SaaS 제품에 대한 액세스를 최적화하는 데 도움이 되는 네트워크 아키텍처 옵션과 현장 테스트를 거친 모범 사례를 설명합니다. 이 가이드의 권장 사항을 구현하면 다음을 지원합니다.

- 통합 용이성 - 온보딩부터 프로덕션까지 복잡하지 않은 고객 여정을 제공하여 고객의 가치 실현 시간을 단축하고 수익 인식 주기를 단축할 수 있습니다.
- 적응성 - 변화하는 요구 사항에 맞게 조정하여 고객의 기존 네트워크 인프라와 원활하게 통합합니다. 이렇게 하면 제품의 가치 제안이 향상됩니다.
- 총 소유 비용 - 네트워크 액세스를 표준화하여 변경 비용 및 테넌트당 비용을 줄입니다. 배포 일관성을 개선하면 근본 원인 분석 또는 복구를 수행하는 시간을 줄일 수도 있습니다.
- 종속성 관리 - 다양한 네트워크 액세스 옵션의 종속성, 장기 영향 및 장단점을 이해합니다. 이렇게 하면 제품 리더가 정보에 입각한 제품 결정을 내리는 데 도움이 됩니다.
- 구성성 및 확장성 - 핵심 기능 개발을 운영 인프라와 분리합니다. 이렇게 하면 개발 팀이 더 빠르게 움직이고 고객을 위한 가치 창출에 집중할 수 있습니다.
- 신뢰 구축 - SaaS 제품에 대한 복원력, 내결함성, 보안 및 확장 가능한 액세스를 제공하여 규제 위험을 줄이고 고객의 성장을 지원하는 능력에 대한 신뢰를 얻을 수 있습니다.

SaaS 제품에 대한 네트워크 액세스 결정 평가

시장 이해

네트워킹에 대해 지금 내리는 결정에 따라 SaaS 제품의 가치 제안을 고객에게 제공할 수 있는지 여부가 결정됩니다. 이러한 결정의 전략적 중요성에도 불구하고 SaaS 제품에 대한 액세스를 제공하는 것은 종종 순수한 기술적 주제로 인식됩니다. 이러한 인식에 수반되는 위험에는 수익 인식 주기 연장, 운영 비효율성, 비즈니스 전략과의 불일치가 포함됩니다. 예를 들어 신속한 확장이 전략적 비즈니스 목표인 경우, 고려 중인 솔루션이 확장을 지원할 수 있을 만큼 확장 가능하고 유연한지 여부에 따라 의사 결정 프로세스를 안내해야 합니다. 비즈니스 성장에 성공하더라도 운영 오버헤드가 향후 성장의 장애물이 되어서는 안 되며 잘못 정렬된 비용 구조는 모든 수익을 소비할 수 있습니다.

예를 들어 다음 시장 고려 사항이 네트워킹과 같은 제품의 기술적 측면에 미치는 영향을 고려합니다.

- 비즈니스 모델이 구독 기반인 경우 고객은 대규모 선결제 투자보다는 예측 가능하고 반복적인 비용이 있는 솔루션을 선호할 가능성이 높습니다.
- 비즈니스 전략이 높은 가치의 엔터프라이즈 수준 고객을 대상으로 하는 경우 보안, 거버넌스 및 규정 준수 기준에 따라 SaaS 제품을 고려할지 여부가 결정됩니다.
- 대상 시장이 대부분 스타트업인 경우 통합 용이성, 가치 실현 시간 및 적응성이 중요한 요인일 수 있습니다. 시작은 일반적으로 속도와 민첩성을 우선시합니다. 브랜드를 구축하고 수익을 빠르게 창출해야 하므로 빠르고 통합하기 쉬운 솔루션을 선호하고, 비용 효율적으로 확장할 수 있으며, 전문가에 대한 종속성을 줄이고, 귀중한 주기를 연결하지 않을 가능성이 높습니다.
- 일부 비즈니스에는 안정적이고 처리량이 많으며 지연 시간이 짧은 액세스가 필요합니다. 여기에는 엔터테인먼트 및 미디어 산업, 제조 및 금융 거래 처리가 포함됩니다. 이러한 고객이 대상 고객인 경우 신뢰성이 주요 관심사입니다.

이러한 모든 경우 네트워킹 액세스가 원활하지 않으면 고객은 정상인 SaaS 오퍼링을 인식할 수 있습니다. 네트워킹이 장애물이 되는 경우 비즈니스 사례를 지원하지 않습니다. 고객이 제공하는 서비스에 안정적으로 액세스할 수 없는 경우 SaaS 제품의 가치 제안은 nil입니다.

역할 이해

비즈니스 목표를 지원하는 데 있어 여러분의 역할은 여러분이 누구인지, 특정 개인 및 팀 목표가 무엇인지, 고객이 누구인지, 무엇이 중요한지에 따라 달라집니다. 일반적으로 고객과 상호 작용하는 팀의 일원이 아니더라도 고객이 누구인지, 무엇이 필요한지 걱정해야 합니다. 엔지니어링 및 개발 팀은 내부

고객, 특히 정기적으로 상호 작용하는 고객과도 우려해야 합니다. 일반적으로 운영 및 고객 성공 팀입니다.

영업 조직의 일원인 경우 단순한 기술 주제인 것처럼 보이지만 네트워킹에 대해 제품 및 엔지니어링 팀과 소통하는 것이 중요합니다. 대상 시장 구조에 대한 인사이트를 공유합니다. 기존 및 잠재적 고객과 파트너의 요구 사항과 문제점을 전달합니다. 놓친 기회, 세그먼트당 예측 성장 및 이벤트에 대한 데이터와 일화를 공유합니다. 비즈니스 성장을 지원하는 조직의 역량에 문제가 되는 질문을 합니다. 이렇게 하면 기회 수가 증가하고 비즈니스의 장기적인 수익성이 향상됩니다. 궁극적으로 이는 조직이 미래 확장 및 개발에 자금을 지원하는 데 도움이 됩니다.

엔지니어링 조직의 일원인 경우 솔루션 초안을 작성하기 전에 조직의 비즈니스 전략을 이해합니다. 비즈니스 전략에 맞게 조정하면 다양한 네트워크 액세스 옵션을 평가하는 데 적합한 지표를 선택하는 데 도움이 됩니다. 또한 조직이 성장함에 따라 비용이 많이 드는 대규모 네트워크 재설계를 방지할 수 있습니다. 비즈니스 조정은 팀이 향후 문제에 필요한 리소스를 보호하고 유지하는 데 도움이 됩니다. 팀의 인력, 전문성 개발을 위한 예산 또는 최첨단 기술에 대한 액세스는 비즈니스 조정을 입증하는 능력에 따라 달라집니다. 결정이 조직의 비즈니스 성공에 어떻게 기여했는지 보여주는 것이 가장 좋습니다. 따라서 지표 선택 기준을 포함하여 의사 결정 프로세스를 캡처하는 것이 좋습니다. 지표를 정기적으로 검토하여 비즈니스 목표에 부합하는지 확인합니다. 이렇게 하면 팀이 받을 자격이 있는 크레딧을 얻는 데 도움이 될 수 있습니다. 또한 정기적 검토는 팀이 가정이나 더 이상 사용되지 않는 과거 이유를 기반으로 결정을 내리지 않는지 확인하는 데 도움이 됩니다.

다음 섹션의 지표 목록은 네트워킹 액세스와 관련이 있습니다.

- 제품 및 상용 지표
- 네트워킹 결정에 영향을 미치는 엔지니어링 지표

이 가이드는 전체적으로 이러한 지표의 하위 집합을 사용하여 SaaS 제품에 대한 최적의 네트워크 액세스 접근 방식을 식별하는 데 도움이 됩니다. 비즈니스와 가장 중요하고 관련성이 높은 지표를 선택한 다음 해당 지표를 기반으로 접근 방식을 평가합니다.

네트워킹 결정에 영향을 미치는 제품 및 상용 지표

제품 및 상업 팀은 성공 기준을 사용하여 비즈니스 목표를 충족하는지 평가합니다. 이 섹션에서는 조직이 내리는 네트워킹 액세스 결정의 긍정적 또는 부정적 영향을 받을 수 있는 제품 또는 상용 지표에 대해 설명합니다.

이러한 지표 및 자체 평가 질문을 사용하여 네트워크 액세스 접근 방식이 비즈니스 입지 및 시장 전략에 어떻게 부합하는지 평가합니다. 이 평가를 통해 현재 네트워킹 결정이 회사의 시장 차별화, 경쟁 우위 및 대상 고객 요구 사항을 지원하는지 확인할 수 있습니다.

이 섹션에는 다음 주제에 대한 지표 및 자체 평가 질문이 포함되어 있습니다.

- 비즈니스 모델 및 시장 입지
- 총 주소 지정 가능 시장, 신규 클라이언트 확보율, 성장 및 확장성
- 고객 경험 및 보존
- 효율성 및 재무 성과
- 규정 준수 및 위험 관리
- 파트너 전략

비즈니스 모델 및 시장 입지

이러한 지표는 경쟁 차별화, 시장 도달 범위, 브랜드 인식을 포함하여 시장에서의 회사 입지와 관련이 있습니다. 네트워크 액세스 접근 방식과 비즈니스 모델 간의 조정을 평가하는 것이 중요합니다. 구독 기반, 사용량 기반, 프리미엄, 계층형, 마켓플레이스, API 우선 또는 화이트 레이블 여부에 관계없이 평가를 수행합니다. 모델이 조직의 목표와 고객의 목표를 지원하는지 확인합니다.

높은 점수 기준

네트워크 액세스 접근 방식은 비즈니스 모델에 원활하게 부합합니다. 이를 통해 서비스의 채택 및 제공을 용이하게 할 수 있습니다. 비즈니스 모델의 장기적인 재무적 실행 가능성을 지원하며 비용 구조는 예상 성장과 호환됩니다. 제품을 채택할 때 고객 또는 파트너의 마찰을 최소화합니다. 이렇게 하면 사용자 경험이 향상되고 서비스의 광범위한 활용이 장려됩니다.

점수가 낮은 지표

선택한 네트워크 액세스 접근 방식이 지원해야 하는 비즈니스 모델에 맞지 않습니다. 비용 구조와 배포 소요 시간은 대상 시장에서 채택하는 데 방해가 됩니다. 지속적인 인프라 및 운영 비용은 잠재적 이익을 저해합니다. 이렇게 하면 비즈니스 성장이 방지되고 의도한 규모로 운영하기가 어려워집니다. 또는 네트워크 액세스 접근 방식의 속성으로 인해 고객이 규제상의 이유로 서비스를 고려하지 못할 수 있습니다.

자체 평가 질문

- 초기 배포 및 지속적 전달을 위해 선택한 네트워크 액세스 접근 방식의 비용 영향은 무엇입니까? 접근 방식의 고정 및 가변 비용은 얼마입니까?

- 네트워크 액세스 접근 방식을 비즈니스 모델의 성장 요구 사항에 맞게 효과적이고 효율적으로 확장할 수 있습니까? 개별 테넌트 크기와 온보딩된 테넌트 수를 고려합니다.
- 네트워크 액세스 접근 방식은 비즈니스 모델의 유연성 또는 적응성을 제한할 수 있는 기술적 또는 운영상의 제한을 부과하나요?
- 네트워크 액세스 접근 방식의 경우 배포 리드 타임은 비즈니스 모델에 필요한 시장 출시 속도와 어떻게 일치하나요?

총 주소 지정 가능 시장, 신규 클라이언트 확보율, 성장 및 확장성

네트워킹 결정이 조직의 역량에 미치는 영향을 평가하여 새로운 시장으로 확장하고 고객을 효과적으로 확보하며 운영 확장성을 유지하는 것이 중요합니다. 이러한 요인은 변환 속도에 영향을 미칩니다. 또한 네트워크 액세스 접근 방식이 중요한 시장 세그먼트로의 확장을 지원하는지 아니면 특정 고객 유형에만 서비스를 제공하도록 제한하는지에 영향을 미칩니다.

높은 점수 기준

네트워크 액세스 접근 방식은 조직이 대상 시장 중 상당 부분에 도달하는 데 도움이 되거나 다른 네트워크 접근 방식과 효과적으로 결합하여 시장 범위를 확장할 수 있습니다. 이 접근 방식에는 최소한의 추가 통합 노력이 필요합니다. 이 접근 방식은 배포, 신속한 시장 진입 및 확장을 위한 짧은 리드 타임을 지원합니다. 많은 수의 병렬 배포를 허용합니다. 통합은 고객에게 간단하므로 채택 장벽을 줄이고 고객 경험을 개선합니다. 이 접근 방식은 운영 오버헤드를 최소화하고 운영 용량을 유지하며 성장 예측을 지원합니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 대상 시장 중 일부만 지원하거나 주로 비즈니스 전략에서 우선순위가 지정되지 않은 틈새 세그먼트에 적합합니다. 이미 지원되는 다른 네트워크 액세스 접근 방식을 효과적으로 보완하지는 않습니다. 배포 지연 시장 수요의 리드 타임은 시장 확장과 신규 클라이언트 확보를 제한합니다. 배포 모델은 순차적이므로 수요가 증가함에 따라 서비스 병목 현상의 위험이 증가합니다. 복잡한 통합 프로세스는 잠재적 클라이언트를 방지하여 획득률 및 변환률에 부정적인 영향을 미칩니다. 운영 오버헤드가 크면 조직의 운영 용량이 감소합니다. 이는 예상 성장의 차단 요인이 됩니다.

이러한 지표의 경우 새로운 네트워크 액세스 접근 방식을 도입하면 조직이 전략적 비즈니스 목표를 달성하는 데 도움이 될 수 있는지 평가합니다. 새로운 네트워크 액세스 접근 방식이 원하는 결과를 제공하지 않고 새로운 제품 종속성을 생성하거나 운영 리소스를 소비할 수 있는지 고려합니다.

자체 평가 질문

- 현재 접근 방식에 대상 시장에서 더 큰 세그먼트에 도달하지 못하는 격차가 있습니까?

- 대상 시장 중 70~90%를 차지하기 위해 지원해야 하는 중첩되지 않는 표준화된 네트워크 액세스 접근 방식의 최소 세트는 무엇입니까?
- 각 네트워크 액세스 접근 방식은 어떤 범위를 지원하며 인프라 비용, 운영 주기, 전문가에 대한 종속성과 같은 중요한 지표의 관련 증가는 무엇입니까?
- 네트워크 인프라의 배포 기능 및 서비스 제한은 대상 시장에서의 성장 기대치와 어떻게 일치하나요?
- 네트워크 통합으로 인해 신규 고객의 진입에 장벽이 생기나요? 변환율을 개선하기 위해 이러한 문제를 해결하려면 어떻게 해야 하나요?
- 네트워크 관리의 운영 오버헤드는 성장 및 확장성 용량에 어떤 영향을 미치나요?
- 네트워크 배포의 리드 타임을 줄이고 시장 확장 및 고객 확보를 개선하기 위해 구현할 수 있는 전략은 무엇입니까?
- 고객 에코시스템과의 배포 또는 통합을 지연시킬 수 있는 전문가 리소스에 대한 종속성이 있나요?

고객 경험 및 보존

이 섹션의 지표는 조직의 고객 확보 및 유지 능력을 이해하는 데 도움이 됩니다. 네트워킹 액세스 접근 방식과 고객 만족도 간의 관계를 이해하면 제품 및 엔지니어링 팀이 데이터로 정보에 입각한 결정을 내리는 데 도움이 될 수 있습니다.

높은 점수 기준

네트워크 액세스 접근 방식은 안정적이고 관리하기 쉽습니다. 이는 높은 고객 만족도(CSAT) 및 순 촉진자 점수(NPS) 결과에 기여합니다. 이러한 점수는 강력한 브랜드 평판과 고객 충성도를 나타냅니다. 고객의 기존 에코시스템과의 원활한 통합 덕분에 채택 마찰이 적고 전문가에 대한 의존도가 낮습니다. 조직은 고객 신뢰 및 계약 의무를 강화하는 서비스 수준 계약(SLAs)을 일관되게 충족합니다. 고객은 안정적이고 신뢰할 수 있는 서비스를 누릴 수 있으므로 고객 유지율이 높습니다.

점수가 낮은 지표

서비스에 대한 통합이 어렵고 일관성 없는 액세스는 일반적으로 고객 불만과 부정적인 피드백으로 이어집니다. 이로 인해 브랜드 평판이 손상됩니다. 신규 고객은 전문가에 대한 종속성 또는 온보딩 및 통합 시간 연장으로 인해 무료 또는 평가판에서 유료 서비스로 전환하지 못합니다. SLAs를 자주 충족하지 못하면 벌금이 부과되고 신뢰도가 저하되어 잠재적으로 고객 보존률이 낮아질 수 있습니다.

자체 평가 질문

- 네트워크 성능(예: 속도, 가동 시간 및 지연 시간)은 CSAT 및 NPS 결과에 어떤 직접적인 영향을 미치나요? 이러한 점수를 높일 수 있는 구체적인 네트워크 개선 사항은 무엇입니까?

- 현재 네트워크 지연 시간 및 가동 시간 지표는 초기 사용자 경험 및 채택률에 어떤 영향을 미치나요? 이러한 지표를 최적화하려면 어떤 구체적인 네트워크 성능 개선이 필요합니까?
- 네트워크 구성 또는 보안 설정에서 신규 고객의 통합을 복잡하게 만드는 문제가 반복적으로 발생하나요? 이러한 프로세스를 어떻게 간소화할 수 있습니까?
- 네트워크 액세스를 쉽게 구성하면 신규 사용자의 온보딩 경험에 어떤 영향을 미치나요? 초기 사용자 노출을 개선하기 위해 최적화할 수 있는 특정 네트워크 액세스 포인트 또는 리드 타임이 있나요?
- 새 클라이언트에 대한 네트워크 서비스 프로비저닝을 자동화하기 위한 과제는 무엇입니까? 확장성과 안정성을 개선하기 위해이 프로세스를 조정하려면 어떻게 해야 하나요?
- 최근 SLA 위반의 근본 원인을 분석합니다. 네트워크 구성, 용량 계획 또는 외부 공급업체 문제와 관련이 있었나요?
- 네트워크 문제로 인해 SLA 약정을 놓치는 빈도는 얼마나 됩니까? 가장 빈번한 네트워크 관련 장애는 무엇입니까?
- 과거에 고객 만족도에 가장 크게 긍정적인 영향을 미친 네트워크 성능 개선 사항은 무엇입니까?

효율성 및 재무 성과

이 범주는 비용 효율성, 장기 실행 가능성, 수익성, 투자 수익률(ROI), 총 소유 비용(TCO)과 같은 비즈니스의 재무 상태 및 수익성 측면을 평가합니다. 표준화를 통해 네트워크 운영을 간소화하면 운영 오버헤드와 유지 관리 비용을 줄일 수 있습니다. 이는 조직의 성장 목표를 지원합니다.

높은 점수 기준

네트워크 액세스 접근 방식의 비용 구조는 비즈니스 모델과 잘 일치합니다. 지속 가능한 성장을 지원하고 수익성을 높이는 데 드는 상당한 비용 절감을 지원합니다. 효율적인 네트워크 액세스를 통해 신속한 고객 온보딩이 가능하므로 가치 제공 시간이 단축되고 시장 침투가 가속화됩니다. 이렇게 하면 수익 인식 주기가 직접적으로 단축됩니다.

점수가 낮은 지표

고객은 애플리케이션 및 서비스 제공을 가속화하기 위해 경쟁 업체에 의존하고 있습니다. 조직은 복잡하고 다양한 네트워크 구성과 관련된 운영 비용을 늘리고 리드 타임을 연장했습니다. 비용 구조와 비즈니스 모델이 잘못 정렬되어 구독 기반 서비스의 선결제 비용이 높아질 수 있습니다. 잘못된 온보딩 프로세스는 시장 침투를 줄이고 수익 인식을 연기합니다.

자체 평가 질문

- 새로운 서비스 배포의 현재 리드 타임은 무엇이며 출시 시간 및 수익 인식에 어떤 영향을 미치나요?

- 표준화된 네트워크 운영을 통해 오버헤드 및 유지 관리 비용을 얼마나 효과적으로 줄일 수 있습니까?
- 초기 통합을 성공적으로 완료하거나, 매일 운영하거나, 문제를 해결하거나, 변경 사항을 구현하는 데 전문가 리소스가 필요합니까?
- 기술 발전 측면에서 현재 네트워크 투자는 얼마나 지속 가능합니까? 예상되는 시장 개발에 맞는 미래 대비 기술에 투자하고 있습니까?
- 개별 테넌트의 네트워크 트래픽 및 사용과 관련된 비용을 얼마나 효과적으로 할당하고 추적하나요?

규정 준수 및 위험 관리

네트워크 관련 규정 준수를 검증하는 것이 근본적으로 중요합니다. 이렇게 하면 합법적으로 운영되고 고객 신뢰를 유지할 수 있습니다. 네트워크 운영 전반의 표준화는 규정 준수 프로세스를 간소화하고 다양한 관할 구역 및 지역 간의 일관성을 높입니다. 이러한 조치는 서비스를 확장하는 데 도움이 됩니다.

높은 점수 기준

네트워크 운영은 복잡성 없이 법률 표준을 일관되게 준수하므로 시장 확장에 기여하고 채택 마찰을 줄이며 고객 신뢰를 높입니다. 디지털 운영 복원력법(DORA) 및 미국 국립 표준 기술 연구소(NIST)와 같은 중요한 규제 프레임워크를 준수하면 규정 준수에 민감한 고객을 확보하는 데 도움이 됩니다. 규정 준수 상태를 지속적으로 파악하면 감사를 완료하는 데 필요한 시간이 단축됩니다.

점수가 낮은 지표

네트워크 규정 준수의 격차로 인해 높은 채택 마찰, 서비스 시작 지연, 법적 문제 및 잠재적 벌금이 발생합니다. 이러한 문제로 인해 신규 시장으로의 확장 계획이 지연되거나 취소됩니다. 다양한 관할권에서 표준 규정 준수 관행을 유지하기 어렵기 때문에 운영 효율성과 시장 평판에 영향을 미칩니다.

자체 평가 질문

- 네트워크 운영이 관련 규제 또는 업계 지침에 얼마나 잘 부합하나요? 최근 규정 준수 감사에서 밝혀야 했던 것은 무엇입니까?
- 디지털 및 네트워크 보안 영역에서 새로운 규정을 준수하려면 어떻게 해야 하나요?
- 문서화 및 보고 프로세스가 다양한 규제 기관의 요구 사항을 충족하는 데 얼마나 효과적입니까?
- 잠재적 규정 준수 위험이 법적 문제로 이어지기 전에 이를 식별하고 해결하기 위해 마련한 위험 관리 전략은 무엇입니까?
- 네트워크 액세스 접근 방식을 지원하기 위해 네트워크 관리 팀에 필요한 규정 준수 교육 및 인식 수준은 어느 정도입니까?

파트너 전략

네트워크 액세스 접근 방식이 인정받는 파트너, 플랫폼 및 마켓플레이스로 구성된 에코시스템에 얼마나 잘 부합하는지 평가합니다. 이는 특히 성장 전략이 파트너를 통한 규모 조정에 의존하는 경우에 필수적입니다.

높은 점수 기준

네트워크 액세스 접근 방식은 파트너 에코시스템 전체에 통합됩니다. 비용 구조는 주요 파트너의 비즈니스 모델에 잘 맞습니다. 파트너는 SaaS 제품을 원활하게 통합하는 데 필요한 네트워킹 기술을 보유하고 있으며 지속적인 액세스 및 기능을 제공할 수 있습니다.

점수가 낮은 지표

선택한 네트워크 액세스 접근 방식에는 희소하거나 조달하기 어려운 전문 기술, 리소스 또는 장비가 필요합니다. 플랫폼 및 마켓플레이스에서 일반적으로 사용하는 표준 네트워크 액세스 프로토콜과 다릅니다. 이로 인해 조정하기 어려운 예측할 수 없는 비용 구조가 생성됩니다. 네트워크 액세스 접근 방식이 주요 파트너의 비즈니스 모델에 맞지 않습니다.

자체 평가 질문

- 파트너에 대한 네트워크 액세스 접근 방식의 비용 영향은 무엇입니까? 이러한 비용은 비즈니스 모델에 어떻게 부합하나요? 통합의 어느 쪽에 대부분의 비용이 포함되고 몇 개의 운영 주기를 투자해야 합니까?
- 네트워크 액세스 접근 방식의 경우 파트너 관계 또는 에코시스템 확장성에 영향을 미칠 수 있는 통합 또는 유지 관리에 대한 장벽이 있습니까?
- 네트워크 액세스 접근 방식을 최적화하여 에코시스템 전반의 호환성과 통합 용이성을 강화하려면 어떻게 해야 합니까?

네트워킹 결정에 영향을 미치는 엔지니어링 지표

제품 및 상업 팀과 마찬가지로 엔지니어링 팀은 성공 기준을 사용하여 비즈니스 목표를 충족하는지 평가합니다. 그러나 이러한 지표는 서로 다르며 보안 및 규정 준수 요구 사항을 개발, 운영 및 충족하는 팀의 능력에 중점을 둡니다. 이 섹션에서는 조직이 내리는 네트워킹 액세스 결정의 긍정적 또는 부정적 영향을 받을 수 있는 엔지니어링 지표에 대해 설명합니다.

이러한 지표 및 자체 평가 질문을 사용하여 비즈니스 요구 사항 및 기술 역량과 비교하여 현재 네트워크 액세스 접근 방식을 평가합니다. 이 평가는 아키텍처의 격차를 식별하고 전략적 목표에 맞는 개선

사항의 우선순위를 정하는 데 도움이 됩니다. 이러한 기준을 정기적으로 검토하면 네트워크 액세스 전략이 고객의 요구 사항과 조직의 성장 계획을 모두 계속 지원할 수 있습니다.

이 섹션에는 다음 범주 및 주제에 대한 지표 및 자체 평가 질문이 포함되어 있습니다.

- 개발 지표
  - 배포 빈도, 배포 시간 및 스프린트 속도
  - 유연성 및 기능 제공
  - 실패율 변경
  - 코드 품질 및 엔지니어링 팀 성능
  - 기술 부채 감소
  - 확장성, 용량 및 성능
- 운영 우수성 지표
  - 운영 복원력 및 재해 복구
  - 서비스 및 애플리케이션 성능 모니터링
- 보안 및 거버넌스 지표
  - 보안, 규정 준수 및 취약성 관리

SaaS 제품의 네트워크 액세스와 관련된 개발 지표

이 섹션에는 다음 지표가 포함되어 있습니다.

- 배포 빈도, 배포 시간 및 스프린트 속도
- 유연성 및 기능 제공
- 실패율 변경
- 코드 품질 및 엔지니어링 팀 성능
- 기술 부채 감소
- 확장성, 용량 및 성능

배포 빈도, 배포 시간 및 스프린트 속도

개발 주기의 효율성을 최적화하려면 네트워크 스택 프로비저닝이 스프린트 속도에 미치는 영향을 이해해야 합니다.

높은 점수 기준

네트워크 스택 프로비저닝은 간소화되고 자동화되며 수동 개입을 최소화해야 합니다. 스프린트 속도에는 큰 영향을 미치지 않습니다. 네트워크 스택 프로비저닝 및 재배포는 모든 팀원이 수행할 수 있습니다. 이렇게 하면 특수 리소스에 대한 병목 현상과 종속성이 줄어듭니다.

점수가 낮은 지표

네트워크 스택을 프로비저닝하려면 많은 스토리 포인트가 필요합니다. 이는 새로운 기능의 개발을 방해하는 복잡하고 시간이 많이 걸리는 프로세스를 제안합니다. 네트워크 스택을 자주 재배포하면 상당한 시간과 비용 오버헤드가 발생합니다. 네트워크 프로비저닝 작업에는 병목 현상을 일으키고 개발 주기가 느려지는 전문 엔지니어링 전문 지식이 필요합니다.

자체 평가 질문

- 배포 프로세스와 관련된 수동 단계가 있는 경우 배포 빈도와 시간에 어떤 영향을 미치나요?
- 배포 실패 시 롤백은 어떻게 처리됩니까? 배포 빈도와 복구 시간에 미치는 영향은 무엇입니까?
- 새 환경을 설정할 때 네트워크 스택을 프로비저닝하는 데 필요한 스토리 포인트는 몇 개입니까?
- 개발 프로세스 중에 네트워크 스택을 자주 재배포하는 것과 관련된 추가 비용과 시간 오버헤드는 얼마나 됩니까?
- 네트워크 스택 프로비저닝은 전문 엔지니어링 전문 지식에 의존합니까, 아니면 팀원이 관리할 수 있는 작업입니까?

유연성 및 기능 제공

네트워크 액세스 접근 방식은 새로운 기능을 효율적으로 혁신하고 배포하는 엔지니어링 팀의 능력에 영향을 미칠 수 있습니다.

높은 점수 기준

네트워크 액세스 접근 방식은 빠르고 원활한 기능 배포에 필요한 유연성을 제공합니다. 다양한 통신 프로토콜, 단방향 및 양방향 통신, 메시지 크기를 지원합니다. 개발 프로세스 또는 혁신에 상당한 제약을 가하지 않습니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 지원되는 통신 프로토콜이 없거나, 메시지 크기가 유연하지 않거나, 특정 기술 및 관련 전문가 리소스에 의존하기 때문에 팀이 새로운 기능을 롤아웃하는 기능을 제한합니다. 이로 인해 개발 주기가 느려지고 서비스의 진화가 방해를 받을 수 있습니다.

자체 평가 질문

- 네트워크 액세스 접근 방식은 새로운 기능을 개발하고 배포하는 팀의 민첩성에 어떤 영향을 미치나요?
- 네트워크 액세스 접근 방식에 특정 통신 프로토콜 또는 기술의 지원을 제한하는 제한이 있나요?
- 이 접근 방식은 새로운 기술과 혁신의 서비스 통합을 어떻게 촉진하거나 제한하나요?
- 네트워크 액세스 접근 방식은 개발 타임라인과 제품 로드맵에 어떤 영향을 미치나요?

실패율 변경

선택한 네트워크 액세스 접근 방식은 새 서비스 또는 기능을 배포할 때 변경 실패율에 영향을 미칠 수 있습니다. 제어가 클수록 유연성이 향상되는 경우가 많지만 복잡한 라우팅 설정을 관리할 때와 같이 구성이 잘못될 가능성도 높아집니다.

높은 점수 기준

장애 위험을 최소화하면서 네트워크 스택에 대한 변경 사항을 구현할 수 있습니다. 충분한 테스트 메커니즘이 있고, 효율적인 롤백 메커니즘이 있으며, 효과적인 모니터링을 통해 문제를 신속하게 식별하고 해결할 수 있습니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 변경 중에 장애가 발생하기 쉽습니다. 제한된 테스트 옵션, 복잡한 배포 전략 또는 모니터링 및 문제 해결 기능 부족이 있습니다. 문제 해결 세션에는 여러 당사자가 참여해야 합니다. 이로 인해 가동 중지 시간이 증가하고 SaaS 제품의 가용성이 저하될 수 있습니다.

자체 평가 질문

- 네트워크 스택을 업데이트할 때 변경 실패 위험을 완화하기 위해 어떤 조치가 마련되어 있습니까?
- 철저한 테스트 및 검증 프로세스가 있습니까?
- 시스템은 실패한 변경에서 얼마나 빨리 복구할 수 있습니까? 효율적인 롤백 프로세스가 마련되어 있나요?
- 네트워크 스택 변경 중 및 변경 후 문제를 신속하게 감지하고 해결하기 위한 사전 모니터링 및 알림 시스템이 있습니까?
- 네트워크 스택 배포의 과거 변경 실패율은 얼마입니까? 과거 인시던트에서 어떤 교훈을 얻었나요?
- 네트워크 액세스 접근 방식은 변경 구현을 어떻게 촉진하거나 제한하나요? 접근 방식이 서비스 중단을 최소화하나요?

- 네트워크 액세스 접근 방식과 관련된 변경 사항을 배포할 때 프로덕션 환경에서 SaaS 제품의 가용성에 영향을 미칠 위험은 무엇입니까?

코드 품질 및 엔지니어링 팀 성능

네트워크 액세스 접근 방식은 SaaS 제품의 코드 품질에 간접적으로 영향을 미칠 수 있습니다. 네트워크 액세스의 표준화가 부족하면 엔지니어링 팀이 여러 통합 접근 방식을 지원해야 하므로 코드베이스가 팽창할 수 있습니다. 따라서 팀이 고성과 엔지니어링 팀을 유지하는 데 필요한 코드 품질을 심층적으로 개발하고 제어하는 데 방해가 될 수 있습니다.

높은 점수 기준

엔지니어링 팀은 지원되는 네트워크 액세스 접근 방식 전반에서 코드 모듈성과 재사용 가능성 덕분에 집중력을 유지합니다. 네트워크 액세스 접근 방식은 기존 배포 파이프라인 및 자동화된 테스트 전략과 호환됩니다.

점수가 낮은 지표

너무 많은 네트워크 액세스 접근 방식의 통합 및 유지 관리와 관련된 오버헤드로 인해 엔지니어링 팀 성능이 저하됩니다. 일부 접근 방식은 복잡성을 크게 높이거나, 기술 부채를 발생시키거나, 기능 누락 또는 부족을 해결하기 위한 해결 방법을 개발해야 합니다.

자체 평가 질문

- 네트워크 액세스 접근 방식은 네트워크 변동성을 어떻게 관리하나요?
- 연결 중단을 처리하기 위한 추가 코드를 개발해야 합니까?
- 새로운 네트워크 액세스 접근 방식이 기존 접근 방식과 원활하게 통합됩니까? 아니면 중요한 사용자 지정 개발이 필요합니까?
- 새로운 네트워크 액세스 접근 방식을 채택하는 데 필요한 변경 범위는 어느 정도입니까? 기존 코드베이스와 자동 테스트를 효과적으로 사용할 수 있나요?
- 선택한 네트워크 액세스 접근 방식을 사용하여 서비스를 배포하거나 재배포하는 것이 얼마나 쉽고 어렵나요? 이 작업을 자주 수행할 수 있습니까? 전문가 리소스에 대한 종속성이 있나요?
- 네트워크 액세스 접근 방식이 코딩 표준 및 모범 사례 준수를 용이하게 하거나 복잡하게 하나요?
- 이 접근 방식은 새로운 기능이나 수정 사항을 time-to-market 어떤 영향을 미칩니까?

기술 부채 감소

네트워크 액세스 접근 방식이 기술 부채에 미치는 영향을 평가하려면 확장성, 관찰성 및 보안 기능을 고려해야 합니다.

높은 점수 기준

이 접근 방식은 고객 기반이 확장됨에 따라 인프라 관리를 효과적으로 간소화합니다. 즉시 사용할 수 있는 강력한 관찰 기능을 제공합니다 out-of-the-box. 이렇게 하면 효율적인 모니터링 및 유지 관리가 촉진됩니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 통신 채널을 부적절하게 보호하고 정성적 지표 관찰을 위한 충분한 도구가 부족합니다. 또한 고객 기반이 증가함에 따라 인프라 관리를 위한 추가 개발이 필요하거나 신뢰성 문제에 대한 해결 방법이 필요할 수 있습니다.

자체 평가 질문

- 네트워크 액세스 접근 방식은 인프라의 장기 확장성에 어떤 영향을 미치나요? 추가 투자를 최소화하면서 원활한 성장을 촉진하나요?
- 포함된 관찰성 도구는 얼마나 포괄적입니까? 사전 모니터링 및 문제 해결을 허용하나요?
- 네트워크 액세스 접근 방식이 시간이 지남에 따라 코드베이스의 유지 관리 및 진화에 미칠 것으로 예상되는 영향은 무엇입니까?
- 접근 방식이 기존 및 계획된 인프라와 잘 통합됩니까? 중요한 변경 또는 추가가 필요합니까?

확장성, 용량 및 성능

SaaS 제품에 대한 네트워크 액세스 접근 방식의 적합성을 확인하려면 수요 증가에 따라 최적의 성능을 유지하는 방법을 분석하는 것이 중요합니다.

높은 점수 기준

네트워크 액세스 접근 방식은 원활한 확장을 지원합니다. 요청 처리 중에 짧은 지연 시간을 유지하고 트래픽 급증을 효율적으로 처리합니다. 트래픽 수준 증가에 관계없이 일관된 성능을 제공하며 증가에 운영 제한을 두지 않습니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 내재된 대역폭 제한 또는 인프라 용량 부족으로 인해 효과적으로 확장되지 않습니다. 리소스 프로비저닝 및 관리는 복잡성을 높이거나 종속성을 생성합니다. 특히 혼잡한 네트워크 조건에서 지연 시간, 지터 및 처리량 변동성이 증가하여 서비스 성능이 저하됩니다.

자체 평가 질문

- 네트워크 액세스 접근 방식은 점점 더 많은 테넌트와 데이터 볼륨을 어떻게 수용하나요?
- 향후 수요에 맞게 본질적으로 확장 가능합니까?
- 트래픽이 가장 많거나 빠른 규모 조정 이벤트 중에도 성능이 일관되게 유지되도록 하기 위해 어떤 조치가 마련되어 있습니까?
- 이 접근 방식은 네트워크 지연 시간과 지터를 어떻게 처리하나요? 데이터 처리량을 최적화하고 지연을 최소화하는 메커니즘이 있나요?
- 네트워크 액세스 접근 방식이 다양한 네트워크 조건에 맞게 조정될 수 있나요? 모든 고객에게 단일 테넌트 경험을 제공할 수 있습니까?
- 네트워크 액세스 접근 방식이 기본 인프라에 미치는 영향은 무엇입니까? 기존 시스템을 크게 업그레이드하거나 변경해야 합니까?

SaaS 제품의 네트워크 액세스와 관련된 운영 우수성 지표

이 섹션에는 다음 지표가 포함되어 있습니다.

- 운영 복원력 및 재해 복구
- 서비스 및 애플리케이션 성능 모니터링

운영 복원력 및 재해 복구

네트워크 액세스 접근 방식은 SaaS 제품이 다양한 유형의 중단을 견디고 재해로부터 신속하게 복구하는 데 도움이 되어야 합니다.

높은 점수 기준

수립되고 테스트된 재해 복구 계획은 네트워크 액세스 접근 방식이 재해 복구 요구 사항을 충족함을 일관되게 보여줍니다. 네트워크 액세스 접근 방식은 고가용성 구성을 지원하며, 빠르고 안정적인 자동 장애 조치 메커니즘을 지원합니다.

점수가 낮은 지표

네트워크 액세스 접근 방식을 사용하면 일관된 재해 복구 전략을 수립하기가 어렵습니다. 중단 후 복구 시간이 길어지는 것을 확인할 수 있습니다. 네트워크 인프라의 빈번한 운영 실패는 서비스 제공에 영향을 미치고 있습니다.

자체 평가 질문

- 마지막 재해 복구 훈련은 언제였으며 결과는 어떠했습니까?
- 중단 후 중요한 서비스를 복구하는 데 얼마나 걸리나요? 네트워크 인프라의 어떤 부분을 재배포해야 합니까?
- 재해 복구 계획을 간소화하기 위해 네트워크 인프라를 개선할 수 있는 사항은 무엇입니까?
- 가장 중요한 네트워크 구성 요소에 대한 중복이 있습니까?
- 심각한 중단 후 네트워크 인프라의 잠재적 재배포를 자동화했습니까?
- 네트워크 액세스 접근 방식은 내결함성과 신뢰성을 어떻게 지원하나요? 네트워크 중단을 처리하고 데이터 무결성을 유지하기 위한 기본 제공 메커니즘이 있나요?

서비스 및 애플리케이션 성능 모니터링

네트워킹 액세스 접근 방식은 최적의 운영 및 서비스 가동 시간을 검증하는 데 사용되는 성능 모니터링 도구에 영향을 미칠 수 있습니다. 서비스에 따라 하위 수준 지표(예: 패킷 삭제율) 또는 상위 수준 지표(예: 세션 기간)에 액세스할 수 있습니다. 하위 수준 지표는 네트워크 동작에 대한 상세한 기술적 통찰력을 제공하지만 해석하기가 복잡할 수 있습니다. 반면 상위 수준 지표는 전반적인 사용자 경험을 측정하는 보다 직접적이고 쉬운 방법을 제공하는 경우가 많습니다. 이는 기본 네트워크 상태의 영향을 서비스 품질의 명확한 지표로 집계하기 때문입니다.

높은 점수 기준

실시간에 가까운 인사이트를 제공하는 포괄적인 모니터링 도구를 즉시 사용할 수 있습니다. 성능 문제를 해결하는 자동 알림 및 응답 시스템이 있습니다. 잠재적인 서비스 병목 현상 또는 장애가 사용자에게 영향을 미치기 전에 예측할 수 있습니다.

점수가 낮은 지표

빈번한 서비스 중단 또는 성능 문제는 관찰하거나 조치를 취하지 않고 발생합니다. 서비스 성능에 대한 가시성이 부족하면 성능 병목 현상에 대한 응답이 느려집니다. 네트워크 인프라 문제를 해결하려면 다자간 팀이 필요합니다.

자체 평가 질문

- 현재 사용할 수 있는 모니터링 도구 및 네트워크 인프라 지표는 무엇입니까? 서비스 이상을 탐지하는 데 얼마나 효과적입니까?
- 성능 문제를 얼마나 빨리 식별하고 해결할 수 있습니까?
- 잠재적 성능 문제를 예측하는 메커니즘이 있습니까?
- 관찰성 기능을 개선하기 위해 개선할 수 있는 사항은 무엇입니까?

SaaS 제품의 네트워크 액세스와 관련된 보안 및 거버넌스 지표

이 섹션에는 다음 지표가 포함되어 있습니다.

- 보안, 규정 준수 및 취약성 관리

보안, 규정 준수 및 취약성 관리

보안 표준 준수 및 취약성 관리를 포함하여 네트워크 액세스 접근 방식의 보안 측면을 평가하는 것이 중요합니다.

높은 점수 기준

네트워크 액세스 접근 방식은 팀이 ISO(International Organization for Standardization) 27001, SOC 2(System and Organization Controls 2) 또는 NIST와 같은 보안 프레임워크를 준수하는 데 도움이 됩니다. 이를 통해 정기적인 보안 감사를 쉽게 수행할 수 있습니다. 강력한 암호화 및 인증 메커니즘이 마련되어 있습니다. 네트워크는 격리되며 필요한 리소스만 고객의 인프라에 노출됩니다. 과도한 오버헤드 없이 거의 실시간으로 네트워킹 이상을 발견할 수 있습니다.

점수가 낮은 지표

네트워크 액세스 접근 방식은 반복적인 보안 침해 또는 취약성에 취약하며 주요 보안 표준을 준수하지 않습니다. 보안 인시던트에 대한 탐지 및 대응이 지연되는 경우가 많습니다.

자체 평가 질문

- 선택한 네트워크 액세스 접근 방식과 관련된 최근 보안 침해가 있나요? 그로부터 무엇을 배웠나요?
- 네트워크 액세스 접근 방식은 글로벌 보안 표준을 어떻게 준수하나요?
- 보안 위협을 탐지하고 대응하는 데 얼마나 걸리나요? 네트워크 액세스가이 기능을 어떻게 지원하거나 제한하나요?

- 네트워크 액세스 접근 방식에 대한 보안 평가는 얼마나 자주 수행되나요? 일반적인 도구를 사용하여 네트워크 액세스 접근 방식의 보안을 평가할 수 있습니까? 아니면 특수 소프트웨어가 필요합니까?
- 네트워크 액세스 접근 방식에는 어떤 수준의 보안이 내재되어 있으며, 업계 모범 사례 및 규제 요구 사항에 어떻게 부합하나요?

SaaS 제품의 AWS 네트워킹 서비스 개요

이 섹션에서는이 가이드에서 참조하는 AWS 네트워킹 서비스에 대해 설명합니다. 또한 기능을 비교하고 각 서비스에 대한 보안 고려 사항을 설명합니다.

이 섹션은 다음 주제를 포함합니다:

- AWS 네트워킹 서비스
- 서비스 기능 비교
- 보안 기능 및 고려 사항

AWS 네트워킹 서비스

다음은이 가이드에서 일관되게 설명하는 AWS 서비스 입니다.

AWS PrivateLink

AWS PrivateLink 는 고객이 이미에서 운영 중인 경우 SaaS 제품에 대한 액세스를 제공할 수 있는 클라우드 네이티브 서비스입니다 AWS 클라우드. 고객은 인터페이스 VPC 엔드포인트를 통해 SaaS 제품에 연결합니다. 이는 고객의에 있는 하나 이상의 서브넷에 프로비저닝되는 엔드포인트 네트워크 인터페이스입니다 AWS 계정. 이 가이드의 시나리오에서 트래픽은 인터페이스 VPC 엔드포인트를 통해 이동하고 계정의 Network Load Balancer에 도착합니다. Network Load Balancer는 엔드포인트 서비스로 등록한 SaaS 애플리케이션에 트래픽을 전달합니다. 리소스 VPC 엔드포인트를 통해는 데이터베이스와 같은 다른 리소스에 액세스하는 데도 도움이 될 AWS PrivateLink 수 있습니다.

Amazon VPC Lattice

Amazon VPC Lattice는 SaaS 공급자가 여러 VPCs 및에서 운영하는 고객에게 안전하고 효율적으로 서비스를 제공할 수 있도록 지원하는 애플리케이션 네트워킹 서비스입니다 AWS 계정. 고객은 일관된 네트워크 연결, 강력한 액세스 제어 및 고급 트래픽 관리를 제공하는 VPC Lattice를 통해 SaaS 제품에 액세스합니다. 이러한 시나리오에서 트래픽은 VPC Lattice를 통해 등록된 애플리케이션 서비스로 흐릅니다. 사용하는 컴퓨팅 서비스에 관계없이 확장 가능하고 안전한 통신을 제공합니다.

VPC 피어링

VPC 피어링은 프라이빗 IPv4 주소 또는 IPv6 주소를 사용하여 두 Virtual Private Cloud(VPCs) 간의 트래픽을 라우팅하는 두 VPC 간의 네트워킹 연결입니다. VPC 피어링은 일반적으로 동일한 조직 내의 엔

터티와 같은 신뢰할 수 있는 엔터티 간에 사용됩니다. 고객이 VPCs 중 하나에 피어링 요청을 생성합니다. 수락하면 트래픽VPCs 간에 어느 방향으로든 흐를 수 있습니다. 이 연결 접근 방식은 관리할 중간 서비스 또는 인프라 없이 두 VPCs 간에 직접 통신해야 하므로 고유성이 두드러집니다.

AWS Transit Gateway

AWS Transit Gateway는 VPCs, 가상 프라이빗 네트워크(VPN) 연결, AWS Direct Connect 게이트웨이, VPC의 타사 가상 어플라이언스 및 기타 전송 게이트웨이를 연결할 수 있는 중앙 집중식 네트워크 전송 허브입니다. 전송 게이트웨이는 각 연결에 대해 서로 다른 라우팅 테이블을 가질 수 있습니다. 이를 통해 라우팅의 유연성을 극대화하고 네트워크를 격리할 수 있습니다. 많은 VPCs 함께 연결하거나 중앙 집중식 검사를 수행하는 데 자주 사용됩니다.

AWS Site-to-Site VPN

AWS Site-to-Site VPN는 인터넷 프로토콜 보안(IPsec) 기술을 사용하여 온프레미스 네트워크, 원격 사무실, 공장, 기타 클라우드 공급자 및 AWS 글로벌 네트워크 간에 연결을 설정할 수 있습니다. 연결은 의 VPC에 있는 가상 프라이빗 게이트웨이 또는 전송 게이트웨이에서 , AWS 클라우드온프레미스 또는 다른 CSP의 클라우드에 있을 수 있는 AWS 클라우드 물리적 또는 소프트웨어 기반 고객 게이트웨이로 설정됩니다. 인터넷 또는 물리적 연결을 통해 AWS Direct Connect 연결할 수 있습니다. 를 사용하여 Site-to-Site VPN 연결을 가속화할 수도 있습니다 AWS Global Accelerator. 가속화된 연결은 트래픽을 AWS 엣지 로케이션으로 라우팅하며 지연 시간을 줄이고 성능을 개선합니다.

AWS Direct Connect

AWS Direct Connect는 온프레미스 데이터 센터와 간에 고속 프라이빗 연결을 설정합니다 AWS 클라우드. 퍼블릭 인터넷을 우회하여는에 대한 보다 안정적이고 안전하며 일관된 저지연 연결을 Direct Connect 제공합니다 AWS 클라우드. 고객은 Direct Connect 위치 중 하나에 연결한 다음 호스팅된 연결 또는 전용 연결을 선택합니다 AWS. 이는 SaaS 제품에 대한 흔하지 않은 아키텍처 선택이지만 엔터프라이즈 소비자가 거의 없지만 대기업인 SaaS 공급자에게 매우 적합할 수 있습니다.

서비스 기능 비교

다음 표에는이 가이드에서 AWS 서비스 설명하는의 지원되는 기능이 요약되어 있습니다. 다음은이 표에 포함된 기능에 대한 설명입니다.

- 겹치는 CIDR 범위 - CIDR 범위가 동일하거나 겹치는 두 개 이상의 네트워크를 연결할 수 있습니다.
- 양방향 통신 - SaaS 소비자가 데이터베이스와 같은 내부 리소스를 SaaS 공급자에게 노출할 수 있도록 양방향 통신 채널을 지원할 수 있습니다.

- IPv6 - 단일 또는 이중 스택으로 IPv6 지원 가능
- 점보 프레임 - 프레임 크기가 최대 8,500 바이트인 점보 프레임을 지원할 수 있습니다.
- 하이브리드 클라우드 - 온프레미스 네트워크와의 연결을 지원할 수 있습니다.
- 다중 클라우드 - 서로 다른 클라우드 서비스 공급자의 네트워크 간 연결을 지원할 수 있습니다.

서비스 또는 접근 방식	CIDR 범위 중복	양방향 통신	IPv6	점보 프레임	하이브리드 클라우드	멀티 클라우드
VPC 피어링	아니요	예	예	예[5]	아니요	아니요
AWS PrivateLink	예	예[1]	예	예	아니요[6]	아니요[6]
Amazon VPC Lattice	예	예[1]	예	예	아니요[6]	아니요[6]
AWS Transit Gateway	아니요	예	예	예	예[3]	예[3]
AWS Site-to-Site VPN	아니요	예	예	아니요	예	예
AWS Direct Connect	아니요	예	예	예[2]	예	예
퍼블릭 인터넷 액세스[4]	해당 사항 없음	아니요	예	예	예	예

1. Amazon VPC Lattice의 VPC 리소스 사용

2. 프라이빗 및 전송 가상 인터페이스에만 해당
3. Site-to-Site VPN 또는 AWS Direct Connect 연결 사용
4. Application Load Balancer와 같이 애플리케이션에 공개적으로 액세스할 수 있도록 하는 AWS 리소스의 일반적인 용어입니다.
5. 하나의 내에서 연결을 피어링하는 경우에만 AWS 리전
6. 환경 간 기존 계층 3 연결을 통해 가능

보안 기능 및 고려 사항

다음 표에는이 가이드에서 AWS 서비스 설명하는의 보안 기능이 요약되어 있습니다.

- 인증 수단 - 고객만 서비스에 연결할 수 있도록 하는 방법입니다. 수신 요청에 대한 또 다른 인증 수준은 일반적으로 특히 공유 테넌트 환경에서 여전히 필요합니다.
- 전송 중 암호화 - 전송 중 암호화가 기본적으로 제공되는지 여부를 설명합니다. 네이티브 암호화는 VPCs 간 또는 데이터 센터 간 모든 트래픽에 대해가 AWS 제공하는 암호화VPCs 설명합니다. 보조 암호화는 사용자가 제어하고 각 서비스에서 중지할 수 있는 암호화를 설명합니다.

서비스 또는 접근 방식	인증 수단	전송 중 데이터 암호화
VPC 피어링	고객의 AWS 계정 및 VPC에 대한 피어링 요청을 시작하거나 고객이 시작한 요청을 수락합니다. VPC 피어링 연결 수락 또는 거부를 참조하세요.	네이티브 암호화만
AWS PrivateLink	서비스에 엔드포인트를 생성할 AWS 계정 수 있는를 선택합니다. 이러한 계정을 허용된 보안 주체라고 합니다. 연결 요청 수락 또는 거부를 참조하세요.	네이티브 암호화만
Amazon VPC Lattice	VPC Lattice 서비스 또는 서비스 네트워크를 고객의와 공유합니다 AWS 계정. VPC Lattice 엔터티 공유를 참조하세요.	기본 암호화 및 보조 TLS 암호화

AWS Transit Gateway	고객이에서 피어링 연결 요청을 생성 AWS 계정하거나 사용자가 요청을 시작합니다. Amazon VPC Transit Gateways의 Transit Gateway 피어링 연결을 참조하세요.	VPN 연결을 사용한 기본 암호화 및 보조 IPsec 암호화
AWS Site-to-Site VPN	고객의 디바이스에서 IPsec 사전 공유 키 또는 프라이빗 인증서를 사용합니다. AWS Site-to-Site VPN 터널 인증 옵션을 참조하세요.	보조 IPsec 암호화
AWS Direct Connect	고객이에서 가상 인터페이스 요청을 생성합니다 AWS 계정. Direct Connect 가상 인터페이스 및 호스팅 가상 인터페이스를 참조하세요.	일부 사이트에서는 추가 계층 2 암호화가 가능합니다. Direct Connect 위치를 참조하세요.
퍼블릭 인터넷 액세스[1]	사용자 지정 인증이 필요합니다.	추가 TLS 암호화 가능

1. Application Load Balancer와 같이 애플리케이션에 공개적으로 액세스할 수 있도록 하는 AWS 리소스의 일반적인 용어입니다.

SaaS 제품에 대한 네트워크 액세스 옵션 평가

조직에 중요한 지표는 고객이 누구인지, 비즈니스 전략 및 조직 목표에 따라 달라집니다. 이 가이드에서는 네트워킹 액세스 접근 방식을 선택하는 데 사용할 수 있는 지표를 제시하지만 사용 사례의 고유한 요구 사항을 충족하는 지표의 우선순위를 지정해야 합니다.

이 섹션은 다음 주제를 포함합니다:

- 평가 지표
- 총 소유 비용
- 네트워킹 값 맵

평가 지표

일부 지표는 조직 및 사용 사례 전반에서 일관되며, 이는 평가에 도움이 될 수 있는 지표입니다. 다음은 이러한 지표입니다.

- 통합 용이성 - 신규 고객을 얼마나 빠르고 쉽게 온보딩할 수 있습니까?
- 총 소유 비용(TCO) - 비용 구조는 무엇입니까? 고정 및 가변 인프라 비용 외에도 운영 오버헤드, 전문가에 대한 종속성, 변경 구현 비용 및 규정 준수와 관련된 주요 추가 비용 고려 사항이 있습니다. 자세한 내용은 총 소유 비용(을)를 참조하세요.
- 확장성 - 네트워크 액세스 접근 방식을 확장하여 회사의 성장을 지원할 수 있습니까? 고객 기반 규모 조정에는 중요한 아키텍처 및 조직 고려 사항이 있습니다. 현재 지원하는 것보다 5~100배 많은 고객을 수용하도록 규모를 조정할 수 있는 방법을 고려합니다.
- 적응성 - 변경 사항을 쉽게 구현할 수 있습니까? 변경 사항에는 새 애플리케이션, 새 기능, 다른 플랫폼 또는 다른 네트워크가 포함될 수 있습니다.
- 네트워크 격리 - 고객에게 얼마나 많은 네트워크 인프라를 노출하고 있습니까? 적절한 수준의 액세스를 제공하고 있습니까? 아니면 전체 네트워크를 노출하고 있습니까? 네트워크 리소스를 조기에 격리하면 나중에 보안, 개인 정보 보호 및 규정 준수 보장을 더 쉽게 제공할 수 있습니다.
- 관찰성 - 서비스 장애 또는 성능 저하를 감지하는 기능은 무엇입니까? 문제를 식별하는 것이 얼마나 쉽고 빠르나요? 고객이 장애 지점을 이해하고 해결하는 데 얼마나 빨리(그리고 어떤 오버헤드로) 도움이 될 수 있습니까?
- 복구 시간 - 서비스 장애 또는 성능 저하 감지와 작업 재개 사이의 리드 타임은 얼마입니까? 이 기능에 영향을 미치는 요인은 무엇입니까?

다른 지표는 비즈니스 운영, 전략 또는 목표와 관련이 있으므로 조직 또는 상품에 고유합니다. 사용자만 이러한 지표를 평가할 수 있습니다. 다음은 이러한 지표입니다.

- 비즈니스 모델 조정 - 비즈니스 모델은 무엇이며 개별 액세스 접근 방식이 이에 얼마나 잘 부합하나요?
- 총 주소 지정 가능 시장(TAM) - 현재 및 미래 시장은 무엇이며 네트워크 액세스 접근 방식이 얼마나 잘 적용됩니까?
- 투자 수익률(ROI) - 수익성과 마진에서 예상되는 개선 사항은 무엇입니까? 예상되는 재정적 이점이 적응 가능하고 유연한 서비스 액세스에 대한 요구 사항을 충족하기에 충분합니까?
- 규정 준수 - 어떤 종류의 규제 요구 사항이 적용되고 어떤 시장에서 적용됩니까?
- 서비스 수준 계약(SLAs) - 고객이 SaaS 제품을 고가용성으로 사용해야 합니까? 계약상 어떤 종류의 약정을 준수해야 하나요?

총 소유 비용

이 섹션에서는 네트워크 액세스 접근 방식을 비교하는 데 사용되는 평가 지표 중 하나인 총 소유 비용(TCO)을 살펴봅니다. TCO는 고정 및 가변 인프라 비용, 운영 오버헤드, 전문가 종속성, 변경 비용 및 규정 준수 비용으로 구성된 복합 지표입니다.

각 네트워크 액세스 접근 방식의 TCO 등급은 사용 사례에 따라 다를 수 있습니다. 예를 들어 간단한 웹 서비스와 5개의 테넌트가 있는 SaaS 공급자의 변경 비용은 복잡하고 상호 연결된 제품 포트폴리오와 수백 또는 수천 개의 테넌트가 있는 SaaS 공급자와 다릅니다. 또한 모든 구성 요소의 가중치가 동일한 것은 아닙니다. 예를 들어 네트워킹 전문가를 고용하는 것은 개별 서비스 배포를 지원하는 인프라 비용보다 비용이 많이 드는 경우가 많습니다. 다음 표의 값을 초기 방향에 사용하고 추가 논의를 위한 참조점으로 사용합니다.

액세스 접근 방식	고정 인프라 비용	가변 인프라 비용	운영 오버헤드	전문가 종속성	변경 비용	규정 준수 비용
VPC 피어링	없음	없음	높음	낮음	높음	중간
AWS PrivateLink	낮음	낮음	낮음	없음	낮음	낮음

Amazon VPC Lattice	중간	중간	낮음	낮음	낮음	낮음
AWS Transit Gateway	중간	중간	낮음	낮음	낮음	중간
AWS Site-to-Site VPN	중간	높음	높음	중간	중간	낮음
AWS Direct Connect	높음	중간	중간	높음	높음	낮음
퍼블릭 인터넷 액세스	낮음	높음	중간	낮음	낮음	높음

VPC 피어링 비용

VPC 피어링 연결과 관련된 직접적인 인프라 비용은 없습니다. 트래픽이 동일한 가용 영역 내에 있으면 데이터 전송 요금이 부과되지 않습니다. 그러나 각 추가 피어링 연결에 따라 관리 및 복잡성이 기하급수적으로 증가하므로 운영 오버헤드가 클 수 있습니다. 네트워킹에 대한 몇 가지 기본적인 이해만으로는 피어링 연결을 설정하는 데 충분하지만, 네트워크의 변경은 소수 이상의 피어링 연결로 구현하기 어렵습니다. 양 당사자가 개별 서비스가 아닌 전체 VPC를 서로 노출하기 때문에 규정 준수 비용이 약간 더 높습니다.

AWS PrivateLink 비용

AWS PrivateLink 는 종종 운영 오버헤드가 적은 비용 효율적인 솔루션입니다. 이는 SaaS 공급자가 Network Load Balancer만 관리해야 하고 소비자가 VPC 엔드포인트만 관리해야 하기 때문입니다. 양쪽을 투명하게 변경할 수 있으므로 비용이 많이 들고 리소스 집약적인 조직 간 협업이 줄어듭니다. SaaS 공급자가 전체 네트워크가 아닌 원하는 서비스만 노출하기 때문에 규정 준수 비용은 낮은 경향이 있습니다.

Amazon VPC Lattice 비용

Amazon VPC Lattice는 중간 수준의 고정 및 가변 인프라 비용으로 균형 잡힌 비용 구조를 제공합니다. 완전 관리형 서비스 네트워크로서 여러 VPCs에서 서비스 검색, 트래픽 관리 및 액세스 제어를 자동화하여 운영 오버헤드를 크게 줄입니다. 이렇게 하면 수동 네트워킹 구성에 비해 초기 배포와 지속적인 관리가 모두 간소화됩니다. 복잡한 라우팅 업데이트 없이 정책 기반 제어를 통해 변경 사항을 구현할 수 있으므로 네트워킹 전문가에 대한 종속성이 줄어듭니다. VPC Lattice는 내장된 모니터링 및 로깅 기능을 통해 세분화된 액세스 제어와 포괄적인 가시성을 제공하므로 규정 준수 비용은 기존 네트워킹 접근 방식보다 낮은 경향이 있습니다. 이렇게 하면 규정 준수를 더 쉽게 입증할 수 있습니다.

AWS Transit Gateway 비용

AWS Transit Gateway 는 시간당 및 데이터 처리 요금이 보다 크 AWS PrivateLink지만 운영 오버헤드는 비슷합니다. 모든 라우팅 테이블을 올바르게 설정하려면의 AWS Transit Gateway 서비스 및 라우팅에 AWS 대한 심층적인 지식이 있어야 합니다. 인프라를 변경하려면 라우팅 또는 DNS 업데이트가 필요할 수 있습니다. 두 당사자가 하위 네트워크 또는 전체 VPC를 서로 노출할 가능성이 있기 때문에 규정 준수 비용은 VPCs 피어링과 유사합니다. AWS Transit Gateway 라우팅 테이블은 여러 소비자가 공유하므로 주의해서 처리해야 하며 둘 사이의 트래픽을 허용해서는 안 됩니다.

AWS Site-to-Site VPN 비용

Site-to-Site VPN은 기본적으로 트래픽을 인터넷으로 전송하기 때문에 데이터 전송 요금 때문에 가변 비용이 가장 높습니다. 관리형 가상 프라이빗 네트워크(VPN) 서비스이지만 특히 고객 게이트웨이에서 상당한 운영 오버헤드가 발생합니다. 프로비저닝 및 운영에는 네트워킹에 대한 고급 지식이 필요하며, 변경 사항에는 종종 양 당사자의 조치가 필요합니다. 보안 팀이 추가 검토 없이 IPsec 터널을 사전 승인하는 경우가 많기 때문에 규정 준수 비용은 일반적으로 낮습니다.

AWS Direct Connect 비용

AWS Direct Connect 는에 직접 연결되는 프라이빗 물리적 연결이므로 고정 인프라 비용이 가장 큽니다 AWS 클라우드. Border Gateway Protocol(BGP) 세션(필요한 경우)을 설정 및 운영하고, VPN 연결을 운영하고, 트래픽 엔지니어링을 수행하려면 전문 지식이 필요합니다. 이 서비스는 프라이빗 연결을 미디어 액세스 제어 보안(MACsec) 및 IPsec 암호화를 추가로 사용하는 옵션과 혼합하므로 보안 팀의 노력을 줄입니다.

퍼블릭 인터넷 액세스 비용

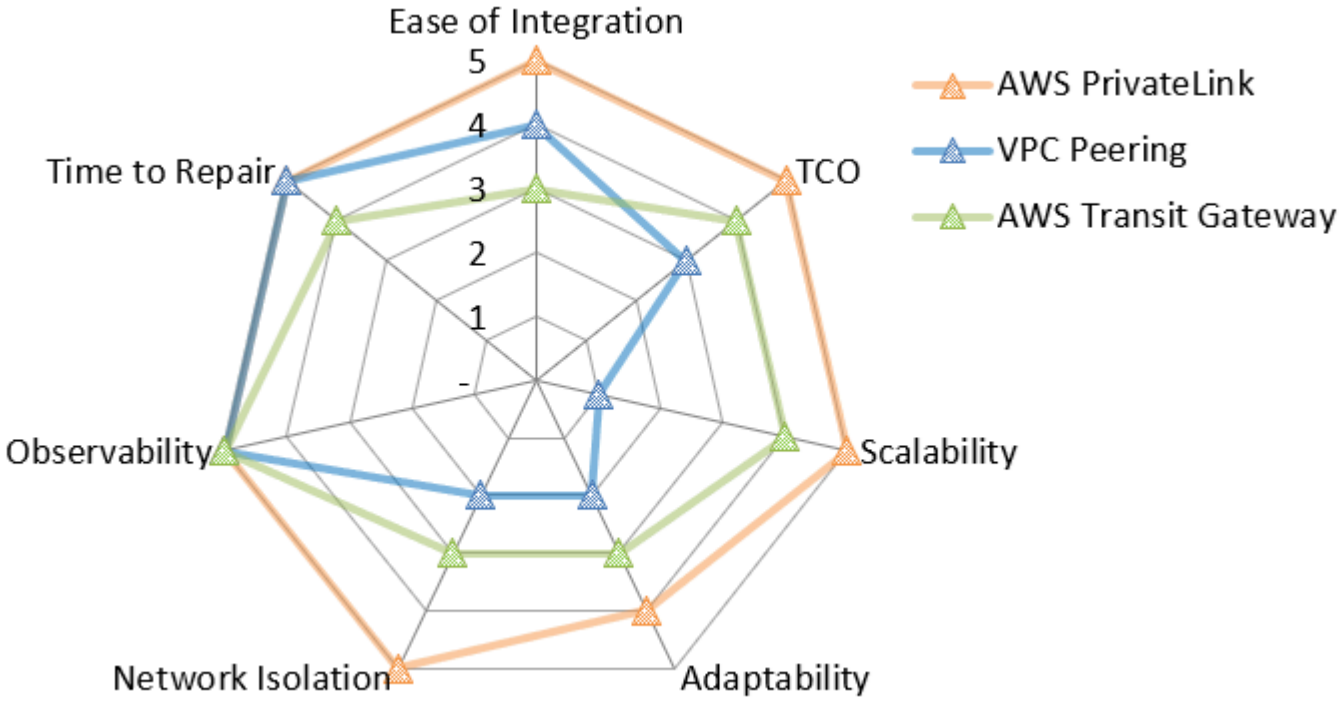
퍼블릭 인터넷 액세스는 Application Load Balancer와 같이 애플리케이션에 공개적으로 액세스할 수 있도록 하는 데 사용할 수 있는 AWS 리소스를 말합니다. 이 접근 방식의 경우 인터넷으로의 데이터 전

송 요금을 포함하여 서비스에 대한 액세스 제공과 관련된 가변 비용이 있습니다. 인터넷에 서비스를 노출하고 추가 보안 및 인증 메커니즘이 필요하기 때문에 운영 오버헤드 및 규정 준수 비용이 상당할 수 있습니다. 그러나 복잡한 라우팅은 없으며 어느 당사자도 서로의 인프라에 대한 세부 정보를 알 필요가 없습니다.

네트워킹 값 맵

이 가이드에는 큰 그림을 보고 정보에 입각한 결정을 내리는 데 도움이 되도록 각 시나리오에 대한 네트워킹 가치 맵이 포함되어 있습니다. 등급은 시나리오마다 다르므로 두 시나리오에서 동일한 서비스가 다르게 평가될 수 있습니다. 값 맵은 모든 범주에서 가상의 완벽한 점수가 5인 방사형 차트입니다.

예를 들어 다음 이미지는 샘플 레이더 차트를 보여줍니다. 여기에는 평가에 도움이 될 수 있는 지표만 포함됩니다. 본인만 평가할 수 있는 추가 지표가 포함된 자체 값 맵을 생성하는 것이 좋습니다.



의 SaaS 제품에 대한 네트워킹 액세스 시나리오 AWS 클라우드

이 섹션에서는의 SaaS 제품에 대한 다양한 네트워크 액세스 옵션을 다룹니다 AWS 클라우드. 내에서 연결 요구 사항이 있을 수 있는 소비자, AWS 클라우드온프레미스 데이터 센터 또는 기타 클라우드 서비스 제공업체(CSPs)의 관점에서 접근 방식에 대해 설명합니다. 또한 여러 유형의 소비자 환경에서의 액세스를 지원해야 할 수도 있습니다.

포괄적인 액세스 전략을 수립하려면 이러한 다양한 환경의 네트워크 연결 요구 사항을 이해하는 것이 중요합니다. 아키텍처 결정은 운영 효율성을 유지하면서 다양한 보안 모델, 성능 기대치 및 기술적 제약을 고려해야 합니다. 올바른 접근 방식은 비즈니스 성장에 따라 확장되고 구현 복잡성과 지속적인 관리 오버헤드를 최소화하는 안전하고 안정적인 연결을 제공합니다.

네트워크 액세스 옵션을 평가할 때 인프라 비용뿐만 아니라 운영 오버헤드 및 규정 준수 요구 사항을 포함하여 각 접근 방식이 총 소유 비용에 미치는 영향을 고려합니다. 일부 접근 방식은 확장성이 뛰어나지만 복잡성이 발생할 수 있는 반면, 네트워크 격리를 희생하면서 통합 용이성을 우선시하는 접근 방식도 있습니다. 소비자의 기술적 역량과 리소스도 가장 적합한 솔루션을 결정하는 데 중요한 역할을 합니다.

의 소비자에게와 같은 AWS 클라우드서비스는 보안 및 확장성에서 상당한 이점을 AWS PrivateLink 제공합니다. 온프레미스 소비자는 일관된 성능을 AWS Direct Connect 위해를 활용하거나 비용 효율적인 연결을 위해 Site-to-Site VPN을 활용할 수 있습니다. 다중 클라우드 시나리오에서는 상호 운용성 문제를 신중하게 고려해야 하는 경우가 많으며, 전송 VPC 아키텍처를 사용하여 액세스 패턴을 표준화할 수 있습니다. 어떤 경우에도 SaaS 제품이 발전함에 따라 네트워크 아키텍처가 복원력과 적응력을 유지할 수 있도록 설계는 향후 소비자 및 트래픽 증가를 예상해야 합니다.

이 섹션에는 다음과 같은 시나리오가 포함되어 있습니다.

- 에서 작동하는 SaaS 소비자 AWS
- 온프레미스에서 운영하는 서비스 소비자
- 다른 클라우드 서비스 공급자에서 운영하는 SaaS 소비자
- 하이브리드 환경 지원

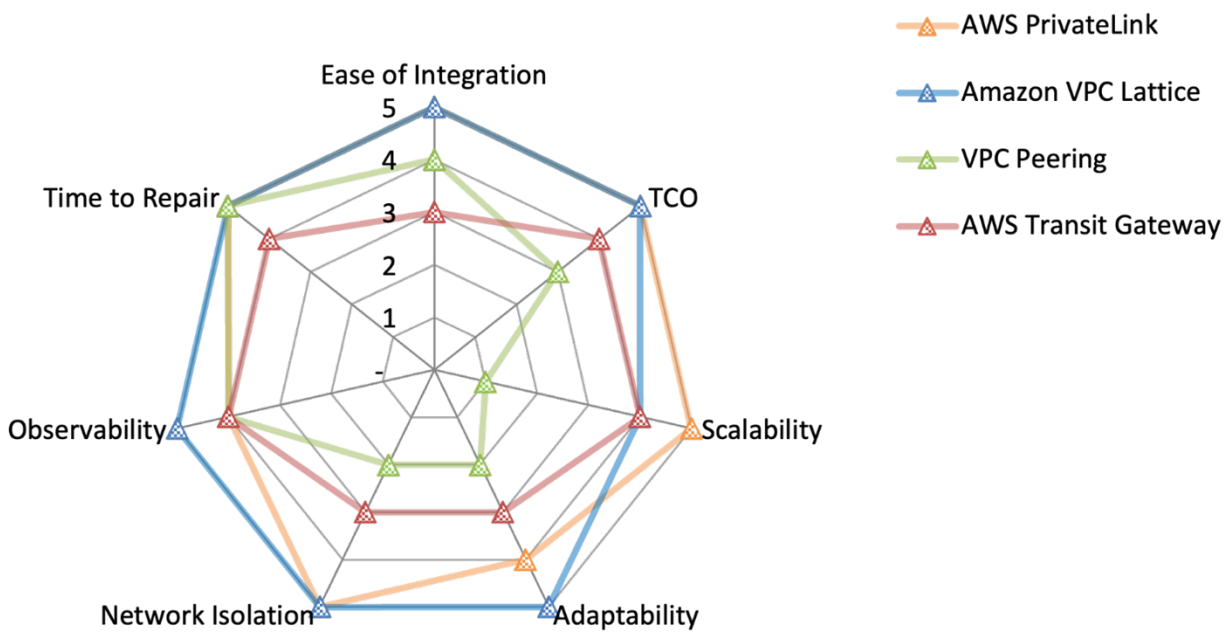
에서 작동하는 SaaS 소비자 AWS

이 섹션에서는 사용자와 소비자가 모두에서 작동하는 경우의 연결 옵션에 대해 설명합니다 AWS 클라우드. 이 시나리오는 많은가 AWS 서비스 기본적으로 통합되고 양 당사자가 전체 AWS 서비스 포트폴리오에 액세스할 수 있기 때문에 가장 큰 유연성을 제공합니다.

이 섹션에서는 다음 네트워크 액세스 접근 방식에 대해 설명합니다.

- 과 AWS PrivateLink통합
- Amazon VPC Lattice 서비스 공유
- VPC 피어링 연결 생성
- VPCs 연결 AWS Transit Gateway

다음 네트워킹 값 맵은 각 평가 지표에 대해 이러한 각 옵션의 점수를 요약합니다. 평가 지표에 대한 자세한 내용은이 가이드의 평가 지표를 참조하세요. 맵에서 5는 최저 TCO, 최상의 네트워크 격리 또는 최저 복구 시간과 같은 최고 점수를 나타냅니다. 이 레이더 차트를 읽는 방법에 대한 자세한 내용은이 가이드네트워킹 값 맵의 섹션을 참조하세요.



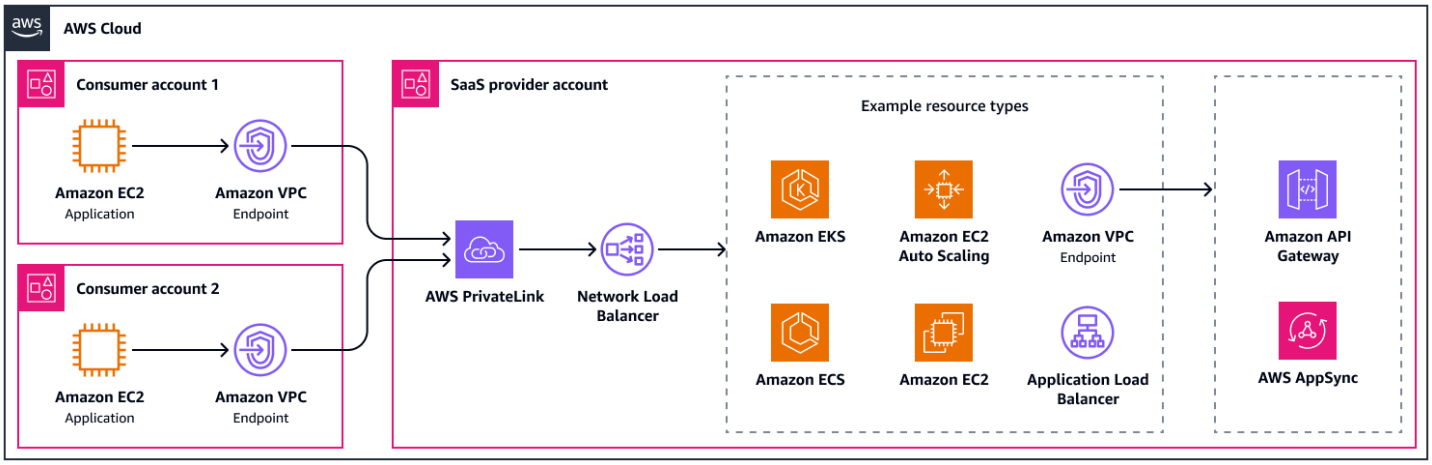
레이더 차트에는 다음 값이 표시됩니다.

평가 지표	AWS PrivateLink	Amazon VPC Lattice	VPC 피어링	AWS Transit Gateway
통합 용이성	5	5	4	3
TCO	5	5	3	4
확장성	5	4	1	4
적응성	4	5	2	3
네트워크 격리	5	5	2	3
Observability	4	5	4	4
복구 시간	5	5	5	4

과 AWS PrivateLink통합

AWS PrivateLink는 SaaS 제품을 통합하는 가장 클라우드 네이티브 방법입니다. SaaS 공급자는 Network Load Balancer 뒤에서 애플리케이션을 호스팅할 수 있습니다. Network Load Balancer는 Application Load Balancer, Amazon Elastic Container Service(Amazon ECS), Amazon Elastic Kubernetes Service(Amazon EKS) 및 Auto Scaling 그룹과 직접 통합됩니다. Network Load Balancer에서 SaaS 공급자 계정의 인터페이스 VPC 엔드포인트로 트래픽을 라우팅할 수도 있습니다. 이를 통해 API를 사용하여 Amazon API Gateway 또는와 같은 애플리케이션에 연결할 수 있습니다AWS AppSync. 애플리케이션에서 데이터베이스와 같이 로드 밸런싱되지 않은 고객 환경의 리소스에 액세스해야 하는 경우 리소스 VPC 엔드포인트를 사용할 수 있습니다.

AWS PrivateLink 는 가용 영역당 최대 100Gbps의 대역폭을 지원합니다. 다음 다이어그램은 몇 가지 가능한 통합이 포함된 기본 구성을 보여줍니다. 이를 통해 두 개의 소비자 계정을 SaaS 공급자 계정에 연결합니다 AWS PrivateLink. 소비자 계정에는 서비스 엔드포인트가 있고 SaaS 공급자 계정에는 Network Load Balancer가 있습니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 통합 용이성: 라우팅 테이블 변경 필요 없음
- 통합 용이성:를 통해 엔드포인트 서비스를 제공할 AWS Marketplace 수 있습니다.
- 통합 용이성: VPC 엔드포인트가 친숙한 DNS 이름 지원
- 확장성: 수천 명의 SaaS 소비자로 확장할 수 있습니다.
- 적응성: 중복 CIDR 범위 지원
- 적응성: IPv6 지원
- 적응성: 교차 리전 지원
- TCO: AWS PrivateLink 는 완전 관리형 서비스이므로 운영 작업이 덜 필요합니다.
- 네트워크 격리: SaaS 공급자로부터 트래픽을 시작할 수 없으므로 SaaS 소비자의 보안 이점
- 네트워크 격리: SaaS 공급자가 전체 서브넷 또는 VPC를 노출하지 않기 때문에 SaaS 공급자의 보안 이점

다음은이 접근 방식의 단점입니다.

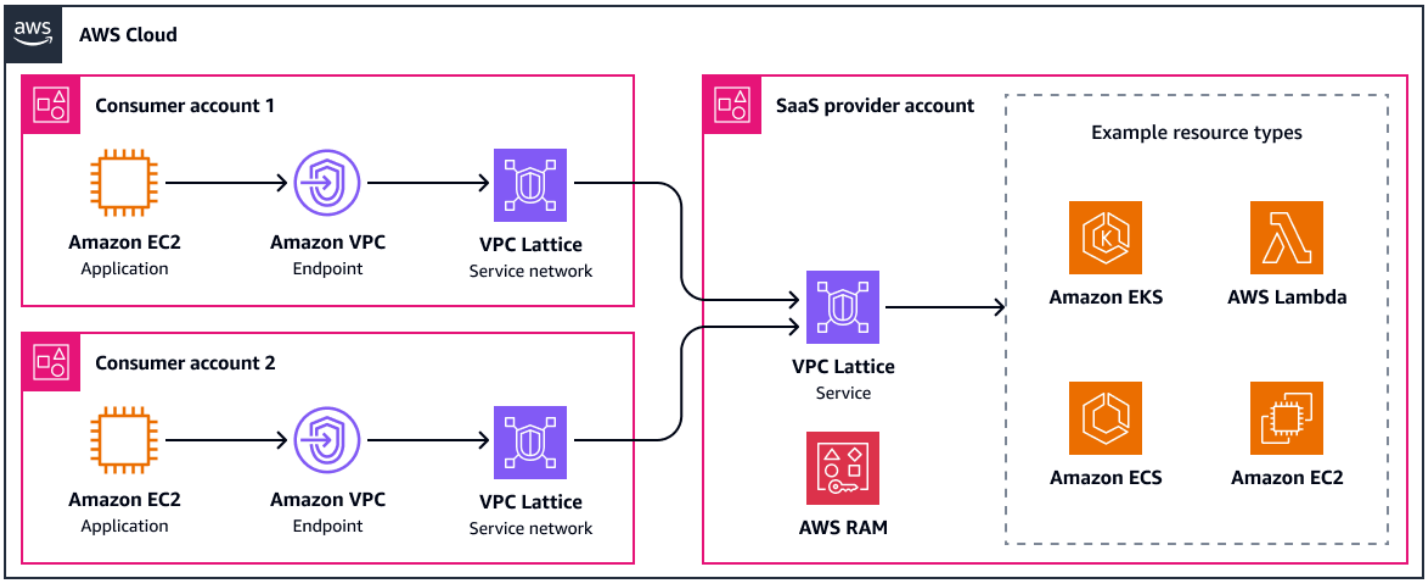
- 적응성: SaaS 공급자는 소비자와 동일한 가용 영역을 사용해야 합니다.
- 적응성: 서비스 시작 통신에는 클라이언트 시작 연결 및 리소스 VPC 엔드포인트에 대한 지원만 필요합니다.
- 적응성: Network Load Balancer는에 대한 유일한 직접 통합입니다. AWS PrivateLink

Amazon VPC Lattice 서비스 공유

Amazon VPC Lattice를 SaaS 애플리케이션의 연결 옵션으로 사용하려면 먼저 SaaS 애플리케이션 구성 요소를 나타내는 VPC Lattice 서비스를 하나 이상 생성합니다. Amazon EC2 인스턴스, 컨테이너 또는 AWS Lambda 함수와 같은 백엔드 대상으로 트래픽을 전달하도록 리스너 및 라우팅 규칙을 구성합니다. 자세한 내용은 VPC Lattice 서비스 네트워크 내에서 Saas 서비스 연결(AWS 블로그 게시물)을 참조하세요. 개념적으로 이는 Application Load Balancer를 구성하는 것과 거의 동일합니다. 그런 다음 (AWS Resource Access ManagerAWS RAM)를 사용하여 SaaS 서비스를 고객 AWS 계정 또는 조직과 안전하게 공유하고 보유한 권한을 지정합니다. 고객은 리소스 공유를 수락한 후 SaaS 서비스를 기존 또는 새로 생성된 VPC Lattice 서비스 네트워크와 연결하여 service-to-service 통신을 활성화할 수 있습니다.

각 VPC Lattice 서비스는 가용 영역당 초당 최대 10Gbps 및 10,000개의 요청을 지원할 수 있습니다. 인증 정책을 구현하면 고객은 SaaS 애플리케이션에 액세스할 수 있는 서비스와 리소스를 세밀하게 제어할 수 있습니다. 리소스 게이트웨이를 사용하여 TCP 연결이 필요한 리소스에 액세스할 수 있습니다. 예를 들어 관리하는 Amazon EKS 클러스터이거나 애플리케이션이 액세스해야 하는 고객 관리형 리소스일 수 있습니다. SaaS 제품에 리소스 게이트웨이를 사용하는 방법에 대한 자세한 내용은 VPC 리소스에 대한 AWS PrivateLink 지원을 AWS 계정 사용하여에 SaaS 기능 확장(AWS 블로그 게시물)을 참조하세요.

다음 다이어그램은 일부 예제 통합이 포함된 상위 수준 VPC Lattice 구성을 보여줍니다. 고객 관리형 서비스 네트워크를 사용하여 SaaS 애플리케이션에 액세스합니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 통합 용이성: 라우팅 테이블 변경 필요 없음
- 통합 용이성: 즉시 서비스 검색
- 확장성: 수천 명의 SaaS 소비자로 확장할 수 있습니다.
- 적응성: 중복 CIDR 범위 지원
- 적응성: IPv6 지원
- 적응성: VPC Lattice 서비스로 모든 AWS 컴퓨팅 서비스와 통합
- TCO: VPC Lattice는 완전 관리형 서비스이므로 운영 작업이 덜 필요합니다.
- TCO: 고급 트래픽 라우팅을 통한 기본 제공 로드 밸런싱
- 네트워크 격리: 인증 정책을 사용한 세분화된 권한 부여
- 네트워크 격리: SaaS 공급자로부터 트래픽을 시작할 수 없으므로 SaaS 소비자의 보안 이점
- 네트워크 격리: 전체 서브넷 또는 VPC를 노출하지 않기 때문에 SaaS 공급자의 보안 이점

다음은이 접근 방식의 단점입니다.

- 적응성: 서비스 시작 통신에는 클라이언트 시작 연결 및 리소스 게이트웨이에 대한 지원만 필요합니다.
- 적응성: 교차 리전 지원 없음

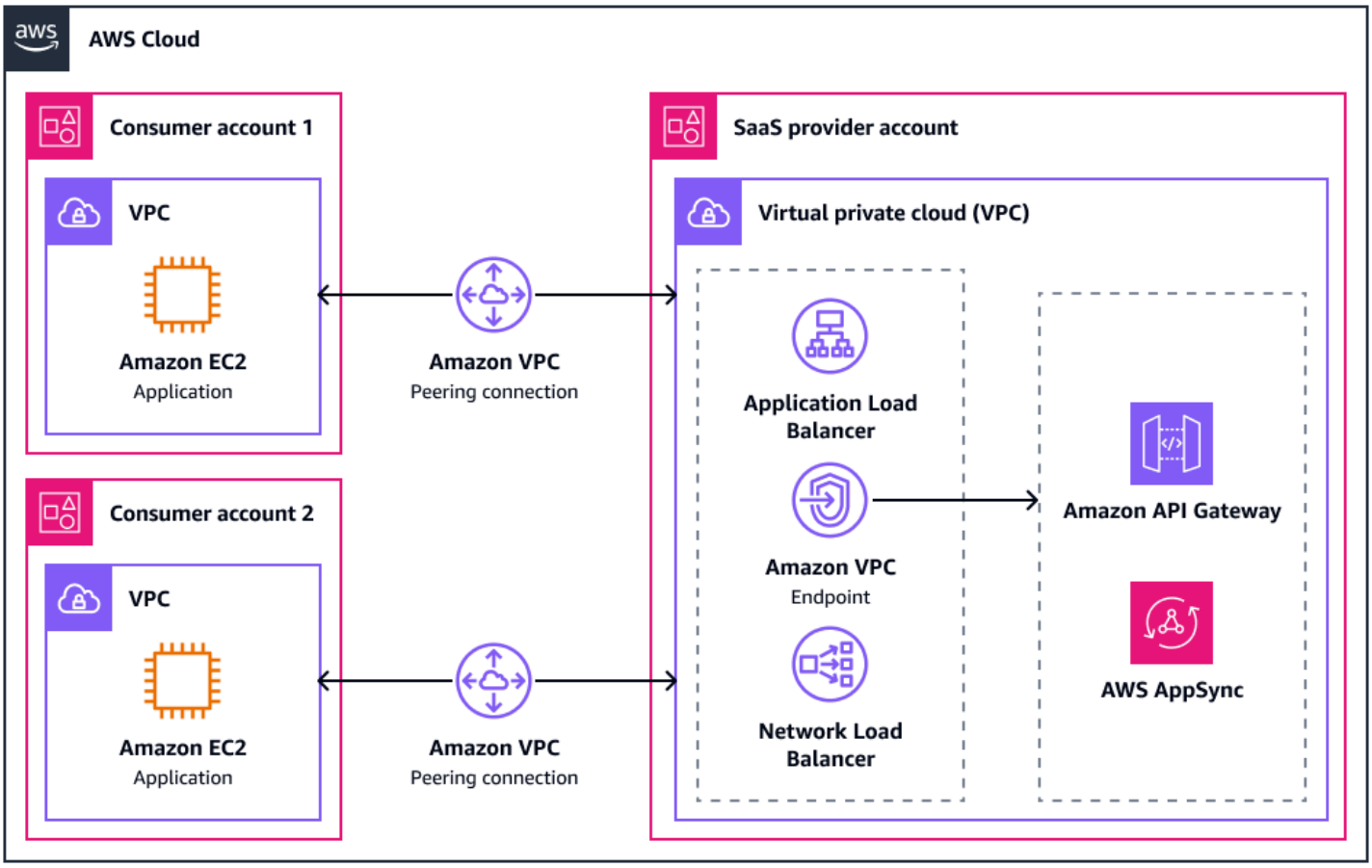
VPC 피어링 연결 생성

VPC 피어링을 사용하여 SaaS 공급자의 VPC를 소비자의 VPC와 연결하면 두 당사자 모두 연결을 시작할 수 있습니다. 이렇게 하려면 두 계정 모두에서 보안 그룹, 방화벽 및 네트워크 액세스 제어 목록(NACLs)을 적절하게 구성해야 합니다. 그렇지 않으면 원치 않는 트래픽이 피어링 연결을 통해 네트워크에 들어갈 수 있습니다. 보안 그룹을 사용하여 피어링된 VPCs. 이렇게 하면 허용 목록 보안 그룹이 허용 목록 IP 주소에 비해 더 명시적이고 세분화된 액세스 제어를 제공하므로 애플리케이션에 대한 액세스를 제어하는 데 도움이 될 수 있습니다.

VPC 피어링을 사용하면 VPC에 배포된 서비스 또는 리소스를 통해 SaaS 제품에 도달할 수 있습니다. 대부분의 SaaS 애플리케이션은 Application Load Balancer 또는 Network Load Balancer 뒤에 있습니다. AWS AppSync 프라이빗 APIs 또는 Amazon API Gateway 프라이빗 APIs는 인터페이스 VPC 엔드포인트를 통한 피어링 연결을 통해 대상이 될 수 있으므로 SaaS 애플리케이션에 대한 다른 일반적인 진입점입니다.

피어링 연결을 설정한 후에는 두 계정의 VPCs에 대한 라우팅 테이블을 업데이트하여 피어링 연결을 각 CIDR 범위의 다음 홉으로 정의해야 합니다. 이 솔루션은 여러 피어링 연결을 빠르게 관리하는 것이 너무 복잡해지기 때문에 소비자가 몇 명 있는 SaaS 공급자에게만 권장됩니다.

다음 다이어그램은 몇 가지 가능한 통합이 포함된 기본 구성을 보여줍니다. 두 소비자 계정VPCs는 SaaS 공급자 계정의 VPC와 피어링 연결이 있습니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 복구 시간: 통신을 위한 단일 장애 지점 없음
- 확장성: VPC 피어링에 대한 대역폭 제한 없음
- TCO: 동일한 가용 영역 내에서 피어링 연결 또는 피어링 연결을 통한 트래픽에 대한 비용 없음
- TCO: 관리할 인프라 없음
- 적응성: IPv6 지원
- 적응성: 리전 간 피어링 지원

다음은이 접근 방식의 단점입니다.

- 적응성: 전이적 라우팅을 지원하지 않음
- 적응성: 중복 CIDR 범위를 지원하지 않음
- 확장성: 제한된 확장성(VPC당 최대 125개의 피어링 연결)
- TCO: 추가 피어링 연결마다 복잡성이 기하급수적으로 증가합니다.
- TCO: 라우팅 테이블 관리, 피어링 연결 자체, 보안 그룹 규칙 및 트래픽 검사의 오버헤드
- 네트워크 격리: 양 당사자의 전체 VPCs가 노출되므로 엄격한 보안 제어가 필요합니다.

VPCs 연결 AWS Transit Gateway

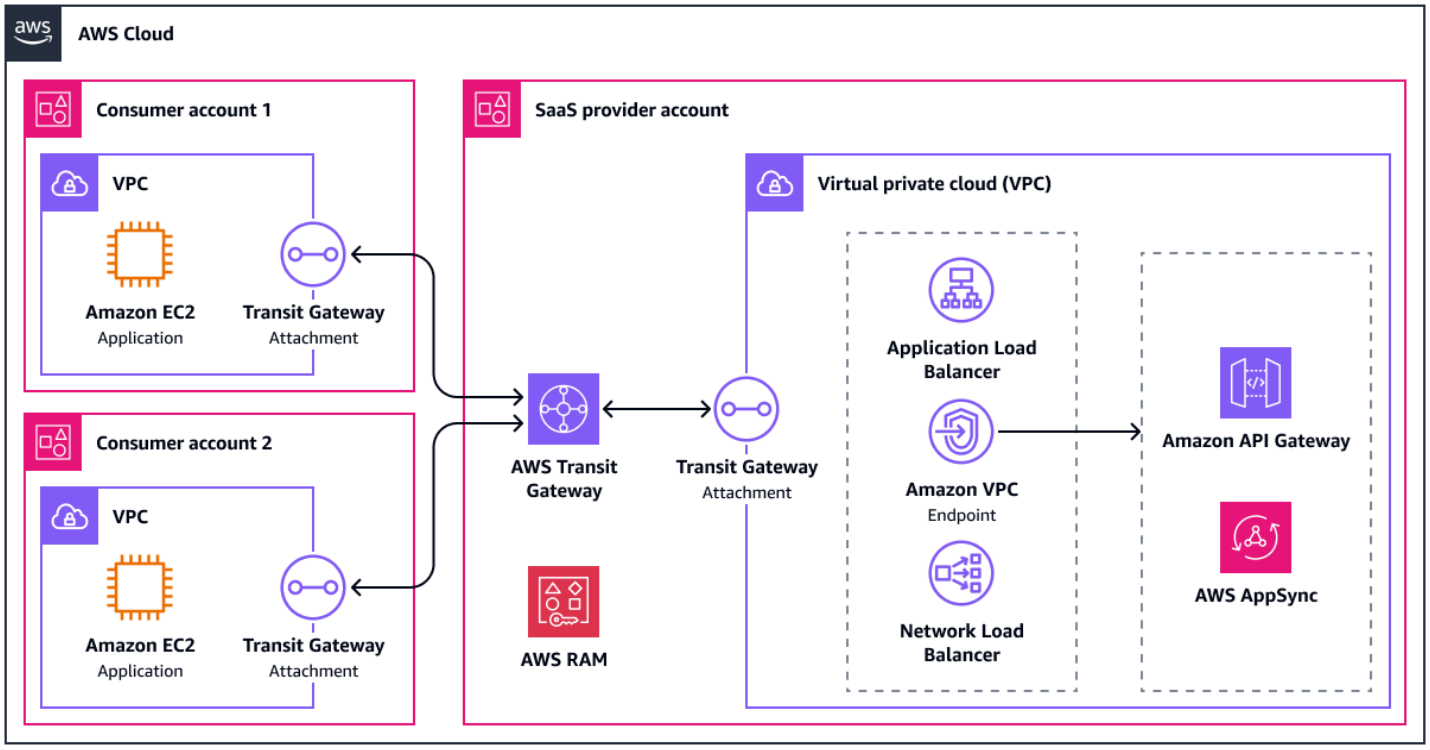
를 통해 VPCs 연결하면 VPC 연결이 AWS Transit Gateway생성되고 VPC에서 트래픽을 라우팅해야 하는 각 가용 영역의 서브넷에 네트워크 인터페이스가 배포됩니다. VPC 연결의 모든 가용 영역에 전용 /28 서브넷을 두는 것이 좋습니다. 자세한 내용은 Amazon VPC Transit Gateways 설계 모범 사례를 참조하세요. 배포된 네트워크 인터페이스를 통해 트래픽을 전송하려면 VPCs에 업데이트된 라우팅 테이블이 필요하며, 그에 따라 Transit Gateway 라우팅 테이블을 업데이트해야 합니다. 다중 테넌트 구성에서는 SaaS 공급자의 VPC가 모든 소비자의 VPCs. 소비자의 VPCs에는 SaaS 공급자의 VPC에 대한 경로만 있어야 합니다.

Transit Gateway는 설계상 가용성이 높습니다. VPC 흐름 로그를 사용한 모니터링을 지원하며 Transit Gateway 연결의 최대 대역폭은 가용 영역당 100Gbps입니다. VPC 피어링과 마찬가지로이 접근 방식은 VPC 간 보안 그룹 참조를 활성화하여 환경 간의 액세스 제어를 간소화합니다.

Transit Gateway를 사용하여 SaaS 제품에 소비자를 연결하는 두 가지 주요 옵션이 있습니다.

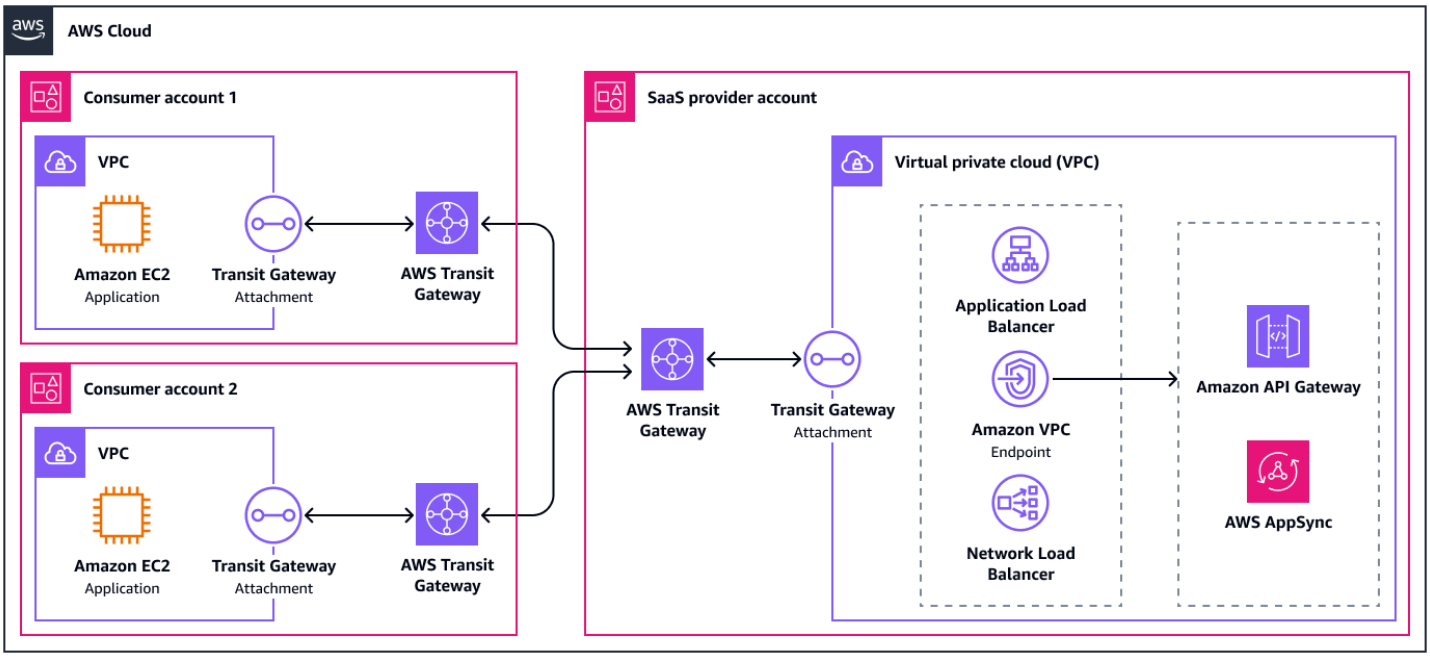
옵션 1: RAM 사용

첫 번째 옵션에서 서비스 공급자는 AWS Resource Access Manager (AWS RAM)를 사용하여 Transit Gateway를 소비자와 공유합니다. 이를 통해 소비자는 자신의 계정에 VPC 연결을 배포할 수 있습니다. 다음 다이어그램은이 옵션을 높은 수준으로 보여줍니다.



옵션 2: 피어링된 전송 게이트웨이

두 번째 옵션은 전송 게이트웨이를 소비자 계정의 전송 게이트웨이와 피어링하는 것입니다. 이렇게 하면 이제 소비자가 전송 게이트웨이 내의 라우팅 테이블을 완전히 제어할 수 있으므로 유연성이 향상됩니다. 예를 들어 서비스와 워크로드 간에 중앙 집중식 검사를 설정할 수 있습니다. 이 옵션의 단점은 전송 게이트웨이 간의 정적 라우팅만 지원된다는 것입니다. 다음 다이어그램은이 옵션을 높은 수준으로 보여줍니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 확장성: 최대 5,000개의 첨부 파일 지원
- 확장성: 연결된 모든 VPCs 한 곳
- 적응성: Transit GatewayVPNs, Direct Connect 게이트웨이 및 타사 SD-WAN 어플라이언스에도 연결할 수 있습니다.
- 적응성: 검사 VPC 추가와 같은 유연한 아키텍처
- 적응성: 전이적 라우팅 지원
- 적응성: 리전 내 및 리전 간 전송 게이트웨이 피어링 가능
- 적응성: IPv6 지원
- TCO: AWS Transit Gateway 는 완전 관리형 서비스이므로 운영 작업이 덜 필요합니다.
- TCO: TCO는 각 추가 전송 게이트웨이 연결에 따라 선형적으로 증가합니다.

다음은이 접근 방식의 단점입니다.

- 통합 용이성: 라우팅 구성에는 고급 네트워킹 지식이 필요합니다.
- 적응성: 중복 CIDR 범위를 지원하지 않음
- TCO: 라우팅 테이블 항목, 보안 그룹 규칙 및 트래픽 검사 관리의 오버헤드
- 보안: 양 당사자의 전체 VPCs가 노출되므로 엄격한 보안 제어가 필요합니다.

온프레미스에서 운영하는 서비스 소비자

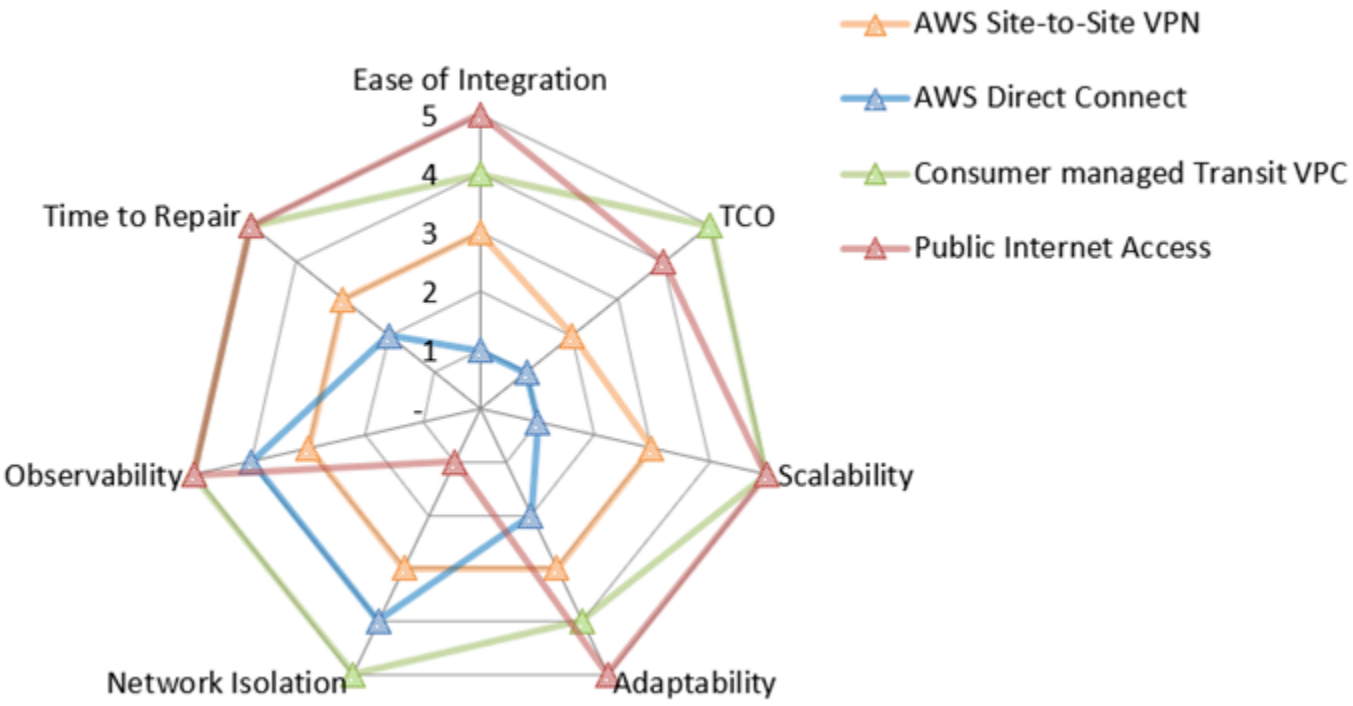
이 섹션에서는의 AWS 클라우드 SaaS 워크로드와 온프레미스 데이터 센터 간의 연결 옵션에 대해 설명합니다. 온프레미스 요구 사항이 있는 많은 소비자, 특히 엔터프라이즈 수준에서는 클라우드를 물리적 네트워크의 확장으로 보고 아키텍처에 이를 반영하려고 합니다. 즉, 논리적 터널을 통해 또는 프라이빗 물리적 연결을 통해 클라우드의 SaaS 제품에 대한 프라이빗 연결을 의미합니다. 다른 소비자는 퍼블릭 인터넷을 통한 연결을 수락하며,이 단원에서도 설명합니다.

이 섹션에서는 다음 네트워크 액세스 접근 방식에 대해 설명합니다.

- 에 연결 AWS Site-to-Site VPN
- 에 연결 AWS Direct Connect
- 전송 VPC 아키텍처에 연결
- 퍼블릭 인터넷을 통해 연결

다음 네트워킹 값 맵은 각 평가 지표에 대해 이러한 각 옵션의 점수를 요약합니다. 평가 지표에 대한 자세한 내용은이 가이드의 평가 지표를 참조하세요. 맵에서 5는 최저 TCO, 최상의 네트워크 격리 또는 최저 복구 시간과 같은 최고 점수를 나타냅니다. 이 레이더 차트를 읽는 방법에 대한 자세한 내용은이 가이드네트워킹 값 맵의 섹션을 참조하세요.

> **Note**
>
> 공급자 관리형 전송 VPC 옵션은 운영 중인 서비스에 따라 점수가 크게 달라지기 때문에 제외됩니다.



레이더 차트는 다음 값을 보여줍니다.

평가 지표	AWS Site-to-Site VPN	AWS Direct Connect	소비자 관리형 전송 VPC	퍼블릭 인터넷 액세스
통합 용이성	3	1	4	5
TCO	2	1	5	4
확장성	3	1	5	5
적응성	3	2	4	5
네트워크 격리	3	4	5	1
Observability	3	4	5	5
복구 시간	3	2	5	5

에 연결 AWS Site-to-Site VPN

AWS Site-to-Site VPN 가상 프라이빗 게이트웨이 또는 전송 게이트웨이에서 연결이 종료될 수 있습니다. 가상 프라이빗 게이트웨이는 단일 VPC에 연결할 수 있는 Site-to-Site VPN 연결 AWS 측의 VPN 엔드포인트입니다. 전송 게이트웨이는 여러 VPCs와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 전송 허브입니다. Site-to-Site VPN 연결 측 AWS 의 VPN 엔드포인트로도 사용할 수 있습니다. 이 섹션에서는 두 옵션에 대해 설명합니다.

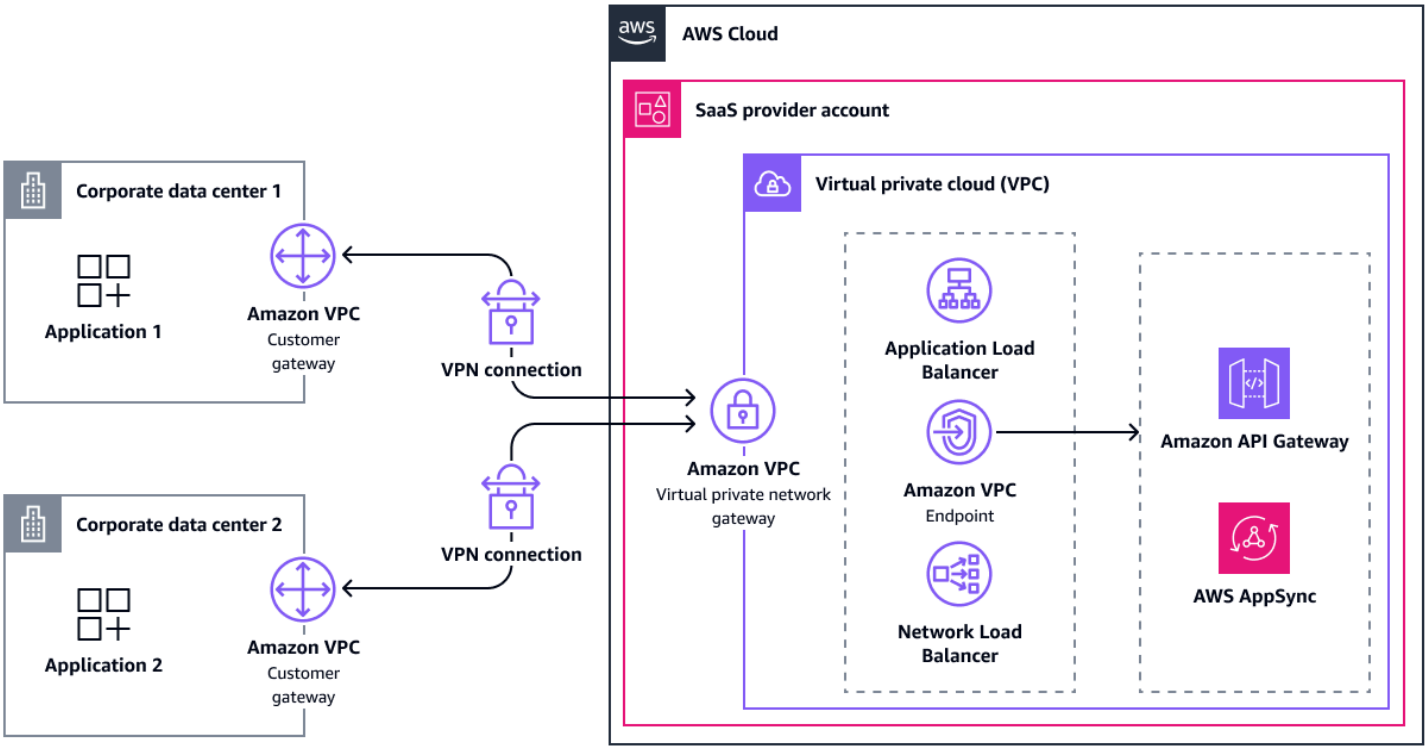
가상 프라이빗 게이트웨이를 통한 연결

가상 프라이빗 게이트웨이를 생성한 후 SaaS 제품이 포함된 VPC에 연결합니다. 그런 다음 경로 전파를 활성화하여 VPN 경로를 VPC 라우팅 테이블에 전파합니다. 이러한 경로는 정적 또는 BGP 광고 동적 경로일 수 있습니다.

고가용성을 위해 Site-to-Site VPN 연결에는 AWS 측면의 두 가용 영역에서 종료되는 두 개의 VPN 터널이 있습니다. 하나를 사용할 수 없게 되면 두 번째 터널이 인계될 수 있습니다. 단일 터널은 최대 1.25 Gbps의 대역폭을 허용합니다. 가상 프라이빗 게이트웨이는 등가 다중 경로 라우팅(ECMP)을 지원하지 않으므로 한 번에 하나의 터널만 사용할 수 있습니다.

내결함성을 높이기 위해 두 번째 물리적 고객 게이트웨이에 대한 두 번째 VPN 연결을 설정할 수 있습니다. 연결이 설정되면 소비자는 SaaS 공급자의 VPC에 있는 리소스에 연결할 수 있습니다.

다음 다이어그램은이 아키텍처를 보여줍니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 복구 시간: 보조 VPN 터널로의 관리형 장애 조치
- 관찰성: Network Synthetic Monitor를 사용하여 관리형 활성 모니터링을 위한 통합
- 통합 용이성: BGP를 통한 동적 라우팅 지원
- 적응성: 대부분의 온프레미스 네트워킹 장비와의 호환성
- 적응성: IPv6 지원
- TCO: AWS Site-to-Site VPN 는 완전 관리형 서비스이므로 운영 작업이 덜 필요합니다.
- TCO: 가상 게이트웨이에는 비용이 들지 않지만 각 게이트웨이에는 두 개의 퍼블릭 IPv4 주소에 대한 요금이 부과됩니다.
- 네트워크 격리: 인터넷을 통한 안전한 프라이빗 통신 활성화

다음은이 접근 방식의 단점입니다.

- 통합 용이성: 소비자가 고객 게이트웨이를 구성해야 함
- 확장성: ECMP 지원 부족으로 대역폭이 가상 게이트웨이당 1.25 Gbps로 제한됨
- 확장성: 네트워크 복잡성 및 운영 오버헤드 증가로 인한 확장 제한
- 적응성: VPN 터널의 내부 IP 주소에 대해서만 IPv6 지원

- 적응성: 전이적 라우팅 없음
- TCO: SaaS 공급자에 대한 수많은 VPN 연결을 유지 관리 및 구성하기 위한 운영 오버헤드

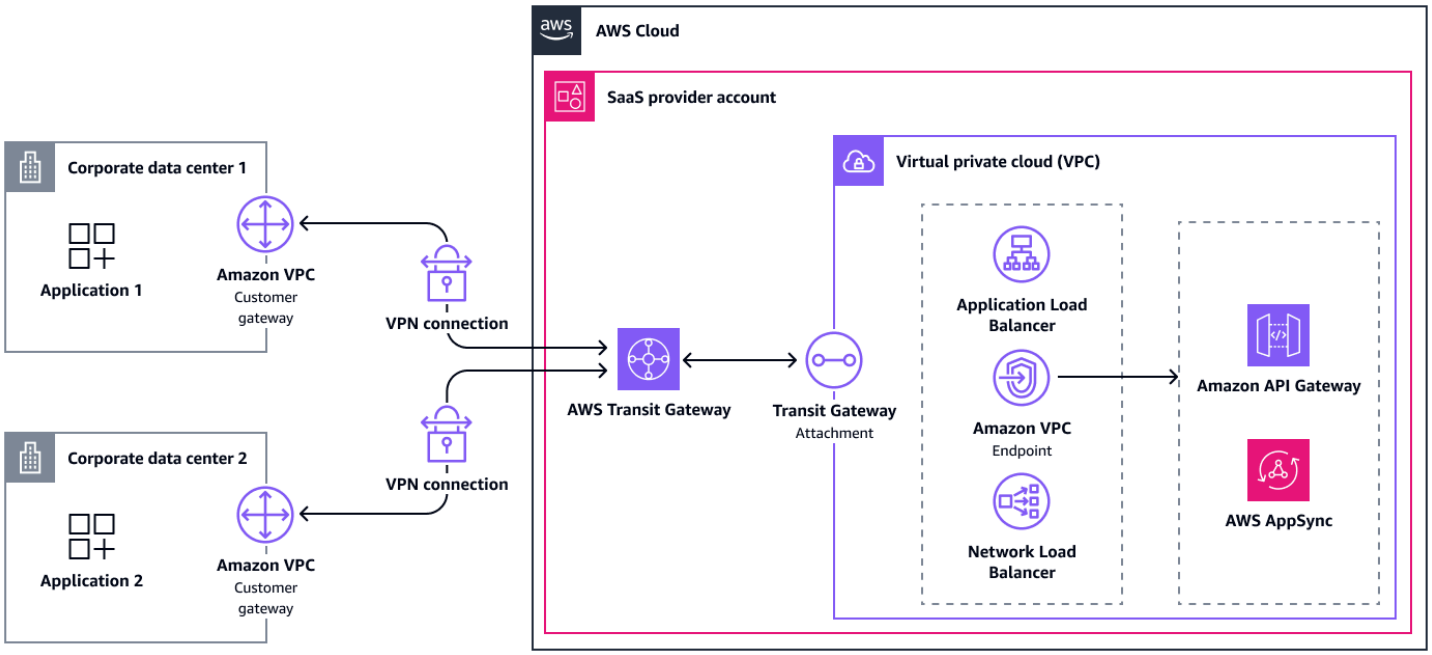
전송 게이트웨이를 통한 연결

전송 게이트웨이를 통한 연결은 가상 게이트웨이와 유사합니다. 하지만 염두에 두어야 할 몇 가지 차이점이 있습니다.

먼저 VPN 연결의 경로는 전송 게이트웨이 라우팅 테이블 내에서 자동으로 전파될 수 있지만 연결된 VPCs에 경로를 수동으로 추가해야 합니다.

가상 게이트웨이와 비교하여 Transit Gateway는 ECMP를 지원합니다. 고객 게이트웨이가 ECMP를 지원하는 경우 두 터널을 모두 사용하여 총 최대 처리량 2.5 Gbps를 달성할 수 있습니다. 동일한 온프레미스 네트워크와 전송 게이트웨이 간에 여러 연결을 설정할 수 있습니다. 이 접근 방식을 사용하면 최대 대역폭을 연결당 최대 2.5 Gbps까지 늘릴 수 있습니다.

다음 다이어그램은이 아키텍처를 보여줍니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 복구 시간: 보조 VPN 터널로의 관리형 장애 조치
- 관찰성: Network Synthetic Monitor를 사용하여 관리형 활성 모니터링을 위한 통합
- 통합 용이성: BGP를 통한 동적 라우팅 지원
- 확장성: ECMP 지원을 통해 VPN 처리량을 확장하여 대규모 대역폭 요구 사항 충족

- 확장성: 단일 전송 게이트웨이에서 지원하는 많은 수의 VPN 연결(최대 5,000개)
- 확장성: 모든 VPN 연결을 관리하고 모니터링할 수 있는 한 곳
- 적응성: 대부분의 온프레미스 네트워킹 장비와의 호환성
- 적응성: IPv6 지원
- 적응성:의 유연성 상속 AWS Transit Gateway
- TCO: AWS Transit Gateway 는 완전 관리형 서비스이므로 운영 작업이 덜 필요합니다.
- TCO: 가상 게이트웨이에는 비용이 들지 않지만 각 게이트웨이에는 두 개의 퍼블릭 IPv4 주소에 대한 요금이 부과됩니다.
- 네트워크 격리: 인터넷을 통한 안전한 프라이빗 통신 활성화

다음은이 접근 방식의 단점입니다.

- 통합 용이성: 소비자가 고객 게이트웨이를 구성해야 함
- 확장성: 네트워크 복잡성 및 운영 오버헤드 증가로 인한 확장 제한
- 적응성: VPN 터널의 내부 IP 주소에 대해서만 IPv6 지원
- TCO: SaaS 공급자에 대한 수많은 VPN 연결을 유지 관리 및 구성하기 위한 운영 오버헤드
- TCO: 사용에 대한 추가 요금 AWS Transit Gateway
- TCO: 전송 게이트웨이 라우팅 테이블을 관리하는 추가 복잡성

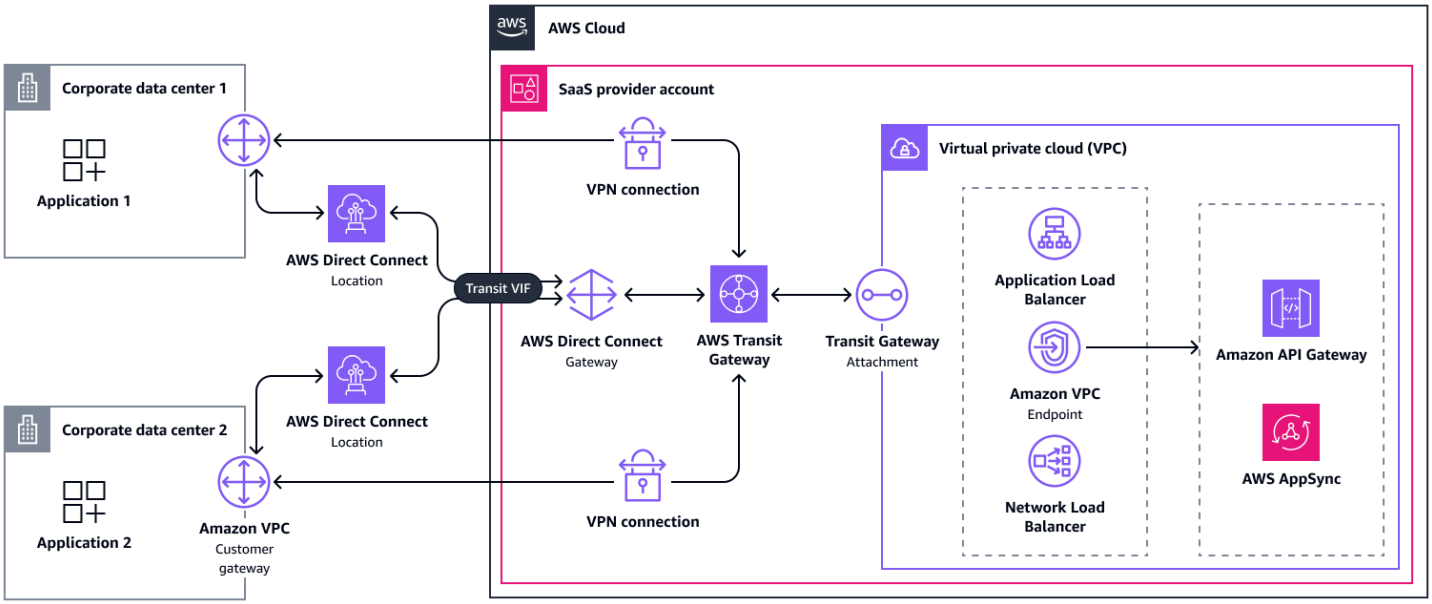
에 연결 AWS Direct Connect

AWS Direct Connect는 표준 이더넷 광섬유 케이블을 통해 내부 네트워크를 Direct Connect 위치에 연결합니다. 다른 아키텍처 옵션과 달리 몇 분 내에 전용 연결을 설정할 수 없습니다. 대신 모든 요구 사항이 충족되면이 프로세스에 최대 며칠이 걸릴 수 있습니다. 그렇지 않으면 시간이 더 걸릴 수 있습니다. 따라서 AWS 계정 팀에 문의하거나이 접근 방식에 AWS Support 도움을 요청하는 것이 좋습니다. 선택적으로 AWS 파트너가 제공하고 다른 고객과 공유하는 호스팅 연결을 선택할 수 있습니다. 아키텍처는에 관계없이 동일합니다. 지연 시간을 줄이거나, 대역폭을 개선하거나, 규제 요구 사항을 준수하기 때문에 선택할 Direct Connect 수 있습니다.

Direct Connect 연결을 사용하려면 소비자가 퍼블릭, 프라이빗 또는 전송 가상 인터페이스를 생성해야 합니다. 다양한 아키텍처 옵션을 사용할 수 있습니다. 여러 온프레미스 위치를에 연결하는 가장 유연한 방법은 Direct Connect 게이트웨이에 연결된 AWS 클라우드 전송 가상 인터페이스입니다. Direct Connect 게이트웨이는 서비스 공급자가 최대 6개의 전송 게이트웨이를 연결할 수 있는 글로벌 논리적 구성 요소입니다. 또한 게이트웨이에 최대 30개의 가상 인터페이스를 연결할 수 있습니다. 확장을 위해

추가 Direct Connect 게이트웨이를 생성할 수 있습니다. SaaS 공급자 계정에서 전송 게이트웨이는 앞서 설명한 대로 VPCs에 연결됩니다.

소비자는 원하는 복원력 수준에 따라 총 1개 또는 2개의 Direct Connect 위치에서 1~4개의 Direct Connect 연결을 사용하여 연결할 수 있습니다. 자세한 내용은 최대 복원력을 Direct Connect 위한 구성을 참조하세요. 인터넷을 통한 AWS Site-to-Site VPN 연결은 Direct Connect 연결을 위한 저렴한 백업 경로 역할을 할 수도 있습니다. 지원되는 Direct Connect 전용 연결은 MACsec을 사용하여 Direct Connect 위치와 데이터 센터 간에 계층 2의 링크를 암호화할 수 있습니다. 데이터의 추가 기밀성을 위해 Site-to-Site VPN 연결을 사용하는 것이 일반적입니다. Site-to-Site VPN 연결은 일반 VPN 연결을 사용하여 전송 게이트웨이에서 종료할 수 있습니다. 다음 다이어그램은이 아키텍처를 보여줍니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 관찰성: Network Synthetic Monitor를 사용하여 관리형 활성 모니터링을 위한 통합
- 확장성: 대역폭 처리량 증가 지원
- 적응성: IPv6 지원
- TCO: 데이터 전송을 줄일 수 있는 가능성
- TCO: 일관된 네트워크 경험
- 네트워크 격리: 규제 요구 사항을 충족할 수 있는 프라이빗 연결

다음은이 접근 방식의 단점입니다.

- 통합 용이성: 설정 시간 및 수동 작업

- 확장성: 추적할 할당량이 여러 개 있으므로 수십 개의 Direct Connect 연결 이상으로 확장성이 제한됨 https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html
- 적응성: 구성 옵션은 사용 가능한 Direct Connect 위치에 따라 다릅니다.
- TCO: 정기 Direct Connect 유지 관리로 인해 조치가 필요한 가동 중지가 발생할 수 있습니다.

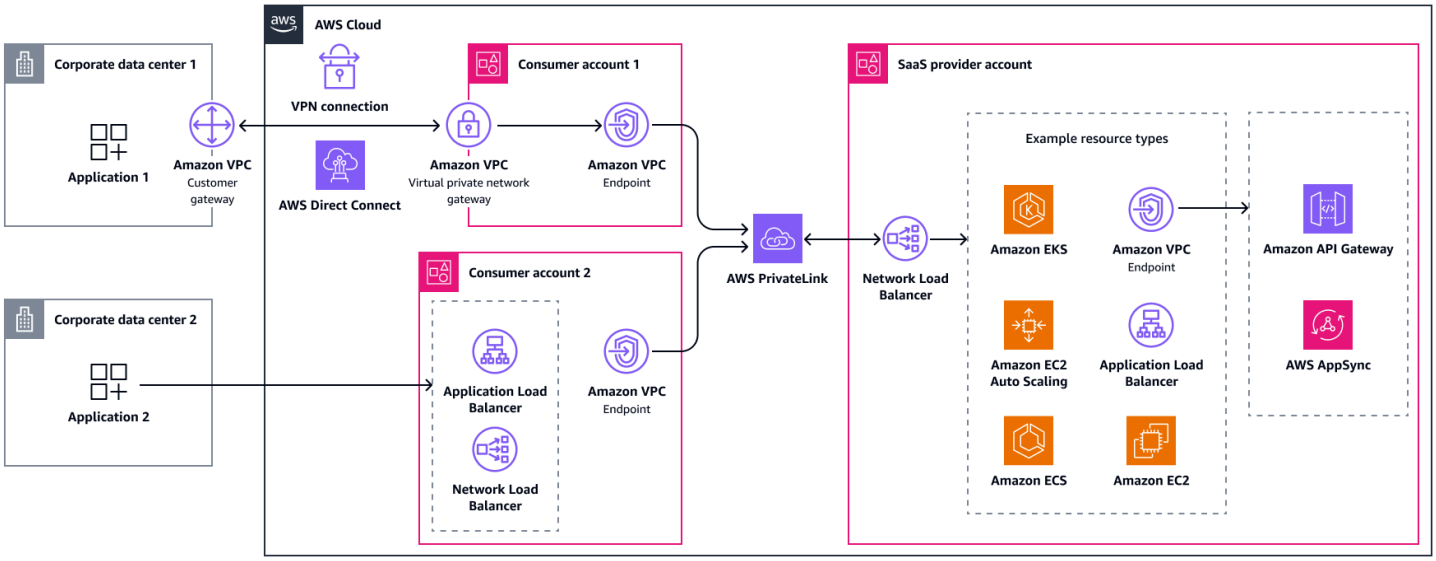
전송 VPC 아키텍처에 연결

Transit VPC는 소비자에게 연결 방법에 대한 유연성을 제공하는 아키텍처 옵션으로 AWS, SaaS 공급자는 이를 통해 서비스에 대한 통합 액세스를 활용할 수 있습니다 AWS PrivateLink. 소비자는 온프레미스에서 진입점(예: 가상 프라이빗 게이트웨이)과 AWS PrivateLink 리소스인 인터페이스 VPC 엔드포인트만 포함하는 전송 VPC에 연결합니다. 전송 VPCs는 SaaS 공급자 또는 소비자가 소유해야 합니다. 이 섹션에서는 두 옵션에 대해 설명합니다.

온프레미스 데이터 센터와 호환되는 CIDR 범위를 사용하여 전송 VPC 및 서브넷을 생성할 수 있습니다. 프라이빗 연결이 필요한 경우 소비자는 AWS Direct Connect 또는를 통해 해당 VPC에 연결할 수 있습니다 AWS Site-to-Site VPN. VPC 엔드포인트를 가리키는 Application Load Balancer 또는 Network Load Balancer를 사용하여 퍼블릭 인터넷에서 전송 계정에 대한 액세스를 구성할 수도 있습니다.

소비자 관리형 전송 VPC

이 접근 방식에서 SaaS 공급자는 전송 VPCs 맡깁니다. 기술적 관점에서 SaaS 공급자의 아키텍처는 를 통해 소비자 AWS 클라우드 에 연결할 때와 동일합니다 AWS PrivateLink. 판매 및 제품 관점에서 볼 때 일부 소비자는 AWS 계정 아직 하지 않기 때문에 추가 노력이 필요합니다. 계정을 열고 운영하는 것을 주저할 수 있습니다. SaaS 공급자는 소비자에게 온프레미스 데이터 센터를 생성하고 AWS 계정 연결하는 방법에 대한 지침을 제공해야 합니다. 다음 다이어그램은 소비자가 전송 VPCs를 소유하는 퍼블릭 액세스와 프라이빗 액세스의 조합을 보여줍니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

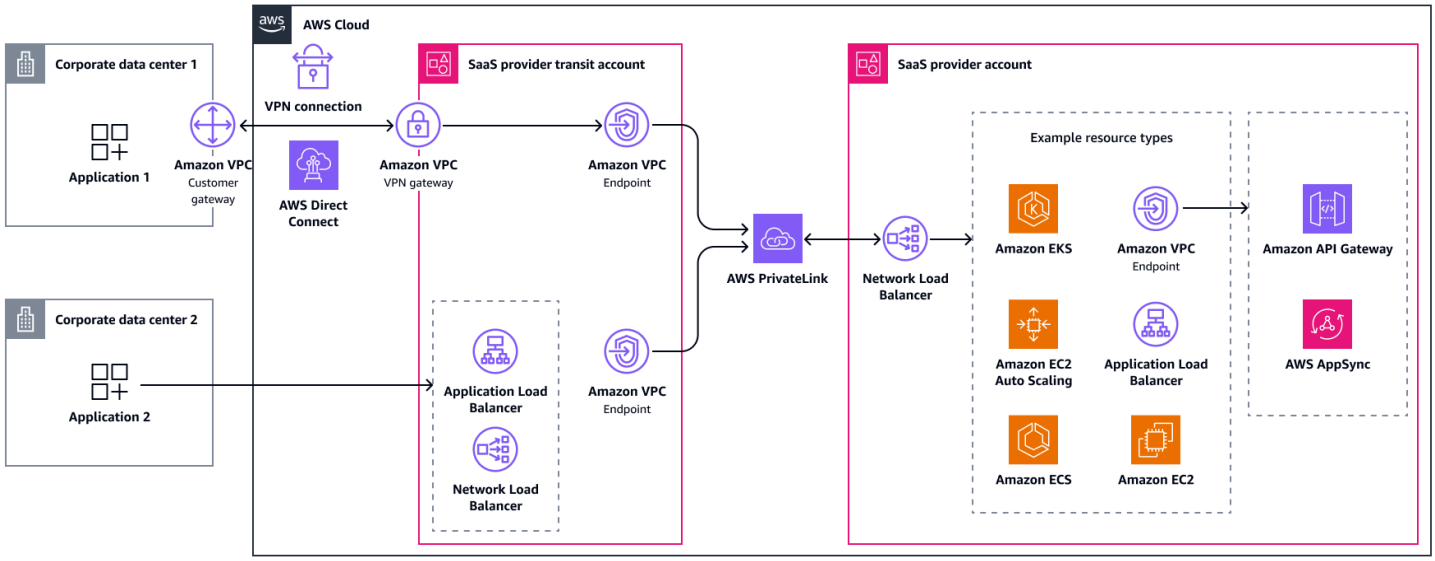
- 복구 시간: 운영 오버헤드는 대부분 SaaS 소비자에게 오프로드됩니다.
- 적응성: SaaS 소비자는 다양한 액세스 옵션 중에서 선택할 수 있습니다.
- 적응성: Site-to-Site VPN 또는를 사용하는 경우에도 CIDR 범위 충돌 없음 Direct Connect
- 모든 지표: 서비스 공급자가 AWS PrivateLink 혜택을 상속합니다.

다음은이 접근 방식의 단점입니다.

- 통합 용이성: SaaS 소비자는 하나 이상의가 필요합니다. AWS 계정
- TCO: 전송 VPC는 완전 관리형 서비스가 아닌 아키텍처이므로 더 많은 운영 노력이 필요합니다.

공급자 관리형 전송 VPC

이 접근 방식은 동일한 기술을 사용하지만 계정 경계와 책임은 변경됩니다. 여기서 SaaS 공급자는 전송 VPCs, 가급적이면 SaaS 제품과 별도의 계정에서 소유합니다. 이렇게 분리하면 비용이 절감되고, 위험이 줄어들며, 전송 계정을 독립적으로 확장할 수 있습니다. 높은 수준의 격리가 필요한 환경의 경우 서브넷을 사용하거나 각 소비자에 대해 별도의 전송 VPC를 생성하여 테넌트 간에 추가 분리를 생성할 수 있습니다. 그런 다음 소비자는 전송 VPC에 연결하는 방법을 선택할 수 있습니다. 이 접근 방식은 총 주소 지정 가능 시장을 확장할 수 있는 더 많은 옵션을 제공하지만 추가 아키텍처 구성 요소를 운영하고 모니터링해야 하기 때문에 SaaS 공급자의 TCO가 더 높습니다.



이 접근 방식은 다음과 같은 이점이 있습니다.

- 적응성: SaaS 소비자는 다양한 액세스 옵션 중에서 선택할 수 있습니다.
- 적응성: SaaS 소비자는 AWS 계정
- 적응성: Site-to-Site VPN 또는를 사용하는 경우에도 CIDR 범위 충돌 없음 Direct Connect

다음은이 접근 방식의 단점입니다.

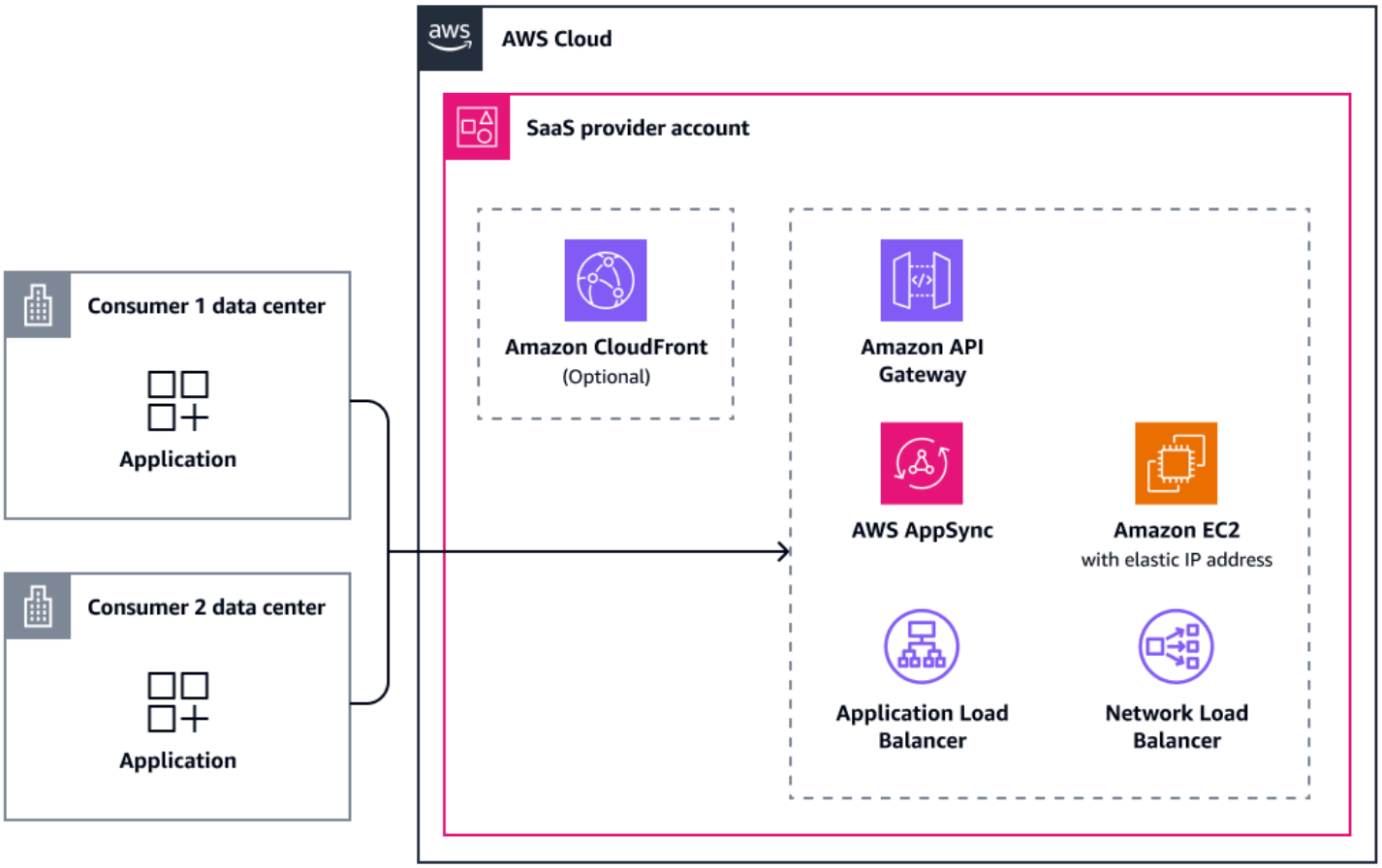
- TCO: 전송 VPC는 완전 관리형 서비스가 아닌 아키텍처이므로 더 많은 운영 노력이 필요합니다.
- TCO: SaaS 공급자는 추가 아키텍처 구성 요소를 운영하고 모니터링해야 합니다.

퍼블릭 인터넷을 통해 연결

퍼블릭 인터넷 액세스는 SaaS 제품에 대한 액세스를 제공하기 위한 유효한 옵션이기도 하지만, 기존 방식으로는 프라이빗 연결을 제공하지 않습니다. 일부 소비자는 자신과 SaaS 공급자 간에 추가 네트워킹 인프라가 필요하지 않기 때문에 여전히 퍼블릭 액세스 접근 방식을 선호할 수 있습니다. 공격 표면 증가에 대한 대가로 복잡성, 비용 및 통합 시간을 줄입니다. 강력한 인증 및 권한 부여 메커니즘은 증가된 위협 수준을 완화하는 데 도움이 될 수 있으며 항상 트래픽을 암호화해야 합니다. 이 시나리오에서는를 사용하는 등 추가 보안 계층을 사용하는 것이 좋습니다AWS WAF.

이 시나리오의 아키텍처는 간단합니다. 소비자는 인터넷을 통해 퍼블릭 호스트(SaaS 공급자)에 연결합니다. 애플리케이션은 탄력적 IP 주소를 사용하여 퍼블릭 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 직접 호스팅할 수 있습니다. 기본 옵션은 Application Load Balancer 또는 유사

한 서비스 뒤에 호스팅하는 것입니다. 성능 향상 및 정적 자산 캐싱을 위해 Amazon CloudFront와 같은 콘텐츠 전송 네트워크를 사용할 수 있습니다. 두 개의 글로벌 정적 애니캐스트 IP 주소를 통해 최소 지연 시간으로 애플리케이션을 제공하려면 Amazon EC2 인스턴스, Network Load Balancer 또는 Application Load Balancer 앞에 AWS Global Accelerator를 배치할 수 있습니다. 또한 CloudFront, Application Load Balancer AWS AppSync및 Amazon API Gateway는 모두와 통합됩니다 AWS WAF. 다음 다이어그램은 퍼블릭 인터넷 액세스 연결 옵션의 개요를 제공합니다.



다음 표에서는이 시나리오에서 지원되는 프로토콜 및 통합에 대해 설명합니다.

서비스 또는 리소스	IPv6	AWS WAF 통합	Global Accelerator 엔드포인트일 수 있음
Amazon CloudFront	지원됨	지원됨	지원되지 않음
Amazon API Gateway	지원됨	지원됨	지원되지 않음
AWS AppSync	일부 지원	지원됨	지원되지 않음

탄력적 IP 주소가 있는 Amazon EC2	지원됨	지원되지 않음	지원됨
Application Load Balancer	지원됨	지원됨	지원됨
Network Load Balancer	지원됨	지원되지 않음	지원됨

이 접근 방식은 다음과 같은 이점이 있습니다.

- 통합 용이성: 단순성 및 접근성
- 확장성: 무제한 규모 조정
- 적응성: CIDR 범위 충돌 가능성 없음
- 적응성: CloudFront 지원

다음은이 접근 방식의 단점입니다.

- 네트워크 격리: 프라이빗 연결 없음
- 네트워크 격리: 강력한 보안 조치 필요

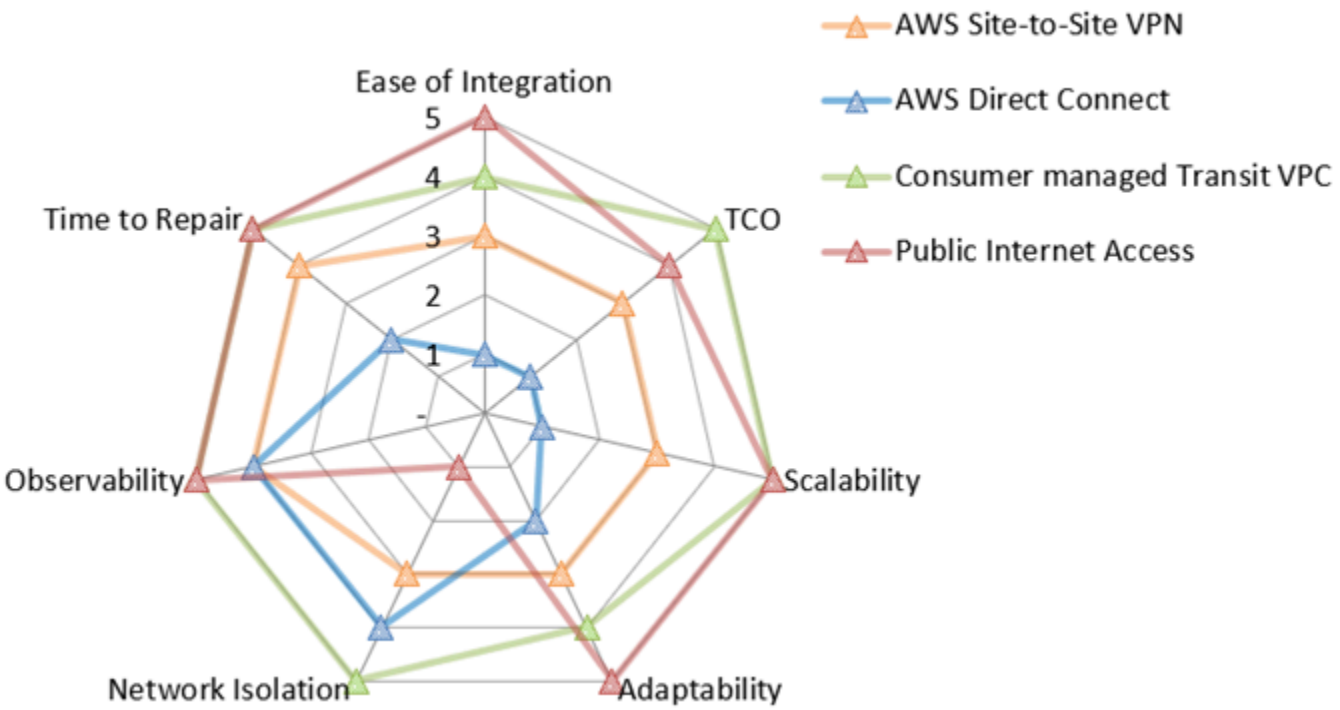
선택한 서비스에 따라 다른 이점과 단점이 적용됩니다.

다른 클라우드 서비스 공급자에서 운영하는 SaaS 소비자

이 시나리오에서는 다른 클라우드 서비스 공급자(CSPs)의 소비자를 위한 솔루션을 설명합니다. 이 시나리오는 온프레미스 데이터 센터에 대한 연결과 몇 가지 공통점을 공유합니다. 실제로 온프레미스 환경의 모든 연결 옵션은 다른 CSPs, 일부 CSPs AWS Direct Connect 에서는 와의 프라이빗 연결도 가능합니다. 대부분의 CSPs AWS Site-to-Site VPN 또는를 AWS 클라우드 통해에 연결하는 방법에 대한 설명서와 지원을 제공합니다 AWS Direct Connect.

Site-to-Site VPN을 선택하면 소비자는 각 CSP의 관리형 게이트웨이 또는 유사한 리소스를 활용할 수 있습니다. 온프레미스 시나리오와 같이 소비자는 직접 설정할 필요가 없습니다. 이는 복구 시간 및 관찰성 개선과 같은 Site-to-Site VPN에 대한 일부 지표에 영향을 미칩니다. 이는 이제 연결의 양쪽 끝이 모두 관리되기 때문입니다.

다음 네트워킹 값 맵은 각 평가 지표에 대해 이러한 각 옵션의 점수를 요약합니다. Site-to-Site VPN의 값은 다르지만 온프레미스 연결의 네트워킹 값 맵과 매우 유사합니다. 평가 지표에 대한 자세한 내용은이 가이드평가 지표의 섹션을 참조하세요. 맵에서 5는 최저 TCO, 최상의 네트워크 격리 또는 최저 복구 시간과 같은 최고 점수를 나타냅니다. 이 레이더 차트를 읽는 방법에 대한 자세한 내용은이 가이드네트워킹 값 맵의 섹션을 참조하세요.



레이더 차트에는 다음 값이 표시됩니다.

평가 지표	AWS Site-to-Site VPN	AWS Direct Connect	소비자 관리형 전송 VPC	퍼블릭 인터넷 액세스
통합 용이성	3	1	4	5
TCO	3	1	5	4
확장성	3	1	5	5
적응성	3	2	4	5
네트워크 격리	3	4	5	1
Observability	4	4	5	5

복구 시간	4	2	5	5

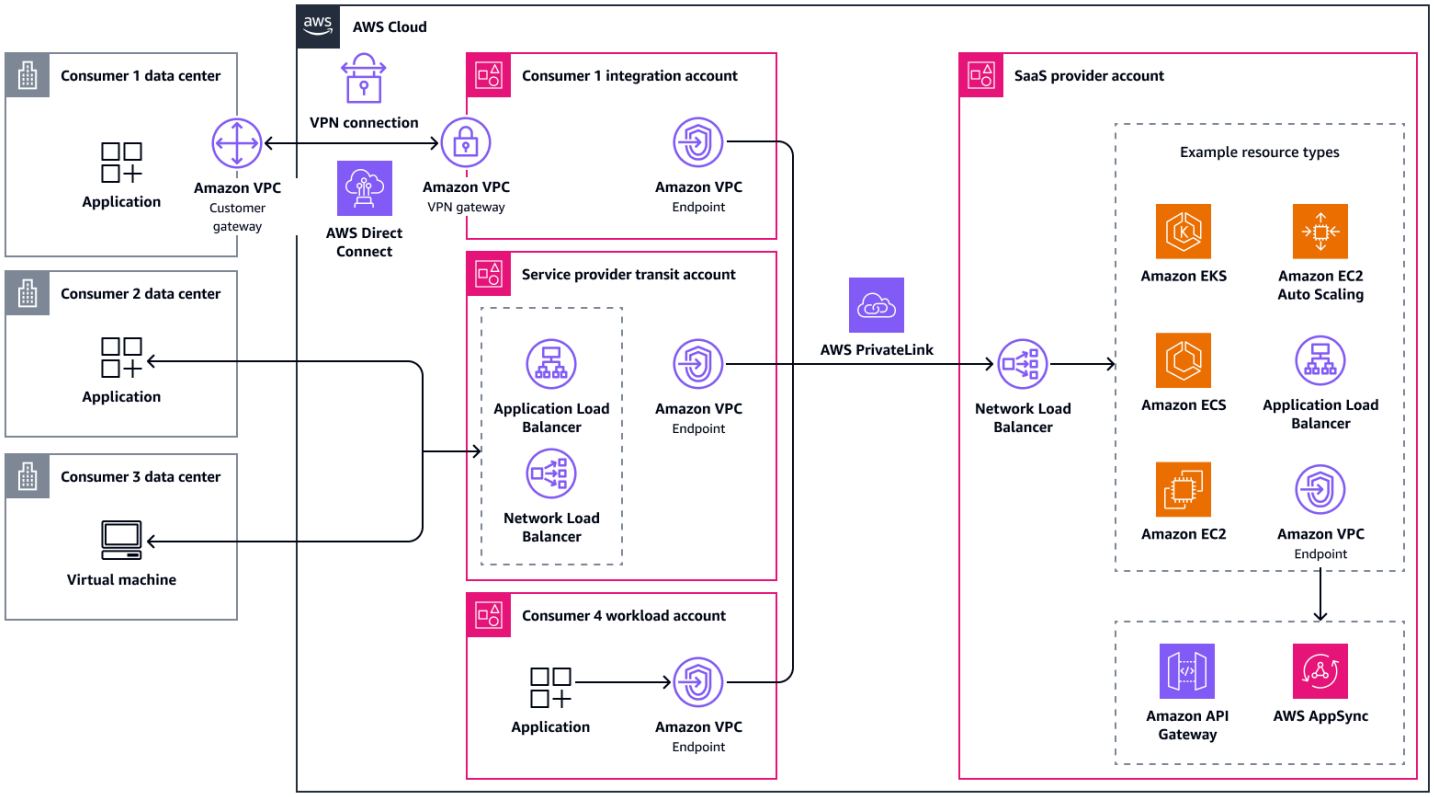
하이브리드 환경 지원

소비자는 서로 다른 환경에서 오는 것이 일반적이며, 각 환경에는 고유한 기술 및 보안 제약이 있습니다. 일부 고객은 인터넷 또는 전용 네트워크 링크를 통한 보안 연결이 필요한 온프레미스 데이터 센터에서 전적으로 운영할 수 있습니다. 다른는 이미 내에서 워크로드를 실행 중일 수 AWS 있으며 지연 시간이 짧은 프라이빗 네트워크 경로를 예상합니다. 세 번째 그룹은 연결이 서로 다른 클라우드 네트워크를 연결해야 하는 다른 CSPs에 의존할 수 있습니다.

그럼에도 불구하고 SaaS 애플리케이션에 대한 표준화된 네트워크 액세스를 목표로 하여 아키텍처를 간소화하고 운영 복잡성을 줄여야 합니다. 이전에 제시한 두 가지 접근 방식인 퍼블릭 인터넷 액세스 및 전송 VPCs 이러한 시나리오에서 잘 작동합니다. 퍼블릭 인터넷 액세스는 고객에게 최소한의 설정으로 가장 빠른 온보딩 경로를 제공합니다. 전송 VPCs 종종를 사용하여 보다 제어된 프라이빗 액세스를 제공합니다 AWS PrivateLink.

SaaS 상품을 설계할 때 단일 네트워크 액세스 모델을 채택하거나 여러 접근 방식을 계층화된 상품으로 결합할 수 있습니다. 예를 들어 연결 용이성과 신속한 온보딩을 우선시하는 고객에게 퍼블릭 액세스 배포 티어를 제공하고 엄격한 규정 준수 또는 보안 제어 요구 사항이 있는 고객에게 프라이빗 액세스 배포 티어를 제공할 수 있습니다. 이러한 계층에는 비용, 성능 및 위험 프로필이 다릅니다. 두 접근 방식을 모두 단일 아키텍처로 결합할 수도 있습니다. 이 경우 퍼블릭 및 프라이빗 경로가 격리된 상태로 유지되도록 강력한 보안 조치가 있는지 확인합니다.

다음 다이어그램은 소비자가 데이터 센터 또는 CSP에서 공개적으로 또는 (에 워크로드가 있는 경우 AWS PrivateLink)를 통해 비공개로 연결할 수 있는 하이브리드 액세스 접근 방식을 보여줍니다 AWS 클라우드.


AWS Cloud
Consumer 1 data center
Application
Amazon VPC
Customer gateway
VPN connection
AWS Direct Connect
Amazon VPC
VPN gateway
Consumer 1 integration account
Amazon VPC
Endpoint
Consumer 2 data center
Application
Consumer 3 data center
Virtual machine
Service provider transit account
Application Load Balancer
Network Load Balancer
Amazon VPC
Endpoint
Consumer 4 workload account
Application
Amazon VPC
Endpoint
AWS PrivateLink
SaaS provider account
Network Load Balancer
Example resource types
Amazon EKS
Amazon EC2 Auto Scaling
Amazon ECS
Application Load Balancer
Amazon EC2
Amazon VPC
Endpoint
Amazon API Gateway
AWS AppSync

의 SaaS 제품에 대한 고급 네트워킹 액세스 시나리오 AWS 클라우드

의 SaaS 제품에 대한 네트워킹 액세스 시나리오 AWS 클라우드 섹션에서 설명하는 아키텍처는 대부분의 사용 사례에 대한 솔루션을 찾는 데 도움이 될 것입니다. 그러나 특정 기술 요구 사항이 있는 몇 가지 시나리오가 있습니다. 많은가이 가이드의 범위를 벗어납니다.

이 섹션에서는 다음과 같은 고급 기술 요구 사항 및 고려 사항에 대해 설명합니다.

- 양방향 통신
- TCP, UDP 및 독점 프로토콜

양방향 통신

경우에 따라 애플리케이션이 예상대로 작동하려면 양방향 트래픽이 필요합니다. 일반적인 사용 사례는 웹후크 또는 알림 서비스입니다. 일반적으로 서버와 클라이언트 간에 WebSocket 연결을 통해 이를 달성할 수 있습니다. 이 연결은 TCP 세션을 열어 두고 두 참가자가 연결을 통해 트래픽을 전송할 수 있도록 합니다. 이 가이드에서 설명하는 대부분의 서비스는 Network Load Balancer, Application Load Balancer, Amazon API Gateway AWS PrivateLink및 AWS AppSync (프라이빗 실시간 엔드포인트를 통해)를 포함하여 기본적으로 WebSocket을 지원합니다.

경우에 따라 SaaS 공급자 측 애플리케이션이 데이터베이스와 같은 소비자 측 리소스에 액세스해야 할 수 있습니다. 연결과 같은 양방향 채널을 통해 AWS Site-to-Site VPN 연결하는 경우 문제가 되지 않습니다.

반면 AWS PrivateLink Elastic Load Balancing은 단방향 트래픽만 지원합니다. 이러한 서비스를 사용하는 경우 SaaS 제품에서 시작하는 트래픽에 대해 다른 네트워크 경로를 설정해야 합니다. 예를 들어 역방향으로 이동하는 추가 AWS PrivateLink 연결일 수 있습니다.

TCP, UDP 및 독점 프로토콜

많은 애플리케이션이 HTTP 또는 HTTPS를 통해 제공되지만 전부는 아닙니다. 일부는 메시지 대기열 원격 측정 지원(MQTT)과 같은 TCP 위에 다른 계층 7 프로토콜을 사용할 수 있습니다. UDP를 사용하여 소비자에게 서비스를 제공하는 경우도 있습니다. 드문 경우지만 서비스는 패킷 내에서 전송해야 하는 독점 프로토콜을 사용합니다(계층 3). 이러한 시나리오에서는 SaaS 서비스를 지원하는 서비스를 이해하는 것이 중요합니다.

계층 3 서비스의 경우 AWS PrivateLink 모든 TCP 및 UDP 트래픽을 지원하는 및 Network Load Balancer를 사용할 수 있습니다.

계층 7 서비스의 경우 Application Load Balancer 및 Amazon CloudFront는 HTTP, HTTPS, WebSocket 및 Google 원격 프로시저 호출(gRPC)을 지원합니다. 마찬가지로 Amazon API Gateway 및 AWS AppSync 각는 HTTP, HTTPS 및 WebSocket을 지원합니다. Amazon CloudFront는 현재 HTTP/3를 지원하는 유일한 서비스입니다.

Amazon VPC Lattice를 사용하여 계층 7 애플리케이션과 계층 3 리소스를 연결할 수 있습니다. HTTP, HTTPS, gRPC, TCP 및 TLS 패스스루를 지원합니다.

애플리케이션이 계층 3을 통해서만 트래픽을 제공할 수 있는 경우 AWS Transit Gateway AWS Direct Connect AWS Site-to-Site VPN, 및 VPC 피어링과 같은 코어 AWS 네트워킹 서비스를 사용하는 것이 중요합니다. 그런 다음 트래픽은 SaaS 소비자에서 SaaS 서비스의 컴퓨팅 계층으로 직접 라우팅되어야 합니다.

에서 네트워크 액세스를 위한 안티 패턴 AWS 클라우드

안티 패턴은 솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다. 이 단원에서 언급한 설계 옵션은 일반적으로 작동하지만 상당한 단점이 있습니다. 가능하면 더 나은 대안을 사용할 수 있으므로 피해야 합니다.

이 섹션에서는 다음 안티 패턴 및 문제에 대해 설명합니다.

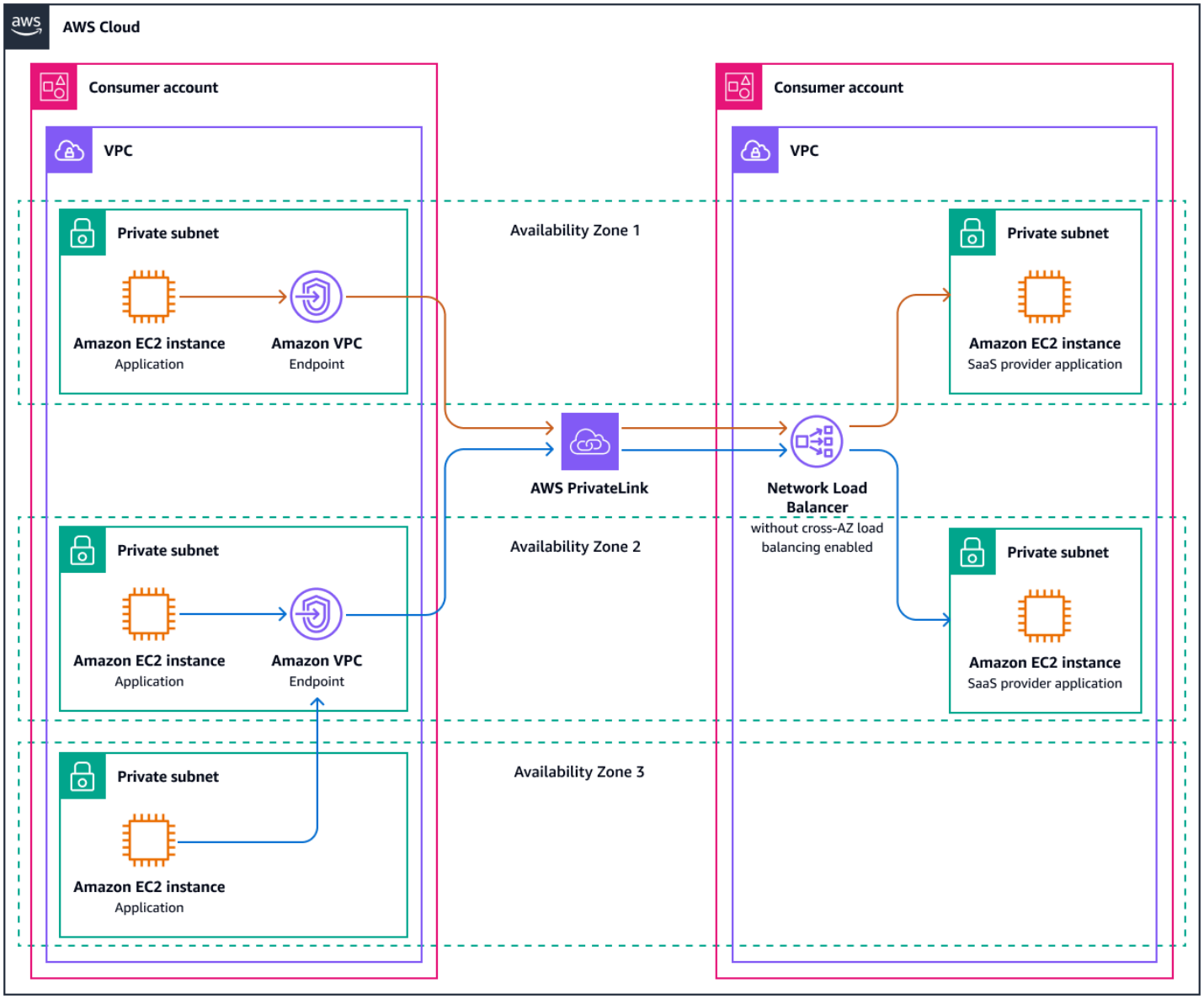
- 와 가용 영역 불일치 AWS PrivateLink
- AWS Site-to-Site VPN 간 연결 AWS 계정

와 가용 영역 불일치 AWS PrivateLink

를 통해 애플리케이션에 대한 액세스를 제공할 때 AWS PrivateLink SaaS 소비자는 애플리케이션이 배포된 가용 영역에서만 인터페이스 VPC 엔드포인트를 생성할 수 있습니다. 예를 들어 애플리케이션이 use1-az1 및에 배포된 경우 use1-az2소비자는에 VPC 엔드포인트를 배포할 수 없습니다use1-az3. 모든 가용 영역에 SaaS 제품을 배포하는 것이 좋습니다. 대부분의 AWS 리전 에는 3개의 가용 영역이 있지만 일부에는 더 많은 가용 영역이 있습니다. 전체 목록은 리전 및 가용 영역을 참조하세요. 를 선택할 때 가용 영역 수를 고려합니다 AWS 리전.

> **Note**
>
> 가용 영역 이름은 가용 영역 IDs 다릅니다. 자세한 내용은 AWS 리소스의 가용 영역 IDs를 참조하세요.

SaaS 공급자가 모든 가용 영역에 배포하지 않기로 선택하면 몇 가지 결과가 발생합니다. SaaS 오퍼링이 use1-az1 및에 배포use1-az2되었지만 소비자가를 포함한 세 개의 가용 영역을 모두 사용하고 있다고 가정합니다use1-az3. 인터페이스 VPC 엔드포인트는 use1-az1 및의 소비자 측에 배포되며use1-az2, 이제의 애플리케이션이 이러한 엔드포인트 중 하나에 액세스use1-az3해야 합니다. 먼저 일치하지 않는 가용 영역의 서브넷에서 각 VPC 엔드포인트로 트래픽을 허용해야 합니다. 소비자는 리전 AWS PrivateLink DNS 이름을 사용하기로 결정할 수 있습니다.이 이름은 VPC 엔드포인트 중 하나로 확인될 수 있으며 두 엔드포인트 간에 트래픽을 균등하게 분산합니다. 또는 소비자가와 같은 엔드포인트로 직접 트래픽을 전송하도록 선택할 수 있습니다use1-az2. 이로 인해 트래픽의 67%가의 공급자 측에 도착use1-az2하고의 33%가 도착합니다use1-az1. 다음 그림은이 시나리오를 보여줍니다.



소비자 수가 많고 트래픽이 고르지 않게 분산되면 워크로드는 한 가용 영역에서 용량 문제가 발생하고 다른 가용 영역에서는 용량이 부족할 수 있습니다. 이 문제를 해결하기 위해 SaaS 공급자는 Network Load Balancer에서 교차 영역 로드 밸런싱을 활성화하여 트래픽을 균등하게 로드 밸런싱하기로 결정할 수 있습니다. 이로 인해 추가 요금이 발생합니다.

서비스 공급자가 하나의 가용 영역만 일치하면 모든 트래픽이 단일 엔드포인트를 통해 들어갑니다. 이로 인해 불균형이 더욱 커집니다. 따라서 소비자는 더 이상 SaaS 제품을 고가용성으로 사용할 수 없습니다. 자체적으로 사용하지 않는 추가 가용 영역을 통해 애플리케이션을 제공하는 경우 소비자에게는 중요하지 않습니다. 최악의 경우 SaaS 공급자는 동일한 가용 영역을 사용하지 않는 소비자에게 서비스를 제공하지 못할 수 있습니다.

드문 경우지만 SaaS 공급자가 모든 가용 영역에 애플리케이션을 프로비저닝할 수 있는 옵션이 없는 경우 누락된 가용 영역에만 서브넷을 생성한 다음 빈 가용 영역으로 서비스를 확장할 수도 있습니다. 그러면 교차 영역 로드 밸런싱이 다른 가용 영역의 실제 애플리케이션 엔드포인트를 통해 수신 트래픽을 분산할 수 있습니다.

AWS Site-to-Site VPN 간 연결 AWS 계정

온프레미스 환경에서 클라우드로 마이그레이션하는 기업은 때때로 전체 네트워크를 리프트 앤 시프트하려고 합니다. 이로 인해 온프레미스와 클라우드 네트워킹 관행 간에 상당한 차이가 있기 때문에 문제가 발생할 수 있습니다. 이러한 사고방식 전환이 발생하지 않으면 한 VPC에서 다른 VPC로의 AWS Site-to-Site VPN 연결과 같은 일이 발생할 수 있습니다. 이 접근 방식은 관리를 AWS 클라우드간소화하고 성능을 개선하는에서 특별히 구축된 네트워킹 서비스를 활용하지 못합니다. 클라우드 네이티브 설계에 적응하면 운영 오버헤드를 줄이고 VPCs.

SaaS 공급자로서이 연결 옵션을 제공할 생각이라면 자신 또는 소비자에게를 사용해야 AWS Site-to-Site VPN 하는 이유를 물어보십시오. 그런 다음 이러한 요구 사항에서 거꾸로 작업하여 더 나은 연결 옵션을 찾습니다. 이 가이드의 서비스 기능 비교 섹션에는 옵션을 식별하는 데 사용할 수 있는 매트릭스가 포함되어 있습니다. 그런 다음이 가이드의 관련 섹션을 살펴보고 사용 사례를 해결하는 아키텍처 접근 방식을 찾을 수 있습니다.

다음 단계

이 가이드에서는 다양한 시나리오에서 다양한 네트워크 액세스 접근 방식을 설명했으며 각 아키텍처의 이점과 단점을 설명합니다. 네트워크 액세스 접근 방식을 선택하는 것이 순전히 기술적인 논의가 되어서는 안 되는 이유를 이해해야 합니다. 비즈니스와 기술 간의 조정은 필수적입니다. 다음 단계 및 권장 사항은 현재 기능을 평가하고, 시장 요구 사항을 분석하고, 거버넌스 제어를 구현하여 네트워크 아키텍처 전략을 평가하고 표준화하는 데 도움이 될 수 있습니다.

이 섹션은 다음 주제를 포함합니다:

- 현재 아키텍처 및 기능 평가
- 시장 및 고객 분석
- 전략적 정렬
- 표준화
- 거버넌스
- 반복

현재 아키텍처 및 기능 평가

이 가이드의 자체 평가 프레임워크, 현재 규제 요구 사항 및 현재 시장 상태(고객 및 경쟁 분석 모두)와 같은 관련 데이터 소스와 비교하여 현재 네트워크 아키텍처를 검토합니다. 예를 들어,에서 대규모로 프로덕션 시스템을 실행한 수십 년의 경험을 기반으로 하는 AWS Well-Architected 프레임워크를 사용하는 것이 좋습니다 AWS 클라우드.

잠재적 예외, 일회성 및 과거 제품 결정을 검토합니다. 궁금해하고, 문제를 제기하고, 자동으로 유효성을 가정하지 마세요. 몇 년 전의 고객 요구 사항은 더 이상 유효하지 않을 수 있습니다. 어려운 가정은 아키텍처의 복잡성을 단순화하고 줄일 수 있는 기회를 제공합니다.

간단히 말해서 조직의 다양한 역할이 액세스하고 이해할 수 있도록 관찰 내용을 문서화합니다. 현재 상태가 대상 상태와 다른 위치, 대상 상태, 영향 및 관찰 시점을 캡처합니다. 이 정보를 기록하면 조직이 새로운 데이터를 기반으로 결정을 내리는 데 도움이 됩니다.

시장 및 고객 분석

시장 추세에 대한 인사이트를 수집합니다. 소비자가 현재 선호하는 SaaS 제품 액세스 방법은 무엇인가요? 고객이 있는 곳을 여전히 만나고 있나요? 고객 집단 또는 행동이 변경되었나요? 경영진이 우주

선을 새로운 시장, 특정 규제 요구 사항이 있는 지역 또는 새로운 고객 계층으로 유도했나요? 비즈니스 또는 운영 모델이 변경되었습니까? 예를 들어 서비스에 화이트 레이블을 지정하는 것을 고려하고 있습니까? 성장 계획에는 고객이 해당 파트너와 연결할 때 서비스를 사용할 수 있도록 파트너와 협력하는 것이 포함되나요?

전략적 정렬

현재 역량, 현재 아키텍처, 시장 및 고객을 이해하면 전략적 조정 회의를 호출합니다. 관련 제품, 비즈니스 및 기술 이해관계자를 통해 여전히 유효한 요구 사항과 고려해야 할 새로운 요구 사항에 도전합니다. 더 이상 필요하지 않은 요구 사항을 삭제하여 복잡성을 줄일 수 있는 기회를 찾습니다. 이는 위원회에서 설계한 것이 아니므로 엔지니어링 팀은 실제 아키텍처 및 구현 세부 정보를 준비하고 소유해야 합니다. 그러나이 회의에서는 이것이 고객과 조직의 이점을 극대화하는 일련의 요구 사항인 이유를 명확히 해야 합니다.

표준화

고객을 유치하기 위해 각 고객이 서비스에 연결하는 방법을 자유롭게 선택하도록 하고 싶을 수 있습니다. 결국 모든 솔루션이 기술적으로 작동할 수 있으며 모든 솔루션을 관리하고 운영할 수 있는 지식과 리소스가 있을 수도 있습니다. 이는 특정 시점까지 잘 작동할 수 있지만 비즈니스가 확장됨에 따라 관리하기가 어려워집니다. 관찰성 스택은 여러 솔루션의 지표를 지원해야 하며 사이트 신뢰성 엔지니어도 이를 이해할 수 있어야 합니다. 각 연결 접근 방식에 대한 up-to-date 설명서가 필요합니다. 애플리케이션의 주요 변경 사항은 제공하는 각 액세스 접근 방식을 기준으로 평가해야 합니다. 각 액세스 접근 방식에 대해 자동화 및 코드형 인프라(IaC)를 작성하고 유지 관리해야 합니다. 서비스에 대한 액세스를 표준화하지 않는 추가 오버헤드는 고객에게 제공하려는 유연성과 비교해야 합니다.

의사 결정을 안내하는 북극 별이 필요한 경우 표준화를 권장합니다. 고객이 제공하는 서비스와 상호 작용하는 방식을 표준화하는 것은 일반적으로 조직 전체에서 많은 성공 지표를 개선하기 위해 취할 수 있는 가장 영향력 있는 조치입니다. 표준화를 통해 제품 팀은 서비스의 비용 구조를 더 쉽게 이해하고 데이터 기반 제품 결정을 내릴 수 있습니다. 운영 팀이 사전 정의된 표준에 따라 개발, 출시 및 운영되는 환경에서 문제를 해결하고 문제 해결 프로세스의 일부를 자동화하는 것이 더 쉽습니다. 이는 악의적인 행위자의 이상, 예상치 못한 동작 또는 행동을 탐지하는 데 도움이 될 수 있습니다. 또한 표준화는 기술적 부채를 줄입니다. 엔지니어링 팀이 프로덕션에 대한 변경 사항을 테스트하고 롤아웃하는 데 걸리는 주기가 줄어듭니다. 또한 시장 출시 속도를 높이고, 셀프 서비스 온보딩 성공을 개선하고, 규제 위험을 줄일 수 있습니다.

따라서 오늘 있을 수 있는 단점도 검토하는 것이 좋습니다. 기존 고객을 지원하는 데 소비하는 운영 주기 수를 정량화합니다. 결과를 과거 데이터와 비교하고 현재 접근 방식이 향후 몇 년 동안 확장되는지

평가합니다. 표준에서 전환해야 할 때마다 해당 요청의 요구 사항에 이의를 제기합니다. 영향을 평가하고 즉각적인 이점과 장기 약정의 균형을 맞춥니다.

사용자 지정이 불가피하지만 표준과 충돌하는 경우 공동 책임 모델을 고려하세요. 이 모델에서 제품은 요청된 변경 사항으로부터 대부분 보호되며 사용자 지정은 미니멀한 전용 환경에서 이루어집니다. 예제는 전송 VPC 아키텍처에 연결 섹션을 참조하세요.

거버넌스

규제 요구 사항과 자체 내부 표준을 준수하려면 거버넌스가 필수적입니다. 적절한 거버넌스를 마련하면 표준을 적용할 위치와 방법을 제어할 수 있습니다. 또한 표준과의 차이를 감지하고 필요한 수정 조치에 대해 리소스 소유자에게 알리기 위한 제어를 설정합니다. AWS Organizations, AWS CloudTrail, 및 AWS ConfigAWS Control Tower는에서 워크로드를 관리하고 관리하는 데 도움이 될 수 AWS 서비스 있는 몇 가지 방법입니다 AWS 클라우드.

반복

초기 작업에서 학습한 내용을 사용하여 나중에 일관성을 유지할 수 있도록 가볍고 반복 가능한 프로세스를 설정합니다. 입력이 필요한 역할, 빈도, 데이터 정확성, 데이터 공유 방법, 작업 대상을 정의합니다.

리소스

AWS 설명서

- 에 타사 서비스 통합 AWS 클라우드(AWS 권장 가이드)
- 멀티테넌트 SaaS 권한 부여 및 API 액세스 제어(AWS 권장 가이드)
- 단일 컨트롤 플레인에서 여러 SaaS 제품의 테넌트 관리(AWS 권고 가이드)
- 란 무엇입니까 AWS Direct Connect?(Direct Connect 문서)
- AWS PrivateLink란 무엇인가요? (Amazon VPC 설명서)
- 란 무엇입니까 AWS Site-to-Site VPN? (AWS Site-to-Site VPN 문서)
- 란 무엇입니까 AWS Transit Gateway? (Amazon VPC 설명서)
- VPC 피어링이란 무엇입니까? (Amazon VPC 설명서)

기타 AWS 리소스

- Amazon Virtual Private Cloud 연결 옵션(AWS 백서)
- AWS re:Invent 2021 - AWS 워크로드에 적합한 로드 밸런서를 선택하는 방법(YouTube)
- SaaS란 무엇입니까?(AWS 웹 사이트)
- AWS SaaS Factory 프로그램(AWS Partner 프로그램)
- 의 다중 테넌트 아키텍처 지침 AWS(AWS 솔루션 라이브러리)

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2025년 9월 12일

AWS 권장 가이드 용어집

다음은 AWS 권장 가이드에서 제공하는 전략, 가이드 및 패턴에서 일반적으로 사용되는 용어입니다. 용어집 항목을 제안하려면 용어집 끝에 있는 피드백 제공 링크를 사용하십시오.

숫자

7가지 전략

애플리케이션을 클라우드로 이전하기 위한 7가지 일반적인 마이그레이션 전략 이러한 전략은 Gartner가 2011년에 파악한 5가지 전략을 기반으로 하며 다음으로 구성됩니다.

- 리팩터링/리아키텍트 - 클라우드 네이티브 기능을 최대한 활용하여 애플리케이션을 이동하고 해당 아키텍처를 수정함으로써 민첩성, 성능 및 확장성을 개선합니다. 여기에는 일반적으로 운영 체제와 데이터베이스 이식이 포함됩니다. 예: 온프레미스 Oracle 데이터베이스를 Amazon Aurora PostgreSQL 호환 에디션으로 마이그레이션합니다.
- 리플랫포밍(리프트 앤드 리셰이프) - 애플리케이션을 클라우드로 이동하고 일정 수준의 최적화를 도입하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드의 Amazon Relational Database Service(Amazon RDS) for Oracle로 마이그레이션합니다.
- 재구매(드롭 앤드 숍) - 일반적으로 기존 라이선스에서 SaaS 모델로 전환하여 다른 제품으로 전환합니다. 예: 고객 관계 관리(CRM) 시스템을 Salesforce.com으로 마이그레이션합니다.
- 리호스팅(리프트 앤드 시프트) - 애플리케이션을 변경하지 않고 클라우드로 이동하여 클라우드 기능을 활용합니다. 예: 온프레미스 Oracle 데이터베이스를 AWS 클라우드클라우드의 EC2 인스턴스에 있는 Oracle로 마이그레이션합니다.
- 재배치(하이퍼바이저 수준의 리프트 앤 시프트) - 새 하드웨어를 구매하거나, 애플리케이션을 다시 작성하거나, 기존 운영을 수정하지 않고도 인프라를 클라우드로 이동합니다. 온프레미스 플랫폼에서 동일한 플랫폼의 클라우드 서비스로 서버를 마이그레이션합니다. 예: Microsoft Hyper-V 애플리케이션을 로 마이그레이션합니다 AWS.
- 유지(보관) - 소스 환경에 애플리케이션을 유지합니다. 대규모 리팩터링이 필요하고 해당 작업을 나중으로 연기하려는 애플리케이션과 비즈니스 차원에서 마이그레이션할 이유가 없어 유지하려는 레거시 애플리케이션이 여기에 포함될 수 있습니다.
- 사용 중지 - 소스 환경에서 더 이상 필요하지 않은 애플리케이션을 폐기하거나 제거합니다.

A

A2A(Agent-to-Agent)

작업 위임 및 상태 전송agent-to-agent 공동 작업을 위한 상태 저장 프로토콜입니다.

ABAC

속성 기반 액세스 제어를 참조하세요.

추상화된 서비스

관리형 서비스를 참조하세요.

ACID

원자성, 일관성, 격리성, 내구성을 참조하세요.

능동-능동 마이그레이션

양방향 복제 도구 또는 이중 쓰기 작업을 사용하여 소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되고, 두 데이터베이스 모두 마이그레이션 중 연결 애플리케이션의 트랜잭션을 처리하는 데이터베이스 마이그레이션 방법입니다. 이 방법은 일회성 전환이 필요한 대신 소규모의 제어된 배치로 마이그레이션을 지원합니다. 더 유연하지만 액티브 패시브 마이그레이션보다 더 많은 작업이 필요합니다.

능동-수동 마이그레이션

소스 데이터베이스와 대상 데이터베이스가 동기화된 상태로 유지되지만 소스 데이터베이스만 연결 애플리케이션의 트랜잭션을 처리하고 데이터는 대상 데이터베이스로 복제되는 데이터베이스 마이그레이션 방법입니다. 대상 데이터베이스는 마이그레이션 중 어떤 트랜잭션도 허용하지 않습니다.

에이전트

목표를 달성하기 위한 도구를 사용하여 자율적으로 추론, 계획 및 조치를 취할 수 있는 AI 시스템입니다.

에이전트 운영

대규모 프로덕션 환경에서 AI 에이전트를 구축, 테스트, 배포 및 실행하기 위한 운영 사례입니다.

집계 함수

행 그룹에서 작동하고 그룹에 대한 단일 반환 값을 계산하는 SQL 함수입니다. 집계 함수의 예로 `SUM` 및 `MAX`가 있습니다.

AI

인공 지능을 참조하세요.

AIOps

인공 지능 운영을 참조하세요.

익명화

데이터세트에서 개인 정보를 영구적으로 삭제하는 프로세스입니다. 익명화는 개인 정보 보호에 도움이 될 수 있습니다. 익명화된 데이터는 더 이상 개인 데이터로 간주되지 않습니다.

안티 패턴

솔루션이 다른 솔루션보다 비생산적이거나 비효율적이거나 덜 효과적이어서 반복되는 문제에 자주 사용되는 솔루션입니다.

애플리케이션 제어

맬웨어로부터 시스템을 보호하기 위해 승인된 애플리케이션만 사용하도록 허용하는 보안 접근 방식입니다.

애플리케이션 포트폴리오

애플리케이션 구축 및 유지 관리 비용과 애플리케이션의 비즈니스 가치를 비롯하여 조직에서 사용하는 각 애플리케이션에 대한 세부 정보 모음입니다. 이 정보는 포트폴리오 탐색 및 분석 프로세스의 핵심이며 마이그레이션, 현대화 및 최적화할 애플리케이션을 식별하고 우선순위를 정하는 데 도움이 됩니다.

인공 지능

컴퓨터 기술을 사용하여 학습, 문제 해결, 패턴 인식 등 일반적으로 인간과 관련된 인지 기능을 수행하는 것을 전문으로 하는 컴퓨터 과학 분야입니다. 자세한 내용은 What is Artificial Intelligence?를 참조하십시오.

인공 지능 운영(AIOps)

기계 학습 기법을 사용하여 운영 문제를 해결하고, 운영 인시던트 및 사용자 개입을 줄이고, 서비스 품질을 높이는 프로세스입니다. AWS 마이그레이션 전략에서 AIOps가 사용되는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

비대칭 암호화

한 쌍의 키, 즉 암호화를 위한 퍼블릭 키와 복호화를 위한 프라이빗 키를 사용하는 암호화 알고리즘입니다. 퍼블릭 키는 복호화에 사용되지 않으므로 공유할 수 있지만 프라이빗 키에 대한 액세스는 엄격히 제한되어야 합니다.

원자성, 일관성, 격리성, 내구성(ACID)

오류, 정전 또는 기타 문제가 발생한 경우에도 데이터베이스의 데이터 유효성과 운영 신뢰성을 보장하는 소프트웨어 속성 세트입니다.

ABAC(속성 기반 액세스 제어)

부서, 직무, 팀 이름 등의 사용자 속성을 기반으로 세분화된 권한을 생성하는 방식입니다. 자세한 내용은 AWS Identity and Access Management (IAM) 설명서의 용 ABAC AWS를 참조하세요.

신뢰할 수 있는 데이터 소스

가장 신뢰할 수 있는 정보 소스로 간주되는 기본 버전의 데이터를 저장하는 위치입니다. 익명화, 편집 또는 가명화와 같은 데이터 처리 또는 수정의 목적으로 신뢰할 수 있는 데이터 소스의 데이터를 다른 위치로 복사할 수 있습니다.

가용 영역

다른 가용 영역의 장애로부터 격리 AWS 리전 되고 동일한 리전의 다른 가용 영역에 저렴하고 지연 시간이 짧은 네트워크 연결을 제공하는 내의 고유한 위치입니다.

AWS 클라우드 채택 프레임워크(AWS CAF)

조직이 클라우드로 성공적으로 전환하기 위한 효율적이고 효과적인 계획을 개발하는 AWS 데 도움이 되는의 지침 및 모범 사례 프레임워크입니다. AWS CAF는 지침을 비즈니스, 사람, 거버넌스, 플랫폼, 보안 및 운영이라는 6가지 중점 영역으로 구성합니다. 비즈니스, 사람 및 거버넌스 관점은 비즈니스 기술과 프로세스에 초점을 맞추고, 플랫폼, 보안 및 운영 관점은 전문 기술과 프로세스에 중점을 둡니다. 예를 들어, 사람 관점은 인사(HR), 직원 배치 기능 및 인력 관리를 담당하는 이해관계자를 대상으로 합니다. 이러한 관점에서 AWS CAF는 성공적인 클라우드 채택을 위해 조직을 준비하는 데 도움이 되는 인력 개발, 교육 및 커뮤니케이션에 대한 지침을 제공합니다. 자세한 내용은 AWS CAF 웹사이트와 AWS CAF 백서를 참조하세요.

AWS 워크로드 검증 프레임워크(AWS WQF)

데이터베이스 마이그레이션 워크로드를 평가하고, 마이그레이션 전략을 권장하고, 작업 견적을 제공하는 도구입니다. AWS WQF는 AWS Schema Conversion Tool (AWS SCT)에 포함되어 있습니다. 데이터베이스 스키마 및 코드 객체, 애플리케이션 코드, 종속성 및 성능 특성을 분석하고 평가 보고서를 제공합니다.

B

악성 봇

개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

BCP

비즈니스 연속성 계획을 참조하세요.

동작 그래프

리소스 동작과 시간 경과에 따른 상호 작용에 대한 통합된 대화형 뷰입니다. Amazon Detective에서 동작 그래프를 사용하여 실패한 로그온 시도, 의심스러운 API 직접 호출 및 유사한 작업을 검사할 수 있습니다. 자세한 내용은 Detective 설명서의 Data in a behavior graph를 참조하십시오.

빅 엔디안 시스템

가장 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

바이너리 분류

바이너리 결과(가능한 두 클래스 중 하나)를 예측하는 프로세스입니다. 예를 들어, ML 모델이 “이 이메일이 스팸인가요, 스팸이 아닌가요?”, '이 제품은 책인가요, 자동차인가요?' 등의 문제를 예측해야 할 수 있습니다.

블룸 필터

요소가 세트의 멤버인지 여부를 테스트하는 데 사용되는 메모리 효율성이 높은 확률론적 데이터 구조입니다.

블루/그린(Blue/Green) 배포

동일하지만 별개의 두 환경을 생성하는 배포 전략입니다. 하나의 환경(파란색)에서 현재 애플리케이션 버전을 실행하고 새 애플리케이션 버전은 다른 환경(녹색)에서 실행합니다. 이 전략을 사용하면 영향을 최소화하면서 신속하게 롤백할 수 있습니다.

bot

인터넷을 통해 자동화된 태스크를 실행하고 인적 활동이나 상호 작용을 시뮬레이션하는 소프트웨어 애플리케이션입니다. 인터넷에서 정보를 인덱싱하는 웹 크롤러와 같이 유용하거나 이로운 봇도 있습니다. 악성 봇이라고 하는 다른 일부 봇은 개인 또는 조직을 방해하거나 해를 입히기 위한 봇입니다.

봇넷

맬웨어에 감염되고 봇 허더 또는 봇 운영자와 같은 단일 당사자가 제어하는 봇 네트워크입니다. 봇넷은 봇의 규모와 봇의 영향 범위를 확대하는 가장 잘 알려진 메커니즘입니다.

브랜치

코드 리포지토리의 포함된 영역입니다. 리포지토리에 생성되는 첫 번째 브랜치가 기본 브랜치입니다. 기존 브랜치에서 새 브랜치를 생성한 다음 새 브랜치에서 기능을 개발하거나 버그를 수정할 수 있습니다. 기능을 구축하기 위해 생성하는 브랜치를 일반적으로 기능 브랜치라고 합니다. 기능을 출시할 준비가 되면 기능 브랜치를 기본 브랜치에 다시 병합합니다. 자세한 내용은 About branches(GitHub 설명서)를 참조하십시오.

긴급 액세스 권한

예외적인 상황에서 승인된 프로세스를 통해 사용자가 일반적으로 액세스할 권한이 없는에 액세스할 수 AWS 계정 있는 빠른 방법입니다. 자세한 내용은 AWS Well-Architected 지침의 Implement break-glass procedures 지표를 참조하세요.

브라운필드 전략

사용자 환경의 기존 인프라 시스템 아키텍처에 브라운필드 전략을 채택할 때는 현재 시스템 및 인프라의 제약 조건을 중심으로 아키텍처를 설계합니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

버퍼 캐시

가장 자주 액세스하는 데이터가 저장되는 메모리 영역입니다.

사업 역량

기업이 가치를 창출하기 위해 하는 일(예: 영업, 고객 서비스 또는 마케팅)입니다. 마이크로서비스 아키텍처 및 개발 결정은 비즈니스 역량에 따라 이루어질 수 있습니다. 자세한 내용은 백서의 AWS에서 컨테이너화된 마이크로서비스 실행의 비즈니스 역량 중심의 구성화 섹션을 참조하십시오.

비즈니스 연속성 계획(BCP)

대규모 마이그레이션과 같은 중단 이벤트가 운영에 미치는 잠재적 영향을 해결하고 비즈니스가 신속하게 운영을 재개할 수 있도록 지원하는 계획입니다.

C

CAF

AWS Cloud Adoption Framework를 참조하세요.

카나리 배포

최종 사용자에게 제공하는 느린 증분 릴리스 버전입니다. 확신이 들면 새 버전을 배포하고 현재 버전을 완전히 교체합니다.

CCoE

클라우드 혁신 센터를 참조하세요.

CDC

데이터 캡처 변경을 참조하세요.

변경 데이터 캡처(CDC)

데이터베이스 테이블과 같은 데이터 소스의 변경 내용을 추적하고 변경 사항에 대한 메타데이터를 기록하는 프로세스입니다. 대상 시스템의 변경 내용을 감사하거나 복제하여 동기화를 유지하는 등의 다양한 용도로 CDC를 사용할 수 있습니다.

카오스 엔지니어링

시스템의 복원력을 테스트하기 위해 의도적으로 장애나 중단 이벤트를 도입합니다. AWS Fault Injection Service (AWS FIS)를 사용하여 AWS 워크로드에 스트레스를 주고 응답을 평가하는 실험을 수행할 수 있습니다.

CI/CD

지속적 통합 및 지속적 전송을 참조하세요.

분류

예측을 생성하는 데 도움이 되는 분류 프로세스입니다. 분류 문제에 대한 ML 모델은 이산 값을 예측합니다. 이산 값은 항상 서로 다릅니다. 예를 들어, 모델이 이미지에 자동차가 있는지 여부를 평가해야 할 수 있습니다.

시민 개발자

전문 기술 없이 노코드/로우코드 플랫폼을 사용하여 AI 애플리케이션을 생성하는 비즈니스 사용자입니다.

클라이언트측 암호화

대상이 데이터를 AWS 서비스 수신하기 전에 로컬에서 데이터를 암호화합니다.

클라우드 혁신 센터(CCoE)

클라우드 모범 사례 개발, 리소스 동원, 마이그레이션 타임라인 설정, 대규모 혁신을 통한 조직 선도 등 조직 전체에서 클라우드 채택 노력을 추진하는 다분야 팀입니다. 자세한 내용은 AWS 클라우드 엔터프라이즈 전략 블로그의 CCoE 게시물을 참조하세요.

클라우드 컴퓨팅

원격 데이터 스토리지와 IoT 디바이스 관리에 일반적으로 사용되는 클라우드 기술 클라우드 컴퓨팅은 일반적으로 엣지 컴퓨팅 기술에 연결되어 있습니다.

클라우드 운영 모델

IT 조직에서 하나 이상의 클라우드 환경을 구축, 성숙화 및 최적화하는 데 사용되는 운영 모델입니다. 자세한 내용은 클라우드 운영 모델 구축을 참조하십시오.

클라우드 채택 단계

조직이 AWS 클라우드로 마이그레이션할 때 일반적으로 거치는 4단계는 다음과 같습니다.

- 프로젝트 - 개념 증명 및 학습 목적으로 몇 가지 클라우드 관련 프로젝트 실행
- 기반 – 클라우드 채택 확장을 위한 기초 투자(예: 랜딩 존 생성, CCoE 정의, 운영 모델 구축)
- 마이그레이션 - 개별 애플리케이션 마이그레이션
- Re-invention - 제품 및 서비스 최적화와 클라우드 혁신

이러한 단계는 Stephen Orban이 블로그 게시물 The Journey Toward Cloud-First and the Stages of Adoption on the AWS 클라우드 Enterprise Strategy 블로그에서 정의했습니다. AWS 마이그레이션 전략과 어떤 관련이 있는지에 대한 자세한 내용은 마이그레이션 준비 가이드를 참조하세요.

CMDB

구성 관리 데이터베이스를 참조하세요.

코드 리포지토리

소스 코드와 설명서, 샘플, 스크립트 등의 기타 자산이 버전 관리 프로세스를 통해 저장되고 업데이트되는 위치입니다. 일반적인 클라우드 리포지토리로 GitHub 또는 Bitbucket Cloud가 포함됩니다. 코드의 각 버전을 브랜치라고 합니다. 마이크로서비스 구조에서 각 리포지토리는 단일 기능 전용입니다. 단일 CI/CD 파이프라인은 여러 리포지토리를 사용할 수 있습니다.

콜드 캐시

비어 있거나, 제대로 채워지지 않았거나, 오래되었거나 관련 없는 데이터를 포함하는 버퍼 캐시입니다. 주 메모리나 디스크에서 데이터베이스 인스턴스를 읽어야 하기 때문에 성능에 영향을 미치며, 이는 버퍼 캐시에서 읽는 것보다 느립니다.

콜드 데이터

거의 액세스되지 않고 일반적으로 과거 데이터인 데이터. 이런 종류의 데이터를 쿼리할 때는 일반적으로 느린 쿼리가 허용됩니다. 이 데이터를 성능이 낮고 비용이 저렴한 스토리지 계층 또는 클래스로 옮기면 비용을 절감할 수 있습니다.

컴퓨터 비전(CV)

기계 학습을 사용하여 디지털 이미지 및 비디오와 같은 시각적 형식에서 정보를 분석하고 추출하는 AI 필드입니다. 예를 들어 Amazon SageMaker AI는 CV에 대한 이미지 처리 알고리즘을 제공합니다.

구성 드리프트

워크로드의 경우 구성이 예상되는 상태에서 변경됩니다. 이로 인해 워크로드가 규정을 준수하지 않을 수 있으며, 이는 일반적으로 점진적이고 의도되지 않은 작업입니다.

구성 관리 데이터베이스(CMDB)

하드웨어 및 소프트웨어 구성 요소와 해당 구성을 포함하여 데이터베이스와 해당 IT 환경에 대한 정보를 저장하고 관리하는 리포지토리입니다. 일반적으로 마이그레이션의 포트폴리오 탐색 및 분석 단계에서 CMDB의 데이터를 사용합니다.

규정 준수 팩

규정 준수 및 보안 검사를 사용자 지정하기 위해 조합할 수 있는 AWS Config 규칙 및 문제 해결 작업의 모음입니다. YAML 템플릿을 사용하여 적합성 팩을 AWS 계정 및 리전 또는 조직 전체에 단일 엔터티로 배포할 수 있습니다. 자세한 내용은 AWS Config 설명서의 적합성 팩을 참조하세요.

지속적 통합 및 지속적 전달(CI/CD)

소프트웨어 릴리스 프로세스의 소스, 빌드, 테스트, 스테이징 및 프로덕션 단계를 자동화하는 프로세스입니다. CI/CD는 일반적으로 파이프라인으로 설명됩니다. CI/CD를 통해 프로세스를 자동화하고, 생산성을 높이고, 코드 품질을 개선하고, 더 빠르게 제공할 수 있습니다. 자세한 내용은 지속적 전달의 이점을 참조하십시오. CD는 지속적 배포를 의미하기도 합니다. 자세한 내용은 지속적 전달(Continuous Delivery)과 지속적인 개발을 참조하십시오.

CV

컴퓨터 비전을 참조하세요.

D

저장 데이터

스토리지에 있는 데이터와 같이 네트워크에 고정되어 있는 데이터입니다.

데이터 분류

중요도와 민감도를 기준으로 네트워크의 데이터를 식별하고 분류하는 프로세스입니다. 이 프로세스는 데이터에 대한 적절한 보호 및 보존 제어를 결정하는 데 도움이 되므로 사이버 보안 위험 관리 전략의 중요한 구성 요소입니다. 데이터 분류는 AWS Well-Architected Framework의 보안 원칙 구성 요소입니다. 자세한 내용은 데이터 분류를 참조하십시오.

데이터 드리프트

프로덕션 데이터와 ML 모델 학습에 사용된 데이터 간의 상당한 차이 또는 시간 경과에 따른 입력 데이터의 의미 있는 변화. 데이터 드리프트는 ML 모델 예측의 전반적인 품질, 정확성 및 공정성을 저하시킬 수 있습니다.

전송 중 데이터

네트워크를 통과하고 있는 데이터입니다. 네트워크 리소스 사이를 이동 중인 데이터를 예로 들 수 있습니다.

데이터 메시

중앙 집중식 관리 및 거버넌스를 통해 분산되고 탈중앙화된 데이터 소유권을 제공하는 아키텍처 프레임워크입니다.

데이터 최소화

꼭 필요한 데이터만 수집하고 처리하는 원칙입니다. 에서 데이터를 최소화하면 개인 정보 보호 위험, 비용 및 분석 탄소 발자국을 줄일 AWS 클라우드 수 있습니다.

데이터 경계

신뢰할 수 있는 자격 증명만 예상 네트워크에서 신뢰할 수 있는 리소스에 액세스하도록 하는 데 도움이 되는 AWS 환경의 예방 가드레일 세트입니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

데이터 사전 처리

원시 데이터를 ML 모델이 쉽게 구문 분석할 수 있는 형식으로 변환하는 것입니다. 데이터를 사전 처리한다는 것은 특정 열이나 행을 제거하고 누락된 값, 일관성이 없는 값 또는 중복 값을 처리함을 의미할 수 있습니다.

데이터 출처

라이프사이클 전반에 걸쳐 데이터의 출처와 기록을 추적하는 프로세스(예: 데이터 생성, 전송, 저장 방법).

데이터 주체

데이터를 수집 및 처리하는 개인입니다.

데이터 웨어하우스

분석과 같은 비즈니스 인텔리전스를 지원하는 데이터 관리 시스템입니다. 데이터 웨어하우스에는 보통 많은 양의 기록 데이터가 포함되며 일반적으로 쿼리 및 분석에 사용됩니다.

데이터 정의 언어(DDL)

데이터베이스에서 테이블 및 객체의 구조를 만들거나 수정하기 위한 명령문 또는 명령입니다.

데이터베이스 조작 언어(DML)

데이터베이스에서 정보를 수정(삽입, 업데이트 및 삭제)하기 위한 명령문 또는 명령입니다.

DDL

데이터 정의 언어를 참조하세요.

딥 앙상블

예측을 위해 여러 딥 러닝 모델을 결합하는 것입니다. 딥 앙상블을 사용하여 더 정확한 예측을 얻거나 예측의 불확실성을 추정할 수 있습니다.

딥 러닝

여러 계층의 인공 신경망을 사용하여 입력 데이터와 관심 대상 변수 간의 매핑을 식별하는 ML 하위 분야입니다.

심층 방어

네트워크와 그 안의 데이터 기밀성, 무결성 및 가용성을 보호하기 위해 컴퓨터 네트워크 전체에 일련의 보안 메커니즘과 제어를 신중하게 계층화하는 정보 보안 접근 방식입니다. 이 전략을 채택하면 AWS Organizations 구조의 여러 계층에 여러 컨트롤을 AWS추가하여 리소스를 보호할 수 있습니다. 예를 들어, 심층 방어 접근 방식은 다단계 인증, 네트워크 세분화 및 암호화를 결합할 수 있습니다.

위임된 관리자

에서 AWS Organizations호환되는 서비스는 AWS 멤버 계정을 등록하여 조직의 계정을 관리하고 해당 서비스에 대한 권한을 관리할 수 있습니다. 이러한 계정을 해당 서비스의 위임된 관리자라고

합니다. 자세한 내용과 호환되는 서비스 목록은 AWS Organizations 설명서의 AWS Organizations와 함께 사용할 수 있는 AWS 서비스를 참조하십시오.

배포

대상 환경에서 애플리케이션, 새 기능 또는 코드 수정 사항을 사용할 수 있도록 하는 프로세스입니다. 배포에는 코드 베이스의 변경 사항을 구현한 다음 애플리케이션 환경에서 해당 코드베이스를 구축하고 실행하는 작업이 포함됩니다.

개발 환경

환경을 참조하세요.

탐지 제어

이벤트 발생 후 탐지, 기록 및 알림을 수행하도록 설계된 보안 제어입니다. 이러한 제어는 기존의 예방적 제어를 우회한 보안 이벤트를 알리는 2차 방어선입니다. 자세한 내용은 AWS에서 보안 제어 구현의 탐지 제어를 참조하세요.

개발 가치 흐름 매핑 (DVSM)

소프트웨어 개발 라이프사이클에서 속도와 품질에 부정적인 영향을 미치는 제약 조건을 식별하고 우선 순위를 지정하는 데 사용되는 프로세스입니다. DVSM은 원래 린 제조 방식을 위해 설계된 가치 흐름 매핑 프로세스를 확장합니다. 소프트웨어 개발 프로세스를 통해 가치를 창출하고 이동하는 데 필요한 단계와 팀에 중점을 둡니다.

디지털 트윈

건물, 공장, 산업 장비 또는 생산 라인과 같은 실제 시스템을 가상으로 표현한 것입니다. 디지털 트윈은 예측 유지 보수, 원격 모니터링, 생산 최적화를 지원합니다.

차원 테이블

스타 스키마에서 팩트 테이블의 정량적 데이터에 대한 데이터 속성을 포함하는 더 작은 테이블을 말합니다. 차원 테이블 속성은 일반적으로 텍스트 필드나 텍스트처럼 동작하는 개별 숫자입니다. 이러한 속성은 보통 쿼리 제약, 필터링 및 결과 세트 레이블 지정에 사용됩니다.

재해

워크로드 또는 시스템이 기본 배포 위치에서 비즈니스 목표를 달성하지 못하게 방해하는 이벤트입니다. 이러한 이벤트는 자연재해, 기술적 오류, 의도하지 않은 구성 오류 또는 멀웨어 공격과 같은 사람의 행동으로 인한 결과일 수 있습니다.

재해 복구(DR)

재해로 인한 가동 중지 시간 및 데이터 손실을 최소화하기 위해 사용하는 전략 및 프로세스입니다. 자세한 내용은 AWS Well-Architected Framework의 Disaster Recovery of Workloads on AWS: Recovery in the Cloud를 참조하세요.

DML

데이터베이스 조작 언어를 참조하세요.

도메인 기반 설계

구성 요소를 각 구성 요소가 제공하는 진화하는 도메인 또는 핵심 비즈니스 목표에 연결하여 복잡한 소프트웨어 시스템을 개발하는 접근 방식입니다. 이 개념은 에릭 에반스에 의해 그의 저서인 도메인 기반 디자인: 소프트웨어 중심의 복잡성 해결(Boston: Addison-Wesley Professional, 2003)에서 소개되었습니다. Strangler Fig 패턴과 함께 도메인 기반 설계를 사용하는 방법에 대한 자세한 내용은 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

DR

재해 복구를 참조하세요.

드리프트 감지

기준이 되는 구성과의 편차 추적을 말합니다. 예를 들어 AWS CloudFormation 를 사용하여 시스템 리소스의 드리프트를 감지하거나를 사용하여 AWS Control Tower 거버넌스 요구 사항 준수에 영향을 미칠 수 있는 랜딩 존의 변경 사항을 감지할 수 있습니다.

DVSM

개발 가치 흐름 매핑을 참조하세요.

E

EDA

탐색 데이터 분석을 참조하세요.

EDI

전자 데이터 교환을 참조하세요.

엣지 컴퓨팅

IoT 네트워크의 엣지에서 스마트 디바이스의 컴퓨팅 성능을 개선하는 기술 엣지 컴퓨팅은 클라우드 컴퓨팅에 비해 보다 통신 지연 시간을 줄이고 응답 시간을 개선할 수 있습니다.

전자 데이터 교환(EDI)

조직 간 비즈니스 문서의 자동화된 교환을 나타냅니다. 자세한 내용은 전자 데이터 교환(EDI)이란 무엇인가요?를 참조하세요.

암호화

사람이 읽을 수 있는 일반 텍스트 데이터를 사이퍼텍스트로 변환하는 컴퓨팅 프로세스입니다.

암호화 키

암호화 알고리즘에 의해 생성되는 무작위 비트의 암호화 문자열입니다. 키의 길이는 다양할 수 있으며 각 키는 예측할 수 없고 고유하게 설계되었습니다.

엔디안

컴퓨터 메모리에 바이트가 저장되는 순서입니다. 빅 엔디안 시스템은 가장 중요한 바이트를 먼저 저장합니다. 리틀 엔디안 시스템은 가장 덜 중요한 바이트를 먼저 저장합니다.

엔드포인트

서비스 엔드포인트를 참조하세요.

엔드포인트 서비스

Virtual Private Cloud(VPC)에서 호스팅하여 다른 사용자와 공유할 수 있는 서비스입니다. 를 사용하여 엔드포인트 서비스를 생성하고 다른 AWS 계정 또는 AWS Identity and Access Management (IAM) 보안 주체에 권한을 AWS PrivateLink 부여할 수 있습니다. 이러한 계정 또는 보안 주체는 인터페이스 VPC 엔드포인트를 생성하여 엔드포인트 서비스에 비공개로 연결할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 설명서의 엔드포인트 서비스 생성을 참조하십시오.

엔터프라이즈 리소스 계획(ERP)

엔터프라이즈의 주요 비즈니스 프로세스(예: 회계, MES, 프로젝트 관리)를 자동화하고 관리하는 시스템입니다.

봉투 암호화

암호화 키를 다른 암호화 키로 암호화하는 프로세스입니다. 자세한 내용은 AWS Key Management Service (AWS KMS) 설명서의 봉투 암호화를 참조하세요.

환경

실행 중인 애플리케이션의 인스턴스입니다. 다음은 클라우드 컴퓨팅의 일반적인 환경 유형입니다.

- 개발 환경 - 애플리케이션 유지 관리를 담당하는 핵심 팀만 사용할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. 개발 환경은 변경 사항을 상위 환경으로 승격하기 전에 테스트하는 데 사용됩니다. 이러한 유형의 환경을 테스트 환경이라고도 합니다.
- 하위 환경 - 초기 빌드 및 테스트에 사용되는 환경을 비롯한 애플리케이션의 모든 개발 환경입니다.
- 프로덕션 환경 - 최종 사용자가 액세스할 수 있는 실행 중인 애플리케이션의 인스턴스입니다. CI/CD 파이프라인에서 프로덕션 환경이 마지막 배포 환경입니다.
- 상위 환경 - 핵심 개발 팀 이외의 사용자가 액세스할 수 있는 모든 환경입니다. 프로덕션 환경, 프로덕션 이전 환경 및 사용자 수용 테스트를 위한 환경이 여기에 포함될 수 있습니다.

에픽

애자일 방법론에서 작업을 구성하고 우선순위를 정하는 데 도움이 되는 기능적 범주입니다. 에픽은 요구 사항 및 구현 작업에 대한 개괄적인 설명을 제공합니다. 예를 들어, AWS CAF 보안 에픽에는 ID 및 액세스 관리, 탐지 제어, 인프라 보안, 데이터 보호 및 인시던트 대응이 포함됩니다. AWS 마이그레이션 전략의 에픽에 대한 자세한 내용은 프로그램 구현 가이드를 참조하십시오.

ERP

엔터프라이즈 리소스 계획을 참조하세요.

탐색 데이터 분석(EDA)

데이터 세트를 분석하여 주요 특성을 파악하는 프로세스입니다. 데이터를 수집 또는 집계한 다음 초기 조사를 수행하여 패턴을 찾고, 이상을 탐지하고, 가정을 확인합니다. EDA는 요약 통계를 계산하고 데이터 시각화를 생성하여 수행됩니다.

F

팩트 테이블

스타 스키마의 중앙 테이블입니다. 비즈니스 운영에 대한 정량적 데이터를 저장합니다. 일반적으로 팩트 테이블은 측정값이 있는 열 및 차원 테이블에 대한 외래 키가 있는 열과 같이 두 가지 열 유형을 포함합니다.

빠른 실패

개발 수명 주기를 줄이기 위해 빈번한 증분 테스트를 사용하는 철학입니다. 애자일 접근 방식의 핵심입니다.

장애 격리 경계

에서 장애의 영향을 제한하고 워크로드의 복원력을 개선하는 데 도움이 되는 가용 영역, AWS 리전 컨트롤 플레인 또는 데이터 플레인과 같은 AWS 클라우드경계입니다. 자세한 내용은 AWS 장애 격리 경계를 참조하세요.

기능 브랜치

브랜치를 참조하세요.

기능

예측에 사용하는 입력 데이터입니다. 예를 들어, 제조 환경에서 기능은 제조 라인에서 주기적으로 캡처되는 이미지일 수 있습니다.

기능 중요도

모델의 예측에 특성이 얼마나 중요한지를 나타냅니다. 이는 일반적으로 SHAP(Shapley Additive Descriptions) 및 통합 그레디언트와 같은 다양한 기법을 통해 계산할 수 있는 수치 점수로 표현됩니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

기능 변환

추가 소스로 데이터를 보강하거나, 값을 조정하거나, 단일 데이터 필드에서 여러 정보 세트를 추출하는 등 ML 프로세스를 위해 데이터를 최적화하는 것입니다. 이를 통해 ML 모델이 데이터를 활용할 수 있습니다. 예를 들어, 날짜 '2021-05-27 00:15:37'을 '2021년', '5월', '목', '15일'로 분류하면 학습 알고리즘이 다양한 데이터 구성 요소와 관련된 미묘한 패턴을 학습하는 데 도움이 됩니다.

퓨샷 프롬프팅

유사한 태스크를 수행하도록 요청하기 전에 LLM에 태스크와 원하는 출력을 보여주는 몇 가지 예제를 제공합니다. 이 기법은 모델이 프롬프트에 포함된 예제(샷)에서 학습하는 컨텍스트 내 학습을 적용합니다. 퓨샷 프롬프팅은 특정 형식 지정, 추론 또는 분야별 지식이 필요한 태스크에 효과적일 수 있습니다. 제로샷 프롬프팅도 참조하세요.

FGAC

세분화된 액세스 제어를 참조하세요.

세분화된 액세스 제어(FGAC)

여러 조건을 사용하여 액세스 요청을 허용하거나 거부합니다.

플래시컷 마이그레이션

단계적 접근 방식을 사용하는 대신 변경 데이터 캡처를 통해 지속적 데이터 복제를 사용하여 최단 시간에 데이터를 마이그레이션하는 데이터베이스 마이그레이션 방법입니다. 목표는 가동 중지 시간을 최소화하는 것입니다.

FM

파운데이션 모델을 참조하세요.

파운데이션 모델(FM)

일반화되고 레이블이 지정되지 않은 데이터의 대규모 데이터세트에서 훈련된 대규모 딥 러닝 신경망입니다. FM은 언어 이해, 텍스트 및 이미지 생성, 자연어 대화와 같은 다양한 일반 태스크를 수행할 수 있습니다. 자세한 내용은 파운데이션 모델이란?을 참조하세요.

FM 게이트웨이

파운데이션 모델에 대한 액세스를 제어하고 정규화하는 중앙 집중식 중개자입니다. LLM 게이트웨이라고도 합니다.

G

생성형 AI

대량의 데이터에서 훈련되었으며 간단한 텍스트 프롬프트를 사용하여 이미지, 비디오, 텍스트, 오디오와 같은 새 콘텐츠와 아티팩트를 생성할 수 있는 AI 모델의 하위 세트입니다. 자세한 내용은 생성형 AI란 무엇인가요?를 참조하세요.

지리적 차단

지리적 제한을 참조하세요.

지리적 제한(지리적 차단)

Amazon CloudFront에서 특정 국가의 사용자가 콘텐츠 배포에 액세스하지 못하도록 하는 옵션입니다. 허용 목록 또는 차단 목록을 사용하여 승인된 국가와 차단된 국가를 지정할 수 있습니다. 자세한 내용은 CloudFront 설명서의 콘텐츠의 지리적 배포 제한을 참조하십시오.

Gitflow 워크플로

하위 환경과 상위 환경이 소스 코드 리포지토리의 서로 다른 브랜치를 사용하는 방식입니다. Gitflow 워크플로는 레거시로 간주되며 트렁크 기반 워크플로는 선호되는 현대적 접근 방식입니다.

골든 이미지

시스템 또는 소프트웨어의 새 인스턴스를 배포하기 위한 템플릿으로 사용되는 해당 시스템 또는 소프트웨어의 스냅샷입니다. 예를 들어 제조 분야에서는 골든 이미지를 사용하여 여러 디바이스에서 소프트웨어를 프로비저닝할 수 있으며 이를 통해 딥이스 제조 작업의 속도, 확장성 및 생산성을 개선할 수 있습니다.

브라운필드 전략

새로운 환경에서 기존 인프라의 부재 시스템 아키텍처에 대한 그린필드 전략을 채택할 때 브라운필드라고도 하는 기존 인프라와의 호환성 제한 없이 모든 새로운 기술을 선택할 수 있습니다. 기존 인프라를 확장하는 경우 브라운필드 전략과 그린필드 전략을 혼합할 수 있습니다.

가드레일

조직 단위(OU) 전체에서 리소스, 정책 및 규정 준수를 관리하는 데 도움이 되는 중요 규칙입니다. 예방 가드레일은 규정 준수 표준에 부합하도록 정책을 시행하며, 서비스 제어 정책과 IAM 권한 경계를 사용하여 구현됩니다. 탐지 가드레일은 정책 위반 및 규정 준수 문제를 감지하고 해결을 위한 알림을 생성하며, 이는 AWS Config Amazon GuardDuty AWS Security Hub CSPM, , AWS Trusted Advisor Amazon Inspector 및 사용자 지정 AWS Lambda 검사를 사용하여 구현됩니다.

가드레일(AI)

책임감 있고 안전한 AI 동작을 보장하기 위해 에이전트 입력 및 출력을 필터링, 검증 및 제약하는 안전 메커니즘입니다.

H

HA

고가용성을 참조하세요.

이기종 데이터베이스 마이그레이션

다른 데이터베이스 엔진을 사용하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Oracle에서 Amazon Aurora로) 이기종 마이그레이션은 일반적으로 리아키텍트 작업의 일부이며 스키마를 변환하는 것은 복잡한 작업일 수 있습니다.AWS 는 스키마 변환에 도움이 되는 AWS SCT를 제공합니다.

높은 가용성(HA)

문제나 재해 발생 시 개입 없이 지속적으로 운영할 수 있는 워크로드의 능력. HA 시스템은 자동으로 장애 조치되고, 지속적으로 고품질 성능을 제공하고, 성능에 미치는 영향을 최소화하면서 다양한 부하와 장애를 처리하도록 설계되었습니다.

히스토리언 현대화

제조 산업의 요구 사항을 더 잘 충족하도록 운영 기술(OT) 시스템을 현대화하고 업그레이드하는 데 사용되는 접근 방식입니다. 히스토리언은 공장의 다양한 출처에서 데이터를 수집하고 저장하는 데 사용되는 일종의 데이터베이스입니다.

홀드아웃 데이터

기계 학습 모델을 훈련하는 데 사용되는 데이터세트에서 보류되는 레이블이 지정된 기록 데이터의 일부입니다. 홀드아웃 데이터를 사용하여 모델 예측을 홀드아웃 데이터와 비교해 모델 성능을 평가할 수 있습니다.

human-in-the-loop(HitL)

중요한 결정 시점에서 인적 검토 및 승인을 위해 에이전트 실행이 일시 중지되는 워크플로 패턴입니다.

동종 데이터베이스 마이그레이션

동일한 데이터베이스 엔진을 공유하는 대상 데이터베이스로 소스 데이터베이스 마이그레이션(예: Microsoft SQL Server에서 Amazon RDS for SQL Server로) 동종 마이그레이션은 일반적으로 리호스팅 또는 리플랫포밍 작업의 일부입니다. 네이티브 데이터베이스 유틸리티를 사용하여 스키마를 마이그레이션할 수 있습니다.

핫 데이터

자주 액세스하는 데이터(예: 실시간 데이터 또는 최근 번역 데이터). 일반적으로 이 데이터에는 빠른 쿼리 응답을 제공하기 위한 고성능 스토리지 계층 또는 클래스가 필요합니다.

핫픽스

프로덕션 환경의 중요한 문제를 해결하기 위한 긴급 수정입니다. 핫픽스는 긴급하기 때문에 일반적인 DevOps 릴리스 워크플로 외부에서 실행됩니다.

하이퍼케어 기간

전환 직후 마이그레이션 팀이 문제를 해결하기 위해 클라우드에서 마이그레이션된 애플리케이션을 관리하고 모니터링하는 기간입니다. 일반적으로 이 기간은 1~4일입니다. 하이퍼케어 기간이 끝나면 마이그레이션 팀은 일반적으로 애플리케이션에 대한 책임을 클라우드 운영 팀에 넘깁니다.

I

IaC

코드형 인프라를 참조하세요.

자격 증명 기반 정책

AWS 클라우드 환경 내에서 권한을 정의하는 하나 이상의 IAM 보안 주체에 연결된 정책입니다.

유휴 애플리케이션

90일 동안 평균 CPU 및 메모리 사용량이 5~20%인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하거나 온프레미스에 유지하는 것이 일반적입니다.

IIoT

산업용 사물 인터넷을 참조하세요.

변경 불가능한 인프라

기존 인프라를 업데이트, 패치 또는 수정하는 대신 프로덕션 워크로드에 대한 새 인프라를 배포하는 모델입니다. 변경 불가능한 인프라는 변경 가능한 인프라보다 본질적으로 더 일관되고 안정적이며 예측 가능합니다. 자세한 내용은 AWS Well-Architected Framework의 변경 불가능한 인프라를 사용하여 배포 모범 사례를 참조하세요.

인바운드(수신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 외부에서 네트워크 연결을 수락, 검사 및 라우팅하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

증분 마이그레이션

한 번에 전체 전환을 수행하는 대신 애플리케이션을 조금씩 마이그레이션하는 전환 전략입니다. 예를 들어, 처음에는 소수의 마이크로서비스나 사용자만 새 시스템으로 이동할 수 있습니다. 모든 것이 제대로 작동하는지 확인한 후에는 레거시 시스템을 폐기할 수 있을 때까지 추가 마이크로서비스 또는 사용자를 점진적으로 이동할 수 있습니다. 이 전략을 사용하면 대규모 마이그레이션과 관련된 위험을 줄일 수 있습니다.

Industry 4.0

연결성, 실시간 데이터, 자동화, 분석 및 AI/ML의 발전을 통해 제조 프로세스의 현대화를 나타내기 위해 2016년에 Klaus Schwab에서 도입한 용어입니다.

인프라

애플리케이션의 환경 내에 포함된 모든 리소스와 자산입니다.

코드형 인프라(IaC)

구성 파일 세트를 통해 애플리케이션의 인프라를 프로비저닝하고 관리하는 프로세스입니다. IaC는 새로운 환경의 반복 가능성, 신뢰성 및 일관성을 위해 인프라 관리를 중앙 집중화하고, 리소스를 표준화하고, 빠르게 확장할 수 있도록 설계되었습니다.

산업용 사물 인터넷(IIoT)

제조, 에너지, 자동차, 의료, 생명과학, 농업 등의 산업 부문에서 인터넷에 연결된 센서 및 디바이스의 사용 자세한 내용은 산업용 사물 인터넷(IoT) 디지털 트랜스포메이션 전략 구축을 참조하십시오.

검사 VPC

AWS 다중 계정 아키텍처에서는 VPC(동일하거나 다른 AWS 리전), 인터넷 및 온프레미스 네트워크 간의 네트워크 트래픽 검사를 관리하는 중앙 집중식 VPCs입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

사물 인터넷(IoT)

인터넷이나 로컬 통신 네트워크를 통해 다른 디바이스 및 시스템과 통신하는 센서 또는 프로세서가 내장된 연결된 물리적 객체의 네트워크 자세한 내용은 IoT란?을 참조하십시오.

해석력

모델의 예측이 입력에 따라 어떻게 달라지는지를 사람이 이해할 수 있는 정도를 설명하는 기계 학습 모델의 특성입니다. 자세한 내용은 기계 학습 모델 해석 가능성을 참조하세요 AWS.

IoT

사물 인터넷을 참조하세요.

IT 정보 라이브러리(ITIL)

IT 서비스를 제공하고 이러한 서비스를 비즈니스 요구 사항에 맞게 조정하기 위한 일련의 모범 사례 ITIL은 ITSM의 기반을 제공합니다.

IT 서비스 관리(ITSM)

조직의 IT 서비스 설계, 구현, 관리 및 지원과 관련된 활동 클라우드 운영을 ITSM 도구와 통합하는 방법에 대한 자세한 내용은 운영 통합 가이드를 참조하십시오.

ITIL

IT 정보 라이브러리를 참조하세요.

ITSM

IT 서비스 관리를 참조하세요.

L

레이블 기반 액세스 제어(LBAC)

사용자 및 데이터 자체에 각각 보안 레이블 값을 명시적으로 할당하는 필수 액세스 제어(MAC)를 구현한 것입니다. 사용자 보안 레이블과 데이터 보안 레이블 간의 교차 부분에 따라 사용자가 볼 수 있는 행과 열이 결정됩니다.

랜딩 존

랜딩 존은 확장 가능하고 안전한 잘 설계된 다중 계정 AWS 환경입니다. 조직은 여기에서부터 보안 및 인프라 환경에 대한 확신을 가지고 워크로드와 애플리케이션을 신속하게 시작하고 배포할 수 있습니다. 랜딩 존에 대한 자세한 내용은 안전하고 확장 가능한 다중 계정 AWS 환경 설정을 참조하십시오.

대규모 언어 모델(LLM)

방대한 양의 데이터에서 사전 훈련된 딥 러닝 AI 모델입니다. LLM은 질문에 대한 답변, 문서 요약, 텍스트를 다른 언어로 번역, 문장 완성과 같은 여러 태스크를 수행할 수 있습니다. 자세한 내용은 대규모 언어 모델(LLM)이란 무엇인가요?를 참조하세요.

대규모 마이그레이션

300대 이상의 서버 마이그레이션입니다.

LBAC

레이블 기반 액세스 제어를 참조하세요.

최소 권한

작업을 수행하는 데 필요한 최소 권한을 부여하는 보안 모범 사례입니다. 자세한 내용은 IAM 설명서의 최소 권한 적용을 참조하십시오.

리프트 앤드 시프트

7R을 참조하세요.

리틀 엔디안 시스템

가장 덜 중요한 바이트를 먼저 저장하는 시스템입니다. 엔디안도 참조하세요.

LLM

대규모 언어 모델을 참조하세요.

하위 환경

환경을 참조하세요.

M

기계 학습(ML)

패턴 인식 및 학습에 알고리즘과 기법을 사용하는 인공 지능의 한 유형입니다. ML은 사물 인터넷(IoT) 데이터와 같은 기록된 데이터를 분석하고 학습하여 패턴을 기반으로 통계 모델을 생성합니다. 자세한 내용은 기계 학습을 참조하십시오.

기본 브랜치

브랜치를 참조하세요.

맬웨어

컴퓨터 보안 또는 프라이버시를 위협하도록 설계된 소프트웨어입니다. 맬웨어는 컴퓨터 시스템을 방해하거나 민감한 정보를 유출하거나 무단 액세스 권한을 확보할 수 있습니다. 맬웨어의 예로 바이러스, 웜, 랜섬웨어, 트로이 목마, 스파이웨어, 키로거 등이 있습니다.

관리형 서비스

AWS 서비스 는 인프라 계층, 운영 체제 및 플랫폼을 AWS 운영하며 사용자는 엔드포인트에 액세스하여 데이터를 저장하고 검색합니다. 관리형 서비스의 예로 Amazon Simple Storage Service(Amazon S3) 및 Amazon DynamoDB가 있습니다. 이를 추상화된 서비스라고도 합니다.

제조 실행 시스템(MES)

원자재를 생산 현장에서 완제품으로 변환하는 생산 프로세스를 추적, 모니터링, 문서화 및 제어하기 위한 소프트웨어 시스템입니다.

MAP

Migration Acceleration Program을 참조하세요.

MCP

모델 컨텍스트 프로토콜을 참조하세요.

Model Context Protocol(MCP)

에이전트 간??? 통신을 위한 상태 비저장 프로토콜입니다.

MCP 서버

모델 컨텍스트 프로토콜을 통해 하나 이상의 도구를 노출하는 서비스입니다.

메커니즘

도구를 생성하고 도구 채택을 유도한 다음 조정을 위해 결과를 검사하는 전체 프로세스입니다. 메커니즘은 작동 시 자체적으로 강화하고 개선하는 주기입니다. 자세한 내용은 AWS Well-Architected Framework의 메커니즘 구축을 참조하세요.

멤버 계정

조직의 일부인 관리 계정을 AWS 계정 제외한 모든 계정. AWS Organizations하나의 계정은 한 번에 하나의 조직 멤버만 될 수 있습니다.

MES

제조 실행 시스템을 참조하세요.

메시지 큐 원격 분석 전송(MQTT)

리소스 제약이 있는 IoT 디바이스에 대한 게시 및 구독 패턴을 기반으로 하는 경량 Machine-to-Machine(M2M) 통신 프로토콜입니다.

마이크로서비스

잘 정의된 API를 통해 통신하고 일반적으로 소규모 자체 팀이 소유하는 소규모 독립 서비스입니다. 예를 들어, 보험 시스템에는 영업, 마케팅 등의 비즈니스 역량이나 구매, 청구, 분석 등의 하위 영역에 매핑되는 마이크로 서비스가 포함될 수 있습니다. 마이크로서비스의 이점으로 민첩성, 유연한 확장, 손쉬운 배포, 재사용 가능한 코드, 복원력 등이 있습니다. 자세한 내용은 AWS 서버리스 서비스를 사용하여 마이크로서비스 통합을 참조하세요.

마이크로서비스 아키텍처

각 애플리케이션 프로세스를 마이크로서비스로 실행하는 독립 구성 요소를 사용하여 애플리케이션을 구축하는 접근 방식입니다. 이러한 마이크로서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 애플리케이션의 특정 기능에 대한 수요에 맞게 이 아키텍처의 각 마이크로서비스를 업데이트, 배포 및 조정할 수 있습니다. 자세한 내용은 에서 마이크로서비스 구현을 참조하세요 AWS.

Migration Acceleration Program(MAP)

조직이 클라우드로 전환하기 위한 강력한 운영 기반을 구축하고 초기 마이그레이션 비용을 상쇄하는 데 도움이 되는 컨설팅 지원, 교육 및 서비스를 제공하는 AWS 프로그램입니다. MAP에는 레거시 마이그레이션을 체계적인 방식으로 실행하기 위한 마이그레이션 방법론과 일반적인 마이그레이션 시나리오를 자동화하고 가속화하는 도구 세트가 포함되어 있습니다.

대규모 마이그레이션

애플리케이션 포트폴리오의 대다수를 웨이브를 통해 클라우드로 이동하는 프로세스로, 각 웨이브에서 더 많은 애플리케이션이 더 빠른 속도로 이동합니다. 이 단계에서는 이전 단계에서 배운 모범 사례와 교훈을 사용하여 팀, 도구 및 프로세스의 마이그레이션 팩토리를 구현하여 자동화 및 민첩한 제공을 통해 워크로드 마이그레이션을 간소화합니다. 이것은 AWS 마이그레이션 전략의 세 번째 단계입니다.

마이그레이션 팩토리

자동화되고 민첩한 접근 방식을 통해 워크로드 마이그레이션을 간소화하는 다기능 팀입니다. 마이그레이션 팩토리 팀에는 일반적으로 스프린트에서 일하는 운영, 비즈니스 분석가 및 소유자, 마이그레이션 엔지니어, 개발자, DevOps 전문가가 포함됩니다. 엔터프라이즈 애플리케이션 포트폴리오의 20~50%는 공장 접근 방식으로 최적화할 수 있는 반복되는 패턴으로 구성되어 있습니다. 자세한 내용은 이 콘텐츠 세트의 클라우드 마이그레이션 팩토리 가이드와 마이그레이션 팩토리에 대한 설명을 참조하십시오.

마이그레이션 메타데이터

마이그레이션을 완료하는 데 필요한 애플리케이션 및 서버에 대한 정보 각 마이그레이션 패턴에는 서로 다른 마이그레이션 메타데이터 세트가 필요합니다. 마이그레이션 메타데이터의 예로는 대상 서브넷, 보안 그룹 및 AWS 계정이 있습니다.

마이그레이션 패턴

사용되는 마이그레이션 전략, 마이그레이션 대상, 마이그레이션 애플리케이션 또는 서비스를 자세히 설명하는 반복 가능한 마이그레이션 작업입니다. 예: AWS Application Migration Service를 사용하여 Amazon EC2로 마이그레이션을 리호스팅합니다.

Migration Portfolio Assessment(MPA)

AWS 클라우드로 마이그레이션하는 비즈니스 사례를 검증하기 위한 정보를 제공하는 온라인 도구입니다. MPA는 상세한 포트폴리오 평가(서버 적정 규모 조정, 가격 책정, TCO 비교, 마이그레이션 비용 분석)와 마이그레이션 계획(애플리케이션 데이터 분석 및 데이터 수집, 애플리케이션 그룹화, 마이그레이션 우선순위 지정, 웨이브 계획)을 제공합니다. MPA 도구(로그인 필요)는 모든 AWS 컨설턴트와 APN 파트너 컨설턴트가 무료로 사용할 수 있습니다.

마이그레이션 준비 상태 평가(MRA)

AWS CAF를 사용하여 조직의 클라우드 준비 상태에 대한 인사이트를 얻고, 강점과 약점을 식별하고, 식별된 격차를 해소하기 위한 행동 계획을 수립하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 가이드를 참조하십시오. MRA는 AWS 마이그레이션 전략의 첫 번째 단계입니다.

마이그레이션 전략

워크로드를 AWS 클라우드로 마이그레이션하는 데 사용되는 접근 방식입니다. 자세한 내용은 이 용어집의 7R 항목과 조직을 동원하여 대규모 마이그레이션 가속화를 참조하세요.

ML

기계 학습을 참조하세요.

현대화

비용을 절감하고 효율성을 높이고 혁신을 활용하기 위해 구식(레거시 또는 모놀리식) 애플리케이션과 해당 인프라를 클라우드의 민첩하고 탄력적이고 가용성이 높은 시스템으로 전환하는 것입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 전략을 참조하세요.

현대화 준비 상태 평가

조직 애플리케이션의 현대화 준비 상태를 파악하고, 이점, 위험 및 종속성을 식별하고, 조직이 해당 애플리케이션의 향후 상태를 얼마나 잘 지원할 수 있는지를 확인하는 데 도움이 되는 평가입니다. 평가 결과는 대상 아키텍처의 청사진, 현대화 프로세스의 개발 단계와 마일스톤을 자세히 설명하는 로드맵 및 파악된 격차를 해소하기 위한 실행 계획입니다. 자세한 내용은 AWS 클라우드에서 애플리케이션의 현대화 준비 상태 평가를 참조하세요.

모놀리식 애플리케이션(모놀리식 유형)

긴밀하게 연결된 프로세스를 사용하여 단일 서비스로 실행되는 애플리케이션입니다. 모놀리식 애플리케이션에는 몇 가지 단점이 있습니다. 한 애플리케이션 기능에 대한 수요가 급증하면 전체 아키텍처 규모를 조정해야 합니다. 코드 베이스가 커지면 모놀리식 애플리케이션의 기능을 추가하거나 개선하는 것도 더 복잡해집니다. 이러한 문제를 해결하기 위해 마이크로서비스 아키텍처를 사용할 수 있습니다. 자세한 내용은 마이크로서비스로 모놀리식 유형 분해를 참조하십시오.

MPA

Migration Portfolio Assessment를 참조하세요.

MQTT

메시지 큐 원격 분석 전송을 참조하세요.

멀티클래스 분류

여러 클래스에 대한 예측(2개 이상의 결과 중 하나 예측)을 생성하는 데 도움이 되는 프로세스입니다. 예를 들어, ML 모델이 '이 제품은 책인가요, 자동차인가요, 휴대폰인가요?' 또는 '이 고객이 가장 관심을 갖는 제품 범주는 무엇인가요?'라고 물을 수 있습니다.

변경 가능한 인프라

프로덕션 워크로드에 대한 기존 인프라를 업데이트하고 수정하는 모델입니다. 일관성, 신뢰성 및 예측 가능성을 높이기 위해 AWS Well-Architected Framework는 변경 불가능한 인프라를 모범 사례로 사용할 것을 권장합니다.

O

OAC

오리진 액세스 제어를 참조하세요.

OAI

오리진 액세스 ID를 참조하세요.

OCM

조직 변경 관리를 참조하세요.

오프라인 마이그레이션

마이그레이션 프로세스 중 소스 워크로드가 중단되는 마이그레이션 방법입니다. 이 방법은 가동 중지 증가를 수반하며 일반적으로 작고 중요하지 않은 워크로드에 사용됩니다.

OI

운영 통합을 참조하세요.

OLA

운영 수준 계약을 참조하세요.

온라인 마이그레이션

소스 워크로드를 오프라인 상태로 전환하지 않고 대상 시스템에 복사하는 마이그레이션 방법입니다. 워크로드에 연결된 애플리케이션은 마이그레이션 중에도 계속 작동할 수 있습니다. 이 방법은 가동 중지 차단 또는 최소화를 수반하며 일반적으로 중요한 프로덕션 워크로드에 사용됩니다.

OPC-UA

Open Process Communications - Unified Architecture(OPC-UA)를 참조하세요.

Open Process Communications - Unified Architecture(OPC-UA)

산업 자동화를 위한 Machine-to-Machine(M2M) 통신 프로토콜입니다. OPC-UA는 데이터 암호화, 인증 및 권한 부여 체계에 관한 상호 운용성 표준을 제공합니다.

운영 수준 협약(OLA)

서비스 수준에 관한 계약(SLA)을 지원하기 위해 직무 IT 그룹이 서로에게 제공하기로 약속한 내용을 명확히 하는 계약입니다.

운영 준비 상태 검토(ORR)

인시던트 및 잠재적 장애의 범위를 이해, 평가 또는 예방하거나 줄이는 데 도움이 되는 질문 체크리스트 및 관련 모범 사례입니다. 자세한 내용은 AWS Well-Architected Framework의 운영 준비 상태 검토(ORR)를 참조하세요.

운영 기술(OT)

물리적 환경에서 작동하여 산업 운영, 장비 및 인프라를 제어하는 하드웨어 및 소프트웨어 시스템입니다. 제조 분야에서 OT 및 정보 기술(IT) 시스템의 통합은 Industry 4.0 트랜스포메이션의 주요 중점 사항입니다.

운영 통합(OI)

클라우드에서 운영을 현대화하는 프로세스로 준비 계획, 자동화 및 통합을 수반합니다. 자세한 내용은 운영 통합 가이드를 참조하십시오.

조직 트레일

조직 AWS 계정 내 모든에 대한 모든 이벤트를 로깅 AWS CloudTrail 하는에서 생성된 추적입니다 AWS Organizations. 이 트레일은 조직에 속한 각 AWS 계정 에 생성되고 각 계정의 활동을 추적합니다. 자세한 내용은 CloudTrail 설명서의 Creating a trail for an organization을 참조하십시오.

조직 변경 관리(OCM)

사람, 문화 및 리더십 관점에서 중대하고 파괴적인 비즈니스 혁신을 관리하기 위한 프레임워크입니다. OCM은 변화 채택을 가속화하고, 과도기적 문제를 해결하고, 문화 및 조직적 변화를 주도함으로써 조직이 새로운 시스템 및 전략을 준비하고 전환할 수 있도록 지원합니다. AWS 마이그레이션 전략에서는 클라우드 채택 프로젝트에 필요한 변경 속도 때문에이 프레임워크를 인력 가속화라고 합니다. 자세한 내용은 사용 가이드를 참조하십시오.

오리진 액세스 제어(OAC)

CloudFront에서 Amazon Simple Storage Service(S3) 콘텐츠를 보호하기 위해 액세스를 제한하는 고급 옵션입니다. OAC는 AWS KMS (SSE-KMS)를 사용한 모든 서버 측 암호화 AWS 리전와 S3 버킷에 대한 동적 PUT 및 DELETE 요청에서 모든 S3 버킷을 지원합니다.

오리진 액세스 ID(OAI)

CloudFront에서 Amazon S3 콘텐츠를 보호하기 위해 액세스를 제한하는 옵션입니다. OAI를 사용하면 CloudFront는 Amazon S3가 인증할 수 있는 보안 주체를 생성합니다. 인증된 보안 주체는 특정 CloudFront 배포를 통해서만 S3 버킷의 콘텐츠에 액세스할 수 있습니다. 더 세분화되고 향상된 액세스 제어를 제공하는 OAC도 참조하십시오.

ORR

운영 준비 상태 검토를 참조하세요.

OT

운영 기술을 참조하세요.

아웃바운드(송신) VPC

AWS 다중 계정 아키텍처에서 애플리케이션 내에서 시작된 네트워크 연결을 처리하는 VPC입니다. AWS Security Reference Architecture에서는 애플리케이션과 더 넓은 인터넷 간의 양방향 인터페이스를 보호하기 위해 인바운드, 아웃바운드 및 검사 VPC로 네트워크 계정을 설정할 것을 권장합니다.

P

권한 경계

사용자나 역할이 가질 수 있는 최대 권한을 설정하기 위해 IAM 보안 주체에 연결되는 IAM 관리 정책입니다. 자세한 내용은 IAM 설명서의 권한 경계를 참조하십시오.

개인 식별 정보(PII)

직접 보거나 다른 관련 데이터와 함께 짝을 지을 때 개인의 신원을 합리적으로 추론하는 데 사용할 수 있는 정보입니다. PII의 예로는 이름, 주소, 연락처 정보 등이 있습니다.

PII

개인 식별 정보를 참조하세요.

플레이북

클라우드에서 핵심 운영 기능을 제공하는 등 마이그레이션과 관련된 작업을 캡처하는 일련의 사전 정의된 단계입니다. 플레이북은 스크립트, 자동화된 런북 또는 현대화된 환경을 운영하는 데 필요한 프로세스나 단계 요약의 형태를 취할 수 있습니다.

PLC

프로그래밍 가능 로직 컨트롤러를 참조하세요.

PLM

제품 수명 주기 관리를 참조하세요.

정책

권한 정의(ID 기반 정책 참조), 액세스 조건 지정(리소스 기반 정책 참조), AWS Organizations 내 조직의 모든 계정에 대한 최대 권한 정의(서비스 제어 정책 참조)와 같은 작업을 수행할 수 있는 객체입니다.

다국어 지속성

데이터 액세스 패턴 및 기타 요구 사항을 기반으로 독립적으로 마이크로서비스의 데이터 스토리지 기술 선택. 마이크로서비스가 동일한 데이터 스토리지 기술을 사용하는 경우 구현 문제가 발생하거나 성능이 저하될 수 있습니다. 요구 사항에 가장 적합한 데이터 저장소를 사용하면 마이크로서비스를 더 쉽게 구현하고 성능과 확장성을 높일 수 있습니다.

포트폴리오 평가

마이그레이션을 계획하기 위해 애플리케이션 포트폴리오를 검색 및 분석하고 우선순위를 정하는 프로세스입니다. 자세한 내용은 마이그레이션 준비 상태 평가를 참조하십시오.

조건자

보통 `WHERE` 절에 있는 `true` 또는 `false`를 반환하는 쿼리 조건입니다.

푸시다운 조건자

전송 전에 쿼리의 데이터를 필터링하는 데이터베이스 쿼리 최적화 기법입니다. 이렇게 하면 관계형 데이터베이스에서 검색하고 처리해야 하는 데이터의 양이 줄고 쿼리 성능이 향상됩니다.

예방적 제어

이벤트 발생을 방지하도록 설계된 보안 제어입니다. 이 제어는 네트워크에 대한 무단 액세스나 원치 않는 변경을 방지하는 데 도움이 되는 1차 방어선입니다. 자세한 내용은 Implementing security controls on AWS의 Preventative controls를 참조하십시오.

보안 주체

작업을 수행하고 리소스에 액세스할 수 AWS 있는의 엔터티입니다. 이 엔터티는 일반적으로 , AWS 계정 IAM 역할 또는 사용자의 루트 사용자입니다. 자세한 내용은 IAM 설명서의 역할 용어 및 개념의 보안 주체를 참조하십시오.

개인 정보 보호 중심 설계

전체 개발 프로세스에서 개인 정보를 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

프라이빗 호스팅 영역

Amazon Route 53에서 하나 이상의 VPC 내 도메인과 하위 도메인에 대한 DNS 쿼리에 응답하는 방법에 대한 정보가 담긴 컨테이너입니다. 자세한 내용은 Route 53 설명서의 프라이빗 호스팅 영역 작업을 참조하십시오.

선제적 제어

규정 미준수 리소스의 배포를 방지하도록 설계된 보안 제어입니다. 이러한 제어는 리소스를 프로비저닝하기 전에 리소스를 스캔합니다. 리소스가 제어를 준수하지 않으면 프로비저닝되지 않습니다. 자세한 내용은 AWS Control Tower 설명서의 제어 참조 가이드를 참조하고 보안 제어 구현의 사전 예방적 제어를 참조하세요. AWS

제품 수명 주기 관리(PLM)

설계, 개발 및 출시부터 성장 및 성숙도를 거쳐 거부 및 제거에 이르기까지 전체 수명 주기 동안 제품의 데이터 및 프로세스 관리를 나타냅니다.

프로덕션 환경

환경을 참조하세요.

프로그래밍 가능 로직 컨트롤러(PLC)

제조 분야에서 기계를 모니터링하고 제조 프로세스를 자동화하는 매우 안정적이고 적응력이 뛰어난 컴퓨터입니다.

프롬프트 체이닝

한 LLM 프롬프트의 출력을 다음 프롬프트의 입력으로 사용하여 더 나은 응답을 생성합니다. 이 기법은 복잡한 태스크를 하위 태스크로 나누거나 예비 응답을 반복적으로 세부 조정하거나 확장하는 데 사용됩니다. 이를 통해 모델 응답의 정확성과 관련성을 개선하고 보다 세분화되고 개인화된 결과를 얻을 수 있습니다.

가명화

데이터세트의 개인 식별자를 자리 표시자 값으로 바꾸는 프로세스입니다. 가명화는 개인 정보를 보호하는 데 도움이 될 수 있습니다. 가명화된 데이터는 여전히 개인 데이터로 간주됩니다.

게시/구독(pub/sub)

여러 마이크로서비스에서 비동기 통신을 지원하여 확장성과 응답성을 개선하는 패턴입니다. 예를 들어 마이크로서비스 기반 MES에서 마이크로서비스는 다른 마이크로서비스가 구독할 수 있는 채널에 이벤트 메시지를 게시할 수 있습니다. 시스템은 게시 서비스를 변경하지 않고도 새 마이크로서비스를 추가할 수 있습니다.

Q

쿼리 계획

SQL 관계형 데이터베이스 시스템의 데이터에 액세스하는 데 사용되는 명령어와 같은 일련의 단계입니다.

쿼리 계획 회귀

데이터베이스 서비스 최적화 프로그램이 데이터베이스 환경을 변경하기 전보다 덜 최적의 계획을 선택하는 경우입니다. 통계, 제한 사항, 환경 설정, 쿼리 파라미터 바인딩 및 데이터베이스 엔진 업데이트의 변경으로 인해 발생할 수 있습니다.

R

RACI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RAG

검색 증강 생성을 참조하세요.

랜섬웨어

결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다.

RASCI 매트릭스

Responsible, Accountable, Consulted, Informed(RACI)를 참조하세요.

RCAC

행 및 열 액세스 제어를 참조하세요.

읽기 전용 복제본

읽기 전용 용도로 사용되는 데이터베이스의 사본입니다. 쿼리를 읽기 전용 복제본으로 라우팅하여 기본 데이터베이스의 로드를 줄일 수 있습니다.

리아키텍팅

7R을 참조하세요.

Recovery Point Objective(RPO)

마지막 데이터 복구 시점 이후 허용되는 최대 시간입니다. 이에 따라 마지막 복구 시점과 서비스 중단 사이에 허용되는 데이터 손실로 간주되는 범위가 결정됩니다.

Recovery Time Objective(RTO)

서비스 중단과 서비스 복원 사이의 허용 가능한 지연 시간입니다.

리팩터링

7R을 참조하세요.

리전

지리적 영역의 AWS 리소스 모음입니다. 각 AWS 리전 는 내결함성, 안정성 및 복원력을 제공하기 위해 서로 격리되고 독립적입니다. 자세한 내용은 계정에서 사용할 수 있는 AWS 리전 지정을 참조하세요.

회귀

숫자 값을 예측하는 ML 기법입니다. 예를 들어, '이 집은 얼마에 팔릴까?'라는 문제를 풀기 위해 ML 모델은 선형 회귀 모델을 사용하여 주택에 대해 알려진 사실(예: 면적)을 기반으로 주택의 매매 가격을 예측할 수 있습니다.

리호스팅

7R을 참조하세요.

릴리스

배포 프로세스에서 변경 사항을 프로덕션 환경으로 승격시키는 행위입니다.

재배치

7R을 참조하세요.

리플랫포밍

7R을 참조하세요.

재구매

7R을 참조하세요.

복원력

중단에 저항하거나 중단을 복구할 수 있는 애플리케이션의 기능입니다. 고가용성 및 재해 복구는 AWS 클라우드에서 복원력을 계획할 때 일반적인 고려 사항입니다. 자세한 내용은 AWS 클라우드 복원력을 참조하세요.

리소스 기반 정책

Amazon S3 버킷, 엔드포인트, 암호화 키 등의 리소스에 연결된 정책입니다. 이 유형의 정책은 액세스가 허용된 보안 주체, 지원되는 작업 및 충족해야 하는 기타 조건을 지정합니다.

RACI(Responsible, Accountable, Consulted, Informed) 매트릭스

마이그레이션 활동 및 클라우드 운영에 참여하는 모든 당사자의 역할과 책임을 정의하는 매트릭스입니다. 매트릭스 이름은 매트릭스에 정의된 책임 유형에서 파생됩니다. 실무 담당자 (R), 의사 결정권자 (A), 업무 수행 조언자 (C), 결과 통보 대상자 (I). 지원자는 (S) 선택사항입니다. 지원자를 포함하면 매트릭스를 RASCI 매트릭스라고 하고, 지원자를 제외하면 RACI 매트릭스라고 합니다.

대응 제어

보안 기준에서 벗어나거나 부정적인 이벤트를 해결하도록 설계된 보안 제어입니다. 자세한 내용은 AWS에서 보안 제어 구현의 대응 제어를 참조하세요.

retain

7R을 참조하세요.

사용 중지

7R을 참조하세요.

검색 증강 세대(RAG)

응답을 생성하기 전에 LLM이 훈련 데이터 소스 외부에 있는 신뢰할 수 있는 데이터 소스를 참조하는 생성형 AI 기술입니다. 예를 들어 RAG 모델은 조직의 지식 기반 또는 사용자 지정 데이터에 대

한 시맨틱 검색을 수행할 수 있습니다. 자세한 내용은 검색 증강 생성(RAG)이란 무엇인가요?를 참조하세요.

교체

공격자가 자격 증명에 액세스하는 것을 더욱 어렵게 만들기 위해 보안 암호를 주기적으로 업데이트하는 프로세스입니다.

행 및 열 액세스 제어(RCAC)

액세스 규칙이 정의된 기본적이고 유연한 SQL 표현식을 사용합니다. RCAC는 행 권한과 열 마스크로 구성됩니다.

RPO

목표 복구 시점(RPO)을 참조하세요.

RTO

목표 복구 시간(RTO)을 참조하세요.

런북

특정 작업을 수행하는 데 필요한 일련의 수동 또는 자동 절차입니다. 일반적으로 오류율이 높은 반복 작업이나 절차를 간소화하기 위해 런북을 만듭니다.

S

SAML 2.0

많은 ID 제공업체(idP)에서 사용하는 개방형 표준입니다. 이 기능을 사용하면 연동 SSO(Single Sign-On)를 AWS Management Console 사용할 수 있으므로 사용자는 조직의 모든 사용자에 대해 IAM에서 사용자를 생성하지 않고도에 로그인하거나 AWS API 작업을 호출할 수 있습니다. SAML 2.0 기반 페더레이션에 대한 자세한 내용은 IAM 설명서의 SAML 2.0 기반 페더레이션 정보를 참조하십시오.

SCADA

감독 제어 및 데이터 획득을 참조하세요.

SCP

서비스 제어 정책을 참조하세요.

보안 암호

에는 암호 또는 사용자 자격 증명과 같이 암호화된 형식으로 저장하는 AWS Secrets Manager기밀 또는 제한된 정보가 있습니다. 보안 암호 값과 메타데이터로 구성됩니다. 보안 암호 값은 바이너리, 단일 문자열 또는 여러 문자열일 수 있습니다. 자세한 내용은 AWS Secrets Manager 설명서의 Secrets Manager 보안 암호란 무엇인가요?를 참조하세요.

보안 중심 설계

전체 개발 프로세스에서 보안을 고려하는 시스템 엔지니어링에서의 접근 방식입니다.

보안 제어

위협 행위자가 보안 취약성을 악용하는 능력을 방지, 탐지 또는 감소시키는 기술적 또는 관리적 가드레일입니다. 보안 제어는 예방, 감지, 대응, 선제적과 같은 기본적인 네 가지 보안 제어 유형으로 구분됩니다.

보안 강화

공격 표면을 줄여 공격에 대한 저항력을 높이는 프로세스입니다. 더 이상 필요하지 않은 리소스 제거, 최소 권한 부여의 보안 모범 사례 구현, 구성 파일의 불필요한 기능 비활성화 등의 작업이 여기에 포함될 수 있습니다.

보안 정보 및 이벤트 관리(SIEM) 시스템

보안 정보 관리(SIM)와 보안 이벤트 관리(SEM) 시스템을 결합하는 도구 및 서비스입니다. SIEM 시스템은 서버, 네트워크, 디바이스 및 기타 소스에서 데이터를 수집, 모니터링 및 분석하여 위협과 보안 침해를 탐지하고 알림을 생성합니다.

보안 응답 자동화

보안 이벤트에 자동으로 응답하거나 이를 해결하도록 설계된 사전 정의되고 프로그래밍된 작업입니다. 이러한 자동화는 보안 모범 사례를 구현하는 데 도움이 되는 탐지 또는 대응 AWS 보안 제어 역할을 합니다. 자동화된 응답 작업의 예로 VPC 보안 그룹 수정, Amazon EC2 인스턴스 패치 적용 또는 자격 증명 교체 등이 있습니다.

서버 측 암호화

데이터를 AWS 서비스 수신하는가 대상에서 데이터를 암호화합니다.

서비스 제어 정책(SCP)

AWS Organizations에 속한 조직의 모든 계정에 대한 권한을 중앙 집중식으로 제어하는 정책입니다. SCP는 관리자가 사용자 또는 역할에 위임할 수 있는 작업에 대해 제한을 설정하거나 가드레일을 정의합니다. SCP를 허용 목록 또는 거부 목록으로 사용하여 허용하거나 금지할 서비스 또는 작

업을 지정할 수 있습니다. 자세한 내용은 AWS Organizations 설명서의 서비스 제어 정책을 참조하세요.

서비스 엔드포인트

에 대한 진입점의 URL입니다 AWS 서비스. 엔드포인트를 사용하여 대상 서비스에 프로그래밍 방식으로 연결할 수 있습니다. 자세한 내용은 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

서비스 수준에 관한 계약(SLA)

IT 팀이 고객에게 제공하기로 약속한 내용(예: 서비스 가동 시간 및 성능)을 명시한 계약입니다.

서비스 수준 지표(SLI)

오류 발생률, 가용성 또는 처리량과 같은 서비스의 성능 측면에 대한 측정값입니다.

서비스 수준 목표(SLO)

서비스 수준 지표로 측정되는 서비스의 상태를 나타내는 목표 지표입니다.

공동 책임 모델

클라우드 보안 및 규정 준수를 AWS 위해와 공유하는 책임을 설명하는 모델입니다. AWS 는 클라우드의 보안을 책임지고, 사용자는 클라우드의 보안을 책임집니다. 자세한 내용은 공동 책임 모델을 참조하십시오.

섀도우 AI

조직 내 관리형 채널 외부에서 구축되거나 사용되는 승인되지 않은 AI 애플리케이션입니다.

SIEM

보안 정보 및 이벤트 관리 시스템을 참조하세요.

단일 장애점(SPOF)

애플리케이션을 중단시킬 수 있는 애플리케이션의 중요한 단일 구성 요소에서 발생하는 장애입니다.

SLA

서비스 수준 계약을 참조하세요.

SLI

서비스 수준 지표를 참조하세요.

SLO

서비스 수준 목표를 참조하세요.

분할 앤 시드 모델

현대화 프로젝트를 확장하고 가속화하기 위한 패턴입니다. 새로운 기능과 제품 릴리스가 정의되면 핵심 팀이 분할되어 새로운 제품 팀이 만들어집니다. 이를 통해 조직의 역량과 서비스 규모를 조정하고, 개발자 생산성을 개선하고, 신속한 혁신을 지원할 수 있습니다. 자세한 내용은 AWS 클라우드에서 애플리케이션을 현대화하기 위한 단계별 접근 방식을 참조하세요.

SPOF

단일 장애점을 참조하세요.

스타 스키마

하나의 큰 팩트 테이블을 사용하여 트랜잭션 또는 측정된 데이터를 저장하고 하나 이상의 더 작은 차원 테이블을 사용하여 데이터 속성을 저장하는 데이터베이스 조직 구조입니다. 이 구조는 데이터 웨어하우스에서 또는 비즈니스 인텔리전스 목적으로 사용하도록 설계되었습니다.

Strangler Fig 패턴

레거시 시스템을 폐기할 수 있을 때까지 시스템 기능을 점진적으로 다시 작성하고 교체하여 모놀리식 시스템을 현대화하기 위한 접근 방식. 이 패턴은 무화과 덩굴이 나무로 자라 결국 숙주를 압도하고 대체하는 것과 비슷합니다. Martin Fowler가 모놀리식 시스템을 다시 작성할 때 위험을 관리하는 방법으로 이 패턴을 도입했습니다. 이 패턴을 적용하는 방법의 예는 컨테이너 및 Amazon API Gateway를 사용하여 기존의 Microsoft ASP.NET(ASMX) 웹 서비스를 점진적으로 현대화하는 방법을 참조하십시오.

서브넷

VPC의 IP 주소 범위입니다. 서브넷은 단일 가용 영역에 상주해야 합니다.

감독 제어 및 데이터 획득(SCADA)

제조 분야에서 하드웨어와 소프트웨어를 사용하여 물리적 자산과 프로덕션 작업을 모니터링하는 시스템입니다.

대칭 암호화

동일한 키를 사용하여 데이터를 암호화하고 복호화하는 암호화 알고리즘입니다.

합성 테스트

사용자 상호 작용을 시뮬레이션하여 잠재적 문제를 감지하거나 성능을 모니터링하는 방식으로 진행되는 시스템 테스트입니다. Amazon CloudWatch Synthetics를 사용하여 이러한 테스트를 생성할 수 있습니다.

시스템 프롬프트

LLM에 컨텍스트, 명령 또는 지침을 제공하여 동작을 지시하는 기법입니다. 시스템 프롬프트는 컨텍스트를 설정하고 사용자와의 상호 작용을 위한 규칙을 설정하는 데 도움이 됩니다.

T

tags

AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 리소스를 손쉽게 관리, 식별, 정리, 검색, 필터링할 수 있습니다. 자세한 내용은 AWS 리소스에 태그 지정을 참조하십시오.

대상 변수

지도 ML에서 예측하려는 값으로, 결과 변수라고도 합니다. 예를 들어, 제조 설정에서 대상 변수는 제품 결함일 수 있습니다.

작업 목록

런북을 통해 진행 상황을 추적하는 데 사용되는 도구입니다. 작업 목록에는 런북의 개요와 완료해야 할 일반 작업 목록이 포함되어 있습니다. 각 일반 작업에 대한 예상 소요 시간, 소유자 및 진행 상황이 작업 목록에 포함됩니다.

테스트 환경

환경을 참조하세요.

훈련

ML 모델이 학습할 수 있는 데이터를 제공하는 것입니다. 훈련 데이터에는 정답이 포함되어야 합니다. 학습 알고리즘은 훈련 데이터에서 대상(예측하려는 답)에 입력 데이터 속성을 매핑하는 패턴을 찾고, 이러한 패턴을 캡처하는 ML 모델을 출력합니다. 그런 다음 ML 모델을 사용하여 대상을 모르는 새 데이터에 대한 예측을 할 수 있습니다.

tool

에이전트가 외부 시스템에서 작업을 수행하기 위해 호출할 수 있는 함수 또는 API입니다.

Transit Gateway

VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 AWS Transit Gateway 설명서의 전송 게이트웨이란 무엇입니까?를 참조하세요.

트렁크 기반 워크플로

개발자가 기능 브랜치에서 로컬로 기능을 구축하고 테스트한 다음 해당 변경 사항을 기본 브랜치에 병합하는 접근 방식입니다. 이후 기본 브랜치는 개발, 프로덕션 이전 및 프로덕션 환경에 순차적으로 구축됩니다.

신뢰할 수 있는 액세스

사용자를 대신하여 AWS Organizations 및 해당 계정에서 조직에서 작업을 수행하도록 지정하는 서비스에 대한 권한 부여. 신뢰할 수 있는 서비스는 필요할 때 각 계정에 서비스 연결 역할을 생성하여 관리 작업을 수행합니다. 자세한 내용은 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하세요 AWS Organizations .

튜닝

ML 모델의 정확도를 높이기 위해 훈련 프로세스의 측면을 여러 변경하는 것입니다. 예를 들어, 레이블링 세트를 생성하고 레이블을 추가한 다음 다양한 설정에서 이러한 단계를 여러 번 반복하여 모델을 최적화하는 방식으로 ML 모델을 훈련할 수 있습니다.

피자 두 판 팀

피자 두 판이면 충분한 소규모 DevOps 팀. 피자 두 판 팀 규모는 소프트웨어 개발에 있어 가능한 최상의 공동 작업 기회를 보장합니다.

U

불확실성

예측 ML 모델의 신뢰성을 저해할 수 있는 부정확하거나 불완전하거나 알려지지 않은 정보를 나타내는 개념입니다. 불확실성에는 두 가지 유형이 있습니다. 인식론적 불확실성은 제한적이고 불완전한 데이터에 의해 발생하는 반면, 우연한 불확실성은 데이터에 내재된 노이즈와 무작위성에 의해 발생합니다.

차별화되지 않은 작업

애플리케이션을 만들고 운영하는 데 필요하지만 최종 사용자에게 직접적인 가치를 제공하거나 경쟁 우위를 제공하지 못하는 작업을 헤비 리프팅이라고도 합니다. 차별화되지 않은 작업의 예로는 조달, 유지보수, 용량 계획 등이 있습니다.

상위 환경

환경을 참조하세요.

V

정리

스토리지를 회수하고 성능을 향상시키기 위해 증분 업데이트 후 정리 작업을 수반하는 데이터베이스 유지 관리 작업입니다.

버전 제어

리포지토리의 소스 코드 변경과 같은 변경 사항을 추적하는 프로세스 및 도구입니다.

VPC 피어링

프라이빗 IP 주소를 사용하여 트래픽을 라우팅할 수 있게 하는 두 VPC 간의 연결입니다. 자세한 내용은 Amazon VPC 설명서의 VPC 피어링이란?을 참조하십시오.

취약성

시스템 보안을 손상시키는 소프트웨어 또는 하드웨어 결함입니다.

W

웜 캐시

자주 액세스하는 최신 관련 데이터를 포함하는 버퍼 캐시입니다. 버퍼 캐시에서 데이터베이스 인스턴스를 읽을 수 있기 때문에 주 메모리나 디스크에서 읽는 것보다 빠릅니다.

웜 데이터

자주 액세스하지 않는 데이터입니다. 이런 종류의 데이터를 쿼리할 때는 일반적으로 적절히 느린 쿼리가 허용됩니다.

창 함수

현재 레코드와 어떤 식으로든 관련된 행 그룹에서 계산을 수행하는 SQL 함수입니다. 창 함수는 이동 평균을 계산하거나 현재 행의 상대적 위치를 기반으로 행 값에 액세스하는 등의 태스크를 처리하는 데 유용합니다.

워크로드

고객 대면 애플리케이션이나 백엔드 프로세스 같이 비즈니스 가치를 창출하는 리소스 및 코드 모음입니다.

워크스트림

마이그레이션 프로젝트에서 특정 작업 세트를 담당하는 직무 그룹입니다. 각 워크스트림은 독립적이지만 프로젝트의 다른 워크스트림을 지원합니다. 예를 들어, 포트폴리오 워크스트림은 애플리케이션 우선순위 지정, 웨이브 계획, 마이그레이션 메타데이터 수집을 담당합니다. 포트폴리오 워크스트림은 이러한 자산을 마이그레이션 워크스트림에 전달하고, 마이그레이션 워크스트림은 서버와 애플리케이션을 마이그레이션합니다.

WORM

Write Once, Read Many(WORM)를 참조하세요.

WQF

AWS Workload Qualification Framework를 참조하세요.

Write Once Read Many(WORM)

데이터를 한 번 쓰고 데이터가 삭제되거나 수정되지 않도록 하는 스토리지 모델입니다. 권한 있는 사용자는 필요한 만큼 여러 번 데이터를 읽을 수 있지만 데이터를 변경할 수는 없습니다. 이 데이터 스토리지 인프라는 변경 불가능한 항목으로 간주됩니다.

Z

제로데이 익스플로잇

제로데이 취약성을 악용하는 공격(일반적으로 맬웨어)입니다.

제로데이 취약성

프로덕션 시스템의 명백한 결함 또는 취약성입니다. 위협 행위자는 이러한 유형의 취약성을 사용하여 시스템을 공격할 수 있습니다. 개발자는 공격의 결과로 취약성을 인지하는 경우가 많습니다.

제로샷 프롬프팅

태스크를 수행하기 위해 LLM에 명령을 제공하지만 안내에 도움이 되는 예제(샷)는 제공하지 않습니다. LLM은 사전 훈련된 지식을 사용하여 태스크를 처리해야 합니다. 제로샷 프롬프팅의 효과는 태스크의 복잡성과 프롬프트의 품질에 따라 달라집니다. 퓨샷 프롬프팅도 참조하세요.

좀비 애플리케이션

평균 CPU 및 메모리 사용량이 5% 미만인 애플리케이션입니다. 마이그레이션 프로젝트에서는 이러한 애플리케이션을 사용 중지하는 것이 일반적입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.