교육 부문에서 단일, 하이브리드 및 멀티클라우드를 위한 전략 구축

AWS 권장 가이드

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 권장 가이드: 교육 부문에서 단일, 하이브리드 및 멀티클라우드를 위한 전략 구축

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

소개 1
개요 1
클라우드 배포 전략 3
단일 클라우드 3
하이브리드 클라우드 3
멀티클라우드 3
권장 사항 4
기본 전략 클라우드 제공업체 선택 4
CCoE 설정 6
SaaS 애플리케이션과 기본 클라우드 서비스 간 차별화 8
각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항 설정 10
가능하고 실현 가능하면 클라우드 네이티브 관리형 서비스 채택 12
기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처 구현 16
단일 클라우드 제공업체를 통해 기술 또는 비즈니스 요구 사항을 충족할 수 없는 워크로드에 대해서만 멀티클라우드 예약 18
사용 사례 예제 21
가상 컴퓨터 랩 21
학생 성공 예측 23
ID 페더레이션 및 Single Sign-On 25
연구 컴퓨팅을 위한 클라우드 버스팅 26
다음 단계 29
기여자 30
참조 자료 31
문서 기록 32
..... xxxiii

교육 부문에서 단일, 하이브리드 및 멀티클라우드를 위한 전략 구축

Amazon Web Services(기여자)

2023년 9월(문서 기록)

교육 기관은 클라우드 컴퓨팅이 제공하는 민첩성, 비용 절감, 보안 및 복원력을 통해 원격 학습, 연구, 학생 경험, 데이터 인사이트 및 관리와 같은 기능을 지원하고자 합니다. 많은 조직이 이 디지털 트랜스포메이션의 일환으로 하이브리드 및 멀티클라우드 배포를 평가하고 있습니다.

이 문서에서는 클라우드 옵션을 평가하는 교육 기관의 임원과 의사 결정권자를 위한 단일, 하이브리드, 멀티클라우드 기술 및 거버넌스 전략 수립에 관한 권장 가이드를 제공합니다. 이 가이드는 AWS 에서 초중고등학교부터 고등 교육에 이르기까지 전 세계 모든 규모의 14,000개 이상의 교육 기관과 협력한 경험을 기반으로 합니다.

개요

교육 기관은 학생, 학부모, 교직원, 직원 및 커뮤니티에 차별화된 서비스와 경험을 제공하기 위해 디지털 트랜스포메이션을 진행함에 따라 다양한 기술적 의사 결정에 직면합니다. 많은 조직에서 이미 민첩성, 탄력성, 복원력, 보안 및 비용 절감을 높이기 위해 클라우드를 채택하기로 결정했습니다. 다양한 팀 간의 기존 관계와 투자를 기반으로 대부분의 조직은 온프레미스 데이터 센터, 콜로케이션 시설 및 클라우드 제공업체의 조합을 사용하고 있습니다. 여러 클라우드 옵션의 가용성을 고려할 때 교육 기관은 종종 단일, 하이브리드 및 멀티클라우드 배포 모델(클라우드 배포 전략 섹션에 정의됨) 중에서 결정해야 합니다.

2개 이상의 클라우드 서비스 제공업체가 제공하는 서비스를 사용하는 멀티클라우드는 오늘날 많은 기관에서 흔히 볼 수 있습니다. IT 팀은 하나의 클라우드 제공업체를 선호할 수 있지만 다른 그룹, 부서 또는 개별 사용자는 대체 제공업체를 선택하거나 이미 사용하고 있을 수 있습니다. 적절한 클라우드 배포 모델로 안내할 명확한 전략이 없는 교육 기관은 많은 과제에 직면합니다. 여기에는 불필요한 복잡성, 직원 수요 증가, 일관되지 않은 거버넌스, 제공업체 사이에서 공통된 기본 기능의 하위 세트로 제한하는 가장 낮은 공통 분모 접근 방식이 포함됩니다. 각 과제는 혁신을 방해하고 디지털 트랜스포메이션을 늦춥니다.

반대로 단일, 하이브리드 및 멀티클라우드를 사용하도록 안내하는 클라우드 전략이 있는 경우 장기 성공을 위해 운영상 지속 가능한 방식으로 클라우드의 이점을 실현하면서 교육 미션 요구 사항을 충족할 수 있습니다. 이 전략을 수립하려면 다음을 권장합니다.

- 기본 전략 클라우드 제공업체를 선택합니다.
- 클라우드 혁신 센터(CCoE)를 수립합니다.
- 서비스형 소프트웨어(SaaS) 애플리케이션과 기본 클라우드 서비스를 구분합니다.
- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항을 설정합니다.
- 가능하고 실현 가능하면 클라우드 네이티브 관리형 솔루션을 채택합니다.
- 기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처를 구현합니다.
- 단일 클라우드 제공업체를 통해 기술 또는 비즈니스 요구 사항을 충족할 수 없는 워크로드에 대해서만 멀티클라우드를 예약합니다.

이러한 모범 사례는 이 백서의 권장 사항 섹션에서 자세히 설명합니다. 각 권장 사항은 중요하지만 조직의 우선순위는 클라우드 채택 단계에 따라 달라집니다. 예를 들어 클라우드 채택을 막 시작하는 경우 기본 전략 클라우드 제공업체를 선택하고, CCoE를 수립하며, 클라우드 네이티브 관리형 솔루션을 채택하는 데 집중합니다. 이미 단일 클라우드 제공업체를 사용하고 있는 경우 핵심 보안 및 거버넌스 요구 사항을 설정하는 데 집중하고 기존 데이터 센터 투자가 지속적인 사용을 장려할 때 하이브리드 아키텍처를 고려합니다. 조직에서 이미 여러 클라우드 제공업체를 사용하고 있는 경우 SaaS 애플리케이션을 차별화하고 실제로 필요한 드문 워크로드에 대해 멀티클라우드 배포를 예약하는 데 집중합니다.

목차

- 클라우드 배포 전략
- 권장 사항
- 사용 사례 예
- 다음 단계
- 기여자
- 참조 자료
- 문서 기록

클라우드 배포 전략

AWS에서는 클라우드 컴퓨팅을 종량제 요금으로 인터넷을 통한 IT 리소스의 온디맨드 전송으로 정의합니다. 물리적 데이터 센터 및 서버를 구매, 소유 및 유지 관리하는 대신 필요에 따라 클라우드 제공업체로부터 컴퓨팅 성능, 스토리지 및 데이터베이스와 같은 기술 서비스에 액세스할 수 있습니다. 클라우드 컴퓨팅을 통해 교육 기관은 하드웨어 조달, 유지 관리 및 용량 계획과 같은 차별화되지 않은 부담을 피할 수 있습니다. 클라우드 솔루션을 채택하고 배포할 때 단일 클라우드, 하이브리드 클라우드, 멀티클라우드와 같은 여러 모델 중에서 선택할 수 있습니다.

단일 클라우드

이 모델은 단일 클라우드 서비스 제공업체만 사용합니다. 단일 클라우드 애플리케이션 및 워크로드는 클라우드에서 직접 구현되거나 이전에 다른 환경에서 호스팅되었다가 클라우드로 마이그레이션될 수 있습니다. 이러한 워크로드에서는 클라우드 제공업체의 하위 수준 인프라 서비스를 사용하거나 상위 수준의 관리형 서비스를 활용할 수도 있습니다. 그럼에도 불구하고 이 모델은 단일 클라우드 제공업체를 채택하고 해당 공급자의 클라우드 서비스만 사용합니다.

하이브리드 클라우드

하이브리드 클라우드 모델은 조직의 자체 온프레미스 데이터 센터와 하나 이상의 클라우드 서비스 제공업체에 리소스를 분산합니다. 일반적으로 이 모델의 목적은 온프레미스에 있는 기존 내부 시스템과의 프라이빗 연결을 유지하면서 조직의 인프라를 클라우드로 확장하는 것입니다.

멀티클라우드

멀티클라우드 모델은 두 개 이상의 클라우드 서비스 제공업체 사이에서 리소스를 배포하고 서비스를 사용합니다. 조직은 멀티클라우드를 선택할 수 있지만, 이는 개별 팀, 부서 또는 직원의 서로 다른 클라우드 제공업체에 대한 선호도 때문에 의도하지 않은 결과인 경우가 많습니다.

권장 사항

이제 단일 클라우드, 하이브리드 클라우드 및 멀티클라우드를 기본적으로 이해했으므로 이 섹션에서는 모델 선택에 대한 자세한 권장 사항을 제공합니다.

- 기본 전략 클라우드 제공업체 선택
- CCoE 설정
- SaaS 애플리케이션과 기본 클라우드 서비스 간 차별화
- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항 설정
- 가능하고 실현 가능하면 클라우드 네이티브 관리형 서비스 채택
- 기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처 구현
- 단일 클라우드 제공업체를 통해 기술 또는 비즈니스 요구 사항을 충족할 수 없는 워크로드에 대해서만 멀티클라우드 예약

기본 전략 클라우드 제공업체 선택

클라우드 채택은 IT 현대화, 비용 효율성 및 혁신에 필수적인 풍부한 이점을 제공합니다. 그러나 제한된 SaaS 애플리케이션 이외의 클라우드 기술을 채택하면 불필요한 비용과 복잡성을 방지하기 위해 교육 기관이 신중하게 계획해야 하는 문제가 발생할 수 있습니다. 클라우드에서 워크로드 구현에 수반되는 기술적 및 비즈니스 변화에는 네트워킹, 보안, 거버넌스 및 운영을 비롯한 핵심 인프라에 대한 직원의 지원과 조정이 필요합니다.

이러한 문제를 효과적으로 해결하는 가장 좋은 방법은 특히 조직이 클라우드 여정의 초기 단계에 있는 경우 대부분의 워크로드를 지원하는 전략적인 기본 클라우드 제공업체를 선택하는 것입니다. 클라우드 이점 실현을 단순화하고 가속화할 수 있도록 해당 제공업체를 중심으로 초점을 맞춘 채택부터 시작합니다. 기본 클라우드 제공업체를 선택하는 작업은 배타적이고 되돌릴 수 없는 결정이 아닙니다. 이를 통해 조직은 클라우드 채택을 반복적으로 발전시킬 수 있습니다. 먼저 몇 가지 서비스에 집중한 다음 필요한 경우 클라우드의 전반적인 이점을 지연시키지 않고 다른 클라우드 서비스로 확장할 수 있습니다. 이 접근 방식은 제공업체의 기능을 활용하고, 직원 기술과 서드 파티 파트너 관계를 집중 및 개발하며, 벤더 관리를 단순화하는 조직의 능력을 극대화합니다.

고객이 여러 클라우드 제공업체를 동시에 채택하려고 시도하면서 클라우드 여정을 시작했지만, 나중에 이러한 결정과 복잡성으로 인해 후회하는 것을 확인했습니다. Gartner는 6 Steps for Planning a Cloud Strategy 기사에서 이 인사이트를 공유합니다. 여기서 2단계는 '멀티클라우드 아키텍처에서 기본 제공업체 우선순위 지정'과 같습니다.

각 클라우드 제공업체는 여러 운영 및 지원 모델, ID 및 액세스 관리, 네트워킹, 운영, 규정 준수 기능 등을 도입합니다. 한 번에 클라우드 제공업체 하나의 운영 모델을 마스터하는 것이 좋습니다. 그런 다음 합리적 근거를 갖춘 경우 추가 클라우드 서비스를 반복적이고 점진적으로 통합할 수 있습니다. 많은 요인이 기본 클라우드 제공업체를 채택하기로 결정하는 데 영향을 미칠 수 있지만 선택을 안내하기 위해 다음 주요 질문을 사용합니다.

- 제공업체는 어떤 폭과 깊이의 서비스를 제공하나요?

  클라우드 제공업체마다 다른 서비스를 제공합니다. 최소한 기본 제공업체에 보안, 거버넌스 및 자동화와 같은 교차 운영 요구 사항뿐만 아니라 모든 기능 요구 사항을 지원하는 데 필요한 기능이 있는지 확인합니다. 혁신 및 운영 우수성에 대한 검증된 실적으로 이러한 기능을 제공하는 제공업체를 선택합니다. 애플리케이션뿐만 아니라 데이터도 고려합니다. 향후 데이터 통합 및 전송 패턴을 고려하여 제공업체 사이에서 대량의 데이터를 이동하는 데 드는 비용, 지연 시간 및 복잡성을 제한합니다. 현재 애플리케이션 및 데이터 요구 사항을 충족하고 시간이 지남에 따라 변화하는 기관의 요구 사항을 충족할 수 있는 새로운 사용 사례를 지원하기 위해 가장 포괄적이고 심층적인 제공업체를 선택합니다.
- 제공업체가 모든 보안 및 규정 준수 요구 사항을 지원할 수 있나요?

  교육 부문에서 보안 및 규정 준수는 모든 기술 배포에 매우 중요합니다. 모든 보안 및 규정 준수 요구 사항을 충족할 수 있는 클라우드 제공업체를 선택합니다. AWS Artifact와 같은 도구는 보안 및 규정 준수 보고서에 대한 온디맨드 액세스를 위한 중앙 리소스를 제공하여 제공업체를 평가하는 데 도움이 될 수 있습니다. 클라우드 제공업체 자체 인프라 및 서비스의 보안 및 규정 준수뿐만 아니라 이러한 서비스를 사용하여 안전하고 규정을 준수하는 솔루션을 설계하는 것이 얼마나 쉬운가도 고려합니다. 클라우드의 안전한 채택을 가속화하기 위해 사전 빌드된 솔루션, 빠른 시작 및 규범적 지침의 조합을 제공하는 제공업체를 우선합니다.
- 제공업체에 강력한 파트너 네트워크가 있나요?

  클라우드 트랜스포메이션만 진행하는 조직은 없습니다. 채택을 가속화하려면 클라우드 제공업체 및 파트너 네트워크의 서비스와 전문 지식을 사용해야 합니다. 이 네트워크에는 클라우드 기술을 실행, 통합 또는 지원하는 소프트웨어를 제공하는 기술 파트너와 클라우드에서 자체 애플리케이션을 설계, 빌드, 실행 및 관리하는 데 도움이 되는 컨설팅 파트너가 포함됩니다. 이미 협력하고 있는 많은 교육 기술 제공업체, 독립 소프트웨어 개발 판매 회사(ISV), 컨설턴트 및 리셀러가 클라우드 제공업체의 파트너 네트워크에 속해 있습니다. 검증된 역량의 가장 강력한 파트너 네트워크를 갖춘 클라우드 제공업체를 우선합니다. 검증된 산업 및 기술 전문 지식을 갖춘 파트너는 꼭 필요합니다.
- 제공업체는 어떤 지원과 기반을 제공하나요?

  새로운 기술을 성공적으로 채택하려면 모범 사례 권장 사항, 구성 지침, 문제 해결 등 교육 및 도움을 요청할 수 있는 메커니즘이 필요합니다. 강력한 지원 및 교육 옵션을 제공하는 클라우드 제공업체를

선택하면 성공을 위한 토대를 마련할 수 있습니다. 제공업체의 공식 지원 모델 및 리소스와 블로그, 포럼, 비디오, 사용 방법 가이드와 같은 사용 가능한 서드 파티 또는 커뮤니티 기반 리소스를 살펴봅니다. 제공업체의 기술 지원 프로그램뿐만 아니라 비즈니스 및 문화 트랜스포메이션에 초점을 맞춘 프로그램도 고려합니다. 예를 들어 AWS Cloud Adoption Framework(AWS CAF)는 기술뿐만 아니라 비즈니스 프로세스와 인력을 포함하는 관점에 집중하여 조직이 디지털 방식으로 혁신할 수 있도록 지원합니다. 광범위한 교육 옵션과 검증되고 신뢰할 수 있는 지원 모델 및 커뮤니티를 제공하는 클라우드 제공업체를 우선합니다.

CCoE 설정

트랜스포메이션 사무소 또는 클라우드 혁신 센터(CCoE)를 통해 클라우드 리더십 기능을 발전시키는 방법을 고려합니다. CCoE는 조직 전체에서 클라우드 기술을 대규모로 구현하기 위한 접근 방식을 개발하고 전파합니다. 클라우드를 성공적으로 채택하려면 관련된 팀 및 부서를 대신하여 발언할 수 있는 담당자를 포함하도록 CCoE를 설계합니다. 처음에는 작게 시작했다가 트랜스포메이션 여정을 진행하면서 필요에 맞게 CCoE를 점진적으로 발전시킵니다. AWS 계정 관리자 및 솔루션 아키텍트와 같은 기본 클라우드 제공업체 담당자가 CCoE 생성을 안내하는 리소스를 제공할 수 있습니다. CCoE는 주제 전문 지식을 확립하고, 동의를 얻으며, 조직 전체에서 신뢰를 얻고, 미션 요구 사항을 충족하기 위한 효과적인 지침을 수립하는 능력을 가속화합니다. 모든 기관에 사용할 수 있는 단일 조직 구조는 없지만, 다음 질문은 고유한 CCoE를 설계하는 데 도움이 됩니다.

- CCoE에 누가 포함되어야 하나요?

  처음에는 CCoE에 얼리어답터와 클라우드 옹호자 몇 명만 포함될 수 있습니다. CCoE는 여전히 작을 수 있지만 클라우드 채택의 영향을 받는 비즈니스 기능과 기술 기능을 모두 담당할 수 있는 옹호자를 포함하도록 발전해야 합니다. 비즈니스 기능에는 변경 관리, 이해관계자 요구 사항, 거버넌스, 교육, 조달 및 통신이 포함됩니다. 이러한 기능은 일반적으로 기관의 관리 및 교육 팀 멤버가 대표합니다. 기술 기능에는 인프라, 자동화, 운영 도구, 보안, 성능 및 가용성이 포함됩니다. 이러한 기능은 일반적으로 기관의 IT 팀 멤버가 대표합니다. 또한 CCoE는 주제 전문 지식을 제공하기 위해 필요에 따라 벤더 및 파트너를 참여시켜야 합니다. CCoE는 유기적인 조직입니다. 멤버십, 양식 및 기능은 시간이 지남에 따라 변경될 가능성이 크며 향후 성숙도 시점에 해체될 수도 있습니다.
- CCoE는 이해관계자와 어떻게 상호 작용하나요?

  CCoE는 다른 팀을 지원하며 클라우드 채택을 성공적으로 알리고 활성화하기 위해 설계되었습니다. 다양한 부서, 학교 및 기능 부문에서 CCoE의 임베딩 부분을 살펴봅니다. 이를 통해 더 광범위한 리소스에 액세스하고 내부 피드백을 더 빠르게 제공할 수 있습니다. 초기에 이해관계자 사이에서 열린 통신 라인과 파트너십 구축에 집중하여 기관 내에서 신뢰를 쌓고 조직 사일로를 해소합니다. CCoE에는 이해관계자와 소통하고, 피드백을 수집하며, 사용자를 교육하기 위한 메커니즘이 정의되어 있

어야 합니다. CCoE의 성공 지표는 이러한 협업 및 통신을 반영해야 합니다. 팀이 기술 빌드를 기준으로만 측정되는 경우 앞으로 더 많은 기술이 빌드되어도 해당 사용 및 성과는 나중의 고려 사항입니다. 대신 지표로, CCoE의 작업을 통해 자체적으로 충분한 팀 수, CCoE가 이니셔티브의 중요한 경로에 존재하는 횟수, 진행된 교육 이벤트 수 또는 CCoE 출력 채택 범위와 같은 사항을 측정해야 합니다. 잘 구성되고 신뢰할 수 있는 CCoE는 신뢰를 기반으로 구축된 더 큰 조직 트랜스포메이션을 위한 초석이 될 수 있습니다.

- CCoE를 설정하려면 어떻게 해야 하나요?

  대부분의 조직은 특정 대상 파일럿 프로젝트에서 클라우드 채택을 시작합니다. 이러한 프로젝트의 일부로 CCoE를 설정합니다. 좋은 출발은 전체 여정의 성공을 정의하는 데 매우 중요합니다.

  - 비즈니스 문제부터 시작합니다. 기술을 위한 기술은 잘못된 전략입니다. 클라우드 기술을 실험하는 경우 작은 규모라도 매력적인 비즈니스 사용 사례를 식별합니다. 그런 다음 해당 사용 사례부터 작업을 시작해 기술이 어떻게 도움이 될 수 있는지에 대한 명확한 목표를 세웁니다. 사일로에서 솔루션을 구현하지 마세요. 프로젝트 구현 이전과 도중에 비즈니스 이해관계자로부터 지속적인 의견을 구합니다. 성공적인 모든 클라우드 프로젝트는 기술을 사용할 기관 유닛과의 긴밀한 협업에 의존합니다.
  - 작게 시작합니다. 양방향 문을 제공하는 위험도가 낮은 프로젝트를 선택합니다. 즉, 프로젝트를 되돌릴 수 있으며 실수를 신속하게 수정할 수 있습니다. 파일럿 프로젝트는 모두 실험에 관한 것입니다. 대규모 고위험 프로젝트를 피하면 구현과 결과를 더 잘 제어할 수 있습니다. 광범위한 목표 대신 구체적이고 정의 가능한 문제를 대상으로 하는 데 도움이 됩니다. 예를 들어 자동화가 궁극적인 목표인 경우 전체 작업 대신 특정 태스크의 자동화를 목표로 합니다.
  - 성과를 정의하고 측정합니다. 명확한 지표를 설정하여 각 프로젝트의 진행 상황과 성과를 평가합니다. 이해관계자 간 기대치의 불일치를 방지하기 위해 원하는 종료 상태를 미리 정의합니다. 비즈니스 이해관계자 및 조직 내 다른 리더와 긴밀히 협력하여 기대치와 측정 가능한 이익을 정의합니다. 또한 결과를 비기술적 언어로 변환하는 것도 중요합니다. 프로젝트가 보존을 개선하고 이탈을 줄이는 방법, 비용을 낮추고 전달 속도를 높이는 방법 등 기관의 목표에 대해 논의합니다.
  - 안전 영역에서 시작합니다. 기관이 익숙한 도메인에서 프로젝트를 선택합니다. 그러면 프로젝트에 실제 영향을 미치는 의미 있고 이해하기 쉬운 목표가 있는지 확인할 수 있습니다. 이러한 프로젝트는 신뢰를 구축하고 조직에 대한 장기적인 결과를 선사합니다. 예를 들어 데이터 분석에 대한 전문 지식이 이미 있는 경우 분석 프로젝트로 시작하여 기존 기술을 활용하면서 클라우드 여정을 시작할 수 있습니다. 모든 기관은 여러 전문 지식을 보유하고 있으며 성공적인 디지털 트랜스포메이션 전략을 수립하려면 고유한 구성 요소를 파악해야 합니다.

SaaS 애플리케이션과 기본 클라우드 서비스 간 차별화

대부분의 교육 기관은 이미 서비스형 소프트웨어(SaaS) 애플리케이션을 채택하고 있습니다. SaaS는 서비스 제공업체가 실행하고 관리하는 완전한 솔루션을 기관에 제공합니다. 일반적인 SaaS 애플리케이션에는 단어 처리 및 이메일과 같은 생산성 애플리케이션이 포함되지만 엔터프라이즈 리소스 계획(ERP), 학생 정보 시스템(SIS), 학습 관리 시스템(LMS)과 같은 많은 미션 크리티컬 워크로드에 대한 SaaS 옵션도 있습니다. 기관이 SaaS 제품을 채택하면 IT 팀은 서비스가 어떻게 유지 관리되는지 또는 인프라가 어떻게 관리되는지에 대해 고민하지 않아도 됩니다. 사용자는 단순히 서비스를 사용하기만 하면 됩니다. 이 전달 모델은 IT 직원의 관리 부담을 줄여줍니다. 특히 IT 팀이 동일한 애플리케이션을 충분히 자체 호스팅할 시간, 리소스 또는 기술이 부족한 경우 많은 기관에서는 IT 전략에 'SaaS 우선' 접근 방식을 채택하기로 선택합니다. 자체 호스팅할 리소스가 있더라도 SaaS 솔루션을 채택하고 대신 다른 프로젝트에 투자하는 것이 여전히 비용 효율적일 수 있습니다.

SaaS 애플리케이션을 사용하는 경우 IT 팀이 기본 인프라를 관리할 필요가 없으므로 벤더는 애플리케이션(온프레미스 데이터 센터, 기본 클라우드 제공업체 또는 대체 클라우드 제공업체)을 호스팅합니다. 전략적 기본 클라우드 제공업체를 선택한 후 벤더의 데이터 센터에서 다른 클라우드 제공업체 또는 온프레미스에서 호스팅되는 SaaS 제품을 사용하기로 선택할 수 있습니다. 반대로 SaaS 애플리케이션이 한 클라우드 제공업체에서 호스팅되더라도 비SaaS 워크로드에 대한 해당 제공업체의 강점에 따라 다른 기본 전략 클라우드 제공업체를 선택할 수 있습니다. 여러 호스팅 환경을 구분하는 일은 자체 호스팅 애플리케이션보다 SaaS에서 덜 중요합니다. 하지만 SaaS가 IT 전략의 일환으로 클라우드에 어떻게 적합한지 평가할 때는 여전히 다음과 같은 주요 질문을 고려해야 합니다.

- SaaS 애플리케이션이 가용성이 높으며, 확장 가능한가요?

  많은 벤더가 이미 SaaS 오퍼링에 대해 클라우드를 채택하기로 결정했습니다. 이를 통해 벤더는 가용성 및 확장성 향상이라는 클라우드 이점을 얻을 수 있습니다. 또한 벤더는 물리적 인프라를 관리하고 유지 관리하는 대신 클라우드의 공동 책임 모델을 채택할 수 있으므로 새로운 기능을 제공하는 데 더 많은 시간과 리소스를 투자할 수 있습니다. 이러한 이점 때문에 클라우드를 우선하고 클라우드 호스팅 솔루션을 제공하는 제공업체를 선호해야 합니다.
- SaaS 애플리케이션이 보안 요구 사항을 충족할 수 있나요?

  SaaS를 평가할 경우 애플리케이션이 저장하는 데이터, 해당 데이터가 사용되는 방식, 해당 데이터를 보호하기 위해 마련된 보안 제어를 알아야 합니다. 자체 호스팅 환경에서와 마찬가지로 데이터 스토리지를 직접 제어하지 못할 수도 있지만, 벤더에 데이터를 적절하게 처리하기 위한 메커니즘과 제어가 있는지 확인해야 합니다. SaaS 솔루션에서 기본 제공되는 보안 기능과 추가 구성이 필요한 기능에 유의하세요. 클라우드를 통해 SaaS 제공업체는 가용성이 뛰어나고 확장 가능한 솔루션을 빌드할 수 있으며 공동 책임 모델로 인해 더 안전한 솔루션을 빌드할 수도 있습니다. 솔루션의 일부로 클라우드 보안 도구 및 서비스를 활용하는 제공업체를 우선해야 합니다.

- SaaS 애플리케이션 데이터는 누가 소유하며 어떻게 액세스할 수 있나요?

  SaaS를 사용하는 경우 제공업체가 기관의 데이터를 올바르게 처리한다고 신뢰합니다. SaaS 애플리케이션에 대한 서비스 약관 및 서비스 수준 계약을 검토하여 데이터 소유권, 가용성 및 내구성과 같은 기여 요인을 이해해야 합니다. 데이터 백업 또는 내보내기 메커니즘을 평가합니다. 제공업체를 전환하거나 제공업체가 서비스를 중단하는 경우에 특히 중요합니다.

- 환경에 관계없이 다른 서비스 및 자체 호스팅 애플리케이션을 SaaS 애플리케이션과 통합할 수 있나요?

  SaaS 솔루션을 채택할 경우 동일한 호스팅 환경을 공유하는 서비스 및 애플리케이션(즉, 동일한 클라우드 제공업체 또는 동일한 벤더의 데이터 센터를 사용하는 애플리케이션)이 더 원활하게 통합될 것이라고 가정하기 쉽습니다. 그러나 오늘날 대부분의 SaaS 솔루션은 API 및 서드 파티 통합을 광범위하게 지원하므로 동일한 환경에서 호스팅되는 솔루션으로 제한하지 마세요. 필요한 통합이 있는 경우 솔루션은 동일한 기본 환경을 공유하지 않아도 됩니다. 예를 들어 클라우드 기반 학생 파일 스토리지용으로 Google Drive 또는 Microsoft OneDrive와 같은 SaaS 솔루션을 사용하고 있다고 가정합니다. 학생에게 가상 데스크톱 및 애플리케이션 스트리밍을 제공하기 위해 Amazon WorkSpaces 애플리케이션이 요구 사항에 가장 적합하다고 판단할 수 있습니다. 이러한 서비스는 서로 다른 환경에서 실행되지만 WorkSpaces 애플리케이션은 Google Drive 및 Microsoft OneDrive와 기본적으로 통합되어 있으므로 학생은 기존 스토리지를 계속 사용할 수 있습니다.

- SaaS 애플리케이션이 중앙 집중식 ID 관리를 지원하나요?

  IT 팀이 서로 다른 ID 저장소를 관리할 필요가 없고 사용자가 여러 자격 증명 세트를 기억할 필요가 없도록 하려면 SaaS 솔루션이 기존 ID 관리 또는 Single Sign-On 솔루션과의 통합을 지원하는지 확인합니다. 조각화된 ID 관리는 생산성을 떨어뜨리고 권한 누적 및 약한 암호와 같은 잘못된 보안 사례로 이어질 수 있습니다. 원하는 SaaS 솔루션이 Single Sign-On 또는 기존 ID 저장소를 지원하지 않는 경우 솔루션 채택의 비즈니스 가치가 사용자 및 직원의 부담 증가보다 큰지 평가합니다.

- SaaS 애플리케이션과의 네트워크 통신을 보호하려면 어떻게 해야 하나요?

  경우에 따라 SaaS 애플리케이션과 통신하기 위해 자체 호스팅 애플리케이션이 필요할 수 있습니다. 일반적으로 이 통신은 적절한 인증 및 권한 부여 메커니즘으로 보호되는 API를 통해 이루어집니다. 그러나 두 애플리케이션의 호스팅 환경에 따라 해당 통신을 단순화하거나 보안하기 위해 대체 또는 추가 메커니즘이 필요할 수 있습니다. 예를 들어 클라우드 제공업체와 애플리케이션을 자체 호스팅하고 동일한 클라우드 제공업체에서 호스팅되는 SaaS 애플리케이션과 통합해야 하는 경우 벤더는 여러 연결 옵션을 제공할 수 있습니다. 클라우드별 피어링 연결, 프라이빗 API 또는 AWS PrivateLink와 같은 프라이빗 인터페이스를 사용하여 해당 통신이 퍼블릭 인터넷을 통과하는 것을 방지할 수 있습니다. 마찬가지로 온프레미스 애플리케이션에 AWS Direct Connect 같은 서비스를 통해

클라우드 제공업체에 대한 전용 네트워크 연결이 있는 경우 동일한 연결을 사용하여 동일한 클라우드 제공업체에서 호스팅되는 SaaS 애플리케이션과 통신할 수 있습니다.

각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항 설정

교육 기관에는 달성해야 하는 다양한 규정 준수, 거버넌스 및 사이버 보안 목표가 있습니다. 이러한 목표를 달성하지 못할 경우 기관의 평판 손실, 벌금, 랜섬, 민감한 데이터 침해, 지적 재산 도용, 미션 크리티컬 기능의 저하나 완전한 손실이 발생할 위험이 있습니다. 공동 책임 모델로 인해 클라우드 서비스를 채택하는 기관은 인프라 보안에 대한 일부 책임을 클라우드 서비스 제공업체에 오프로드하여 관리 부담을 줄일 수 있습니다. 또한 온프레미스 배포에서 사용할 수 없거나 관리하기 어렵거나 비용이 많이 드는 기능을 제공하는 목적별 클라우드 네이티브 보안 서비스의 이점을 누릴 수 있습니다. 예를 들어 웹 애플리케이션 보호를 위한 AWS WAF, 분산 서비스 거부(DDoS) 보호를 위한 AWS Shield, 위협 감지를 위한 Amazon GuardDuty 등의 서비스가 있습니다. 성공적인 클라우드 보안 및 거버넌스 전략을 통해 IT 및 보안 팀은 설계 중심의 보안을 갖춘 시스템을 빌드하는 데 집중할 수 있으며, 기관이 진화하는 미션 요구 사항에 신속하게 적응할 수 있도록 지원하고, 강사와 연구원에게 혁신적인 학습과 혁신을 위한 안전한 환경을 제공할 수 있습니다. 보안 및 거버넌스 요구 사항을 평가하려면 다음 주요 질문을 고려합니다.

- 워크로드가 부합되어야 하는 규정 준수 프레임워크는 무엇인가요?

  교육 기관은 다수의 이해관계자와 이들이 지원하는 워크로드로 인해 많은 규정 준수 프레임워크를 준수해야 합니다. 이러한 규정 준수 프레임워크로, 가족 교육 권리 및 개인정보 보호법(FERPA), 건강 보험 양도 및 책임에 관한 법(HIPAA), 연방정부의 위험 및 인증 관리 프로그램(FedRAMP), 사이버 보안 성숙도 모델 인증(CMMC), 국제 무기 거래 규정(ITAR), 미국 연방수사국 형사사법정보부(CJIS), Payment Card Industry Data Security Standard(PCI DSS)가 포함됩니다. CMMC와 같은 일부 사례에서는 관련 워크로드의 규정 준수가 인증될 때까지 연구 권한 부여 자금이 확보되지 않습니다. 각 프레임워크는 고유하며 워크로드의 하위 세트에만 적용될 수 있습니다. 어떤 워크로드가 어떤 요구 사항을 준수해야 하는지 파악하고 각 워크로드 환경에서 이러한 요구 사항을 달성할 수 있는지 확인합니다. 클라우드 환경에서는 클라우드 제공업체의 책임과 비교하여 사용자의 책임을 이해해야 합니다. 규정 준수를 달성하고 유지하는 데 필요한 지식, 리소스 및 기술 세트가 있어야 합니다.
- 혁신을 저해하지 않고 여러 클라우드 제공업체에서 규정 준수를 적용하기 위해 어떤 메커니즘을 갖추고 있나요?

  교육 기관이 클라우드를 처음 사용하는 경우 기본 전략 클라우드 서비스 제공업체를 하나 선택하고 설계 중심 보안을 갖춘 클라우드 환경을 설계, 엔지니어링 및 운영하는 방법을 이해하는 데 집중하는

것이 좋습니다. 이상적으로는 셀프 서비스 시스템에 자동으로 임베드된 보안 제어를 통해 사용자는 IT 팀의 개입을 최소화하면서 안전한 클라우드 환경을 신속하게 배포할 수 있습니다. 단일 제공업체에 집중하면 보안 및 규정 준수를 보장하기 위해 투자해야 하는 리소스 양과 시간이 제한됩니다. 가장 성공적인 기관은 대부분의 규정 준수 요구 사항을 지원할 수 있고, 강력한 파트너 네트워크를 보유하며, 사전 빌드된 규정 준수 솔루션을 제공하고, 안전한 셀프 서비스 자동화를 사용할 수 있는 클라우드 서비스 제공업체를 선택합니다. 여러 클라우드 제공업체의 보안 및 규정 준수를 보장해야 하는 경우 각 환경의 규정 준수를 관리하기 위한 기술 세트와 리소스를 빌드하려면 추가 투자가 필요합니다. 각 클라우드 제공업체가 여러 기본 환경 또는 랜딩 존을 사용하는 경우 각 랜딩 존이 지원할 수 있는 규정 준수 표준 및 요구 사항을 이해해야 하며, 이에 따라 특정 워크로드를 해당 제공업체에 호스팅할 수 있는지를 결정할 수 있습니다. 각 제공업체의 규정 준수를 별도로 관리하거나 여러 제공업체에서 관리를 중앙 집중화할 수 있는 사용자 지정 빌드 또는 파트너 솔루션을 사용할 수 있습니다. AWS Marketplace에서는 규정 준수 요구 사항을 충족할 수 있는 턴키 솔루션을 제공합니다.

- 여러 클라우드 제공업체의 비용 및 사용량을 어떻게 평가하고 제어할 수 있나요?

  교육 기관이 클라우드를 처음 사용하는 경우 비용 가시성 및 제어 메커니즘을 설정하여 사용 중인 클라우드 서비스, 클라우드 리소스가 속한 사용자, 클라우드 리소스의 목적, 소비를 최적화하여 얻을 수 있는 잠재적 비용 절감을 파악하는 것이 좋습니다. 기관은 클라우드 서비스 제공업체와 협력하여 미션 크리티컬 시스템을 마이그레이션하고 현대화함으로써 상당한 투자 수익을 달성할 수 있습니다. 이는 기업 수준의 계약을 협상하고, 대량 구매 요금을 활용하며, 클라우드 서비스 공급자의 전문 지식을 활용할 수 있기 때문입니다. 여러 제공업체의 비용 및 사용량을 제어해야 하는 경우 사내 프로세스 및 도구를 사용하거나 파트너 솔루션을 사용하여 각 제공업체의 비용 및 사용량을 집계하고 분석할 수 있는 방법을 고려합니다. 많은 조직이 클라우드 재무 운영(FinOps)을 주요 기능으로 식별하며, 클라우드 비용 관리 및 최적화를 위한 기능을 전파하고 구현하는 데 리소스를 할애하기 시작하고 있습니다.

- 시간이 지남에 따라 사용자 권한을 쉽게 관리할 수 있는 메커니즘이 있나요?

  교육 기관에서는 클라우드에 처음 접근할 때 핵심 이해관계자의 요구 사항을 이해하는 것이 좋습니다. 기관 시스템의 사용자로는 학생, 교직원, 연구원, IT 직원, 행정, 보안, 일반 대중 및 서드 파티 협업자가 포함됩니다. 이러한 사용자의 핵심 요구 사항을 식별하고 클라우드 서비스에 대한 액세스 권한을 부여하는 적절한 메커니즘이 있는지 확인해야 합니다. 서로 다른 유형의 사용자에게는 클라우드 서비스에 대한 서로 다른 유형의 액세스가 필요합니다. 예를 들어 학생, 교직원 및 일반 대중이 애플리케이션에 액세스해야 하고, IT 직원, 관리자 및 보안은 클라우드 인프라에 액세스해야 하며, 연구원 및 서드 파티 협업자는 안전한 연구 환경에 액세스해야 합니다. 교직원은 안전한 교육 환경에 액세스해야 하고 학생에게 클라우드 기술에 대한 실습 액세스를 제공하고 싶을 수도 있습니다. 자동화된 방식으로 이러한 ID를 중앙에서 관리할 수 있는 도구가 있어야 하며, 설정된 프로세스를 사용하여 역할과 책임이 시간이 지남에 따라 변화함에 따라 권한을 식별, 부여 및 취소해야 합니다.

- 새 시스템을 ID 관리 솔루션과 적절하게 통합하는 메커니즘이 있나요?

교육 기관에서는 새 시스템을 ID 관리 시스템과 쉽게 통합할 수 있는 것이 좋습니다. 이를 통해 기관은 이해관계자가 ID 관리 시스템에 쉽게 통합할 수 있는 시스템을 조달하고 빌드할 수 있도록 함으로써 다양한 미션 크리티컬 함수를 유연하게 지원할 수 있습니다. 통합 프로세스를 단순화하면 이해관계자가 자체 액세스 제어 조치를 사용할 가능성이 낮아져 Single Sign-On, 패스키 및 다중 인증(MFA)과 같은 보안 모범 사례가 적용되지 않을 수 있습니다. ID 관리 시스템이 기본 통합 또는 업계 표준 프로토콜을 통해 필요한 시스템과 상호 작용할 수 있는지 확인합니다.

- 효과적인 인시던트 감지 및 대응을 지원하는 메커니즘이 있나요?

  교육 기관은 사이버 공격 및 랜섬웨어의 대상이 되는 경우가 많습니다. 이러한 인시던트를 효과적으로 감지하고 대응하려면 양분된 접근 방식을 사용하는 것이 좋습니다.

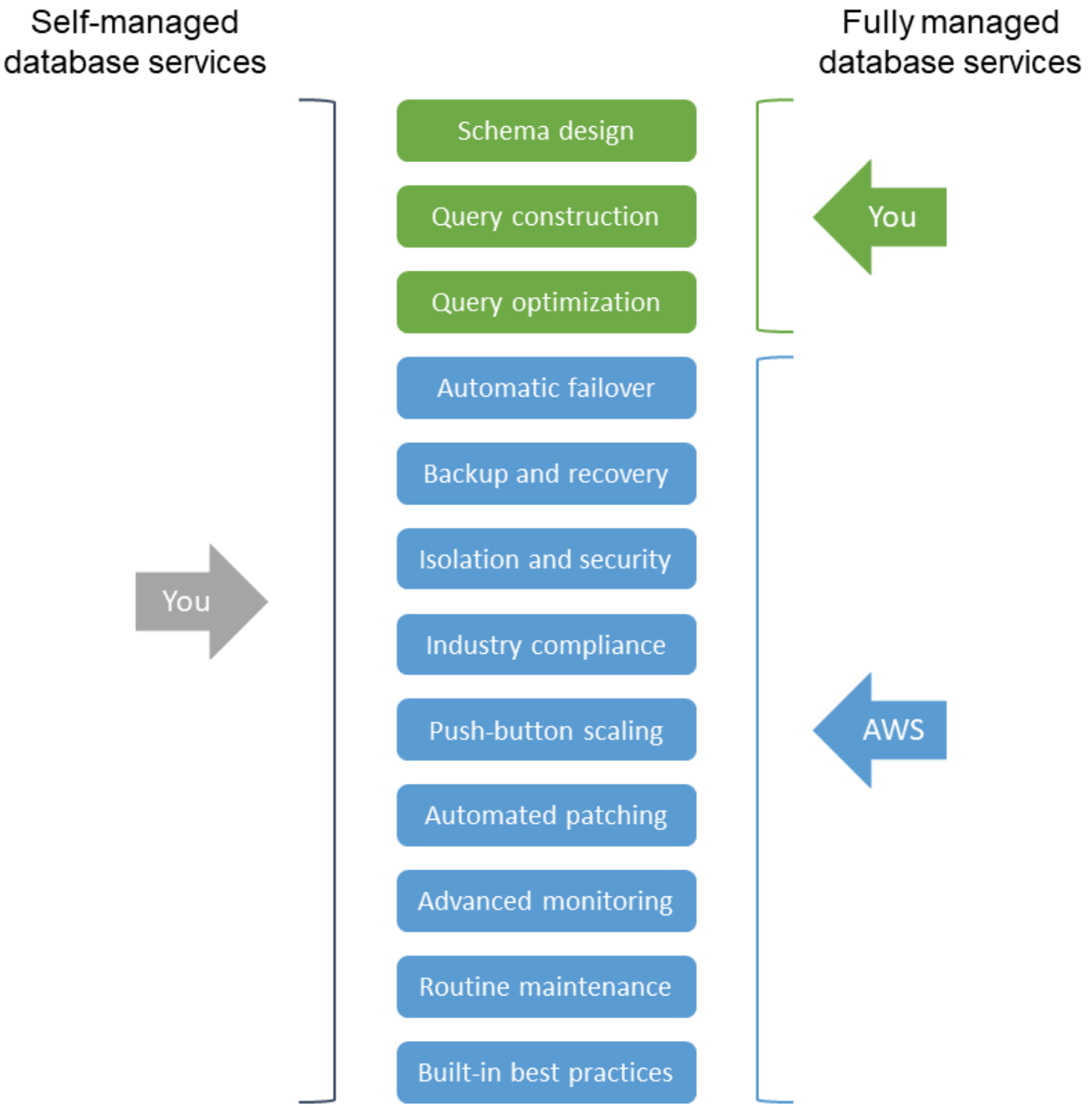
  - 클라우드 환경에 자동으로 임베드되는 보안 제어 형태의 예방 조치에 노력을 집중합니다.
  - 사이버 인시던트 대응 담당자가 적시에 보안 침해를 감지, 억제 및 완화하는 데 도움이 되는 감지 기능을 구현합니다.

규정 준수와 마찬가지로 각 환경에서 이벤트를 감지 및 방지하고 이에 대응할 수 있는 리소스, 기술 세트 및 도구가 있는지 확인해야 합니다. 하나의 기본 클라우드 제공업체에 집중하면 필요한 리소스를 제한할 수 있습니다. 성숙한 보안 운영 팀이 없는 교육 기관은 독립 소프트웨어 개발 판매 회사, 관리형 감지 및 대응 제공업체, 사이버 보안 컨설턴트를 찾아 이러한 영역에서 도움을 받아야 합니다.

가능하고 실현 가능하면 클라우드 네이티브 관리형 서비스 채택

처음에는 클라우드 서비스를 활용하는 방법을 고려할 경우 팀이 익숙한 인프라 서비스 및 개발 도구를 사용하는 것이 최선의 경로로 보일 수 있습니다. 그러나 클라우드 네이티브 관리형 서비스, 특히 서버리스 옵션을 선택하면 비용, 노력 및 복잡성을 크게 줄일 수 있습니다.

클라우드 네이티브 관리형 서비스는 직원의 시간과 노력이 필요한 많은 차별화되지 않은 IT 태스크를 제거하므로 미션 중심 활동에 해당 시간과 노력을 더 잘 소비할 수 있습니다. 또한 제공업체가 서비스의 기능을 개선하면 솔루션은 효율성, 보안, 복원력, 성능 및 기타 특성의 점진적 개선을 자연스럽게 상속합니다. 예를 들어 완전관리형 데이터베이스 서비스는 기능이 풍부한 관계형 데이터베이스 관리 시스템이지만 데이터베이스가 실행되는 기본 서버와 운영 체제를 프로비저닝하고 관리할 필요가 없습니다. 이를 통해 자체 데이터 센터 또는 클라우드에서 프로비저닝하는 자체 관리형 가상 서버에서 관계형 데이터베이스를 유지 관리할 때 일반적으로 필요한 관리 태스크가 제거됩니다. 다음 다이어그램에서는 이 차이를 보여줍니다.



클라우드 네이티브 관리형 서비스를 유사한 자체 관리형 접근 방식과 비교할 경우 인프라 관리 제거의 이점은 명확합니다. 따라서 구매했거나 맞춤 개발한 애플리케이션이 실행하는 구성 요소를 배포해야 할 때마다 클라우드 네이티브 관리형 서비스를 사용하여 시간과 노력을 줄여야 합니다.

팀이 클라우드에서 솔루션을 빌드, 배포 또는 관리할 책임이 있는 경우 클라우드 네이티브 관리형 서비스를 사용하여 클라우드 제공업체의 차별화된 기능과 혁신을 최대한 활용합니다. 이 전략을 사용하면

이러한 프로젝트에 필요한 시간과 노력을 줄이는 동시에 복원력과 보안을 높이는 방식으로 클라우드 서비스를 선택, 통합 및 배포할 수 있습니다. 성공적인 클라우드 전략을 위해서는 사용자 지정 솔루션을 클라우드로 마이그레이션하거나, 클라우드에서 새 솔루션을 개발하거나, 클라우드에 라이선스 소프트웨어를 배포할 때 이러한 클라우드 네이티브 구성 요소를 채택하는 것이 좋습니다. 클라우드 네이티브 관리형 서비스에 대한 옵션을 평가할 경우 다음 주요 질문을 고려합니다.

- 교육 미션의 핵심인 기능에 직원의 시간과 노력을 더 집중해야 하나요?

  가상 서버라 하더라도 서버를 관리하려면 시스템 소프트웨어 업그레이드 및 패치를 통해 최신 상태를 유지할 수 있도록 시간과 주의가 필요합니다. 이러한 태스크를 처리하는 관리형 서비스를 사용하면 IT 직원이 조직의 미션에 더 직접적으로 부합하는 활동에 시간을 할애할 수 있습니다. 예를 들어 컨테이너를 배포해야 하는 경우 서버를 구성하고 유지 관리할 필요가 없도록 AWS Fargate와 같은 서버리스 관리형 서비스를 고려합니다. 기본 인프라를 조달, 프로비저닝 및 관리할 필요가 없으므로 대신 새로운 기능을 제공하고, 성능을 최적화하며, 사용자 경험을 개선하는 데 집중할 수 있습니다. 자체 관리형 옵션을 기준으로 관리형 서비스를 평가할 경우 이 이점을 고려합니다.
- 팀이 클라우드 네이티브 관리형 서비스를 채택하는 데 필요한 노력은 무엇인가요?

  클라우드 네이티브 관리형 서비스를 사용하여 솔루션을 설계하고 구현하는 데는 학습 곡선이 발생할 수 있지만, 솔루션 수명 주기 동안 비용, 시간 및 복잡성을 줄어들기 때문에 이러한 노력을 들일 가치가 충분합니다. 클라우드 컴퓨팅의 온디맨드 종량제 특성으로 인해 클라우드 네이티브 서비스를 사용하면 선결제 투자를 피하면서 보다 민첩한 방식으로 빠르게 반복하고 실험할 수 있습니다. 이를 통해 혁신이 증가하고 프로젝트 타임라인이 단축됩니다. 그러나 이러한 이점을 효과적으로 실현하려면 서비스별 API를 수용하기 위해 코드 리팩터링 및 최적의 사용 패턴에 대한 직원 훈련과 같은 서비스를 채택하고 사용하는 데 필요한 요소를 고려합니다. 서비스가 업계 표준 또는 오픈 소스 API를 사용하더라도 기능 차이 또는 버전 불일치를 처리하도록 애플리케이션을 리팩터링하거나 구성해야 할 수 있습니다.
- 현재 인프라를 어떻게 배포하고 관리하나요? 해당 제어 수준을 유지 관리해야 하나요?

  베어 메탈 호스트, 가상 머신, 관리형 컨테이너 서비스, 서버리스 제품 등 클라우드에서 인프라를 호스팅하고 관리하는 다양한 방법이 있습니다. 현재 온프레미스 환경에서 가상 머신 또는 컨테이너와 같은 유사한 인프라를 사용하고 있더라도 대체 접근 방식이 특정 워크로드에 적합한지 고려합니다. 예를 들어 가상 머신에서 모든 애플리케이션을 실행하는 대신 애플리케이션을 컨테이너화하고 Amazon Elastic Container Service(Amazon ECS)와 같은 관리형 컨테이너 서비스를 활용하는 것이 좋습니다. 이 경우 리팩터링이 필요할 수 있지만 AWS App2Container와 같은 도구를 사용하여 컨테이너화를 단순화하고 지원할 수 있습니다. 이 단계를 한 단계 더 진행하면 모든 구성 요소에 서버 또는 컨테이너를 배포하는 대신 전체 서버리스 옵션을 고려합니다. 서버리스 기술은 자동 규모 조정, 기본 제공 고가용성, 사용량에 따른 결제 모델을 제공하여 민첩성을 높이고 비용을 최적화합니다. 동

시에 서버를 관리하고 용량을 계획하지 않아도 됩니다. AWS Lambda와 같은 서버리스 컴퓨팅 서비스는 서버리스 아키텍처의 핵심입니다. Lambda는 일반적인 프로그래밍 언어를 지원하며, 이를 ㅌ오해 개발자는 인프라를 관리하는 대신 애플리케이션 코드에 집중할 수 있습니다. 각 워크로드에 대한 이러한 옵션을 살펴보고 학습 곡선, 관리 오버헤드, 비용 및 라이선스와 같은 요소를 고려합니다.

- 라이선스가 부여된 소프트웨어의 인프라를 배포하고 관리해야 하나요?

  독립 소프트웨어 개발 판매 회사(ISV)로부터 라이선스가 부여된 소프트웨어를 배포하고 관리하는 경우 클라우드 인프라를 사용한 온프레미스 배포를 모방하는 것이 논리적인 것처럼 보일 수 있습니다. 예를 들어 온프레미스 가상 머신을 클라우드 호스팅 가상 머신으로 대체하는 방법을 고려할 수 있습니다. 이는 실행 가능한 옵션이지만 아키텍처의 구성 요소를 클라우드 네이티브 관리형 서비스로 바꿀 수 있는지 여부를 고려합니다. 예를 들어 동일한 데이터베이스 엔진을 실행하는 동안 관리 부담을 줄이는 완전관리형 데이터베이스 서비스로 자체 관리형 데이터베이스 서버를 교체할 수 있습니다. 많은 ISV에서 이미 관리형 서비스를 활용하는 클라우드 아키텍처를 사용하고 있으며 배포를 단순화하기 위해 사전 빌드된 템플릿을 제공할 수도 있습니다. 가능하면 클라우드 배포에 대한 규범적 지침과 지원을 제공하는 ISV를 우선해야 합니다. 클라우드에 라이선스가 부여된 소프트웨어를 배포하기 전에 ISV에 문의하여 클라우드 환경 라이선스가 온프레미스 라이선스와 어떻게 다를 수 있는지 파악해야 합니다.

- 관리형 서비스를 사용하면 벤더 종속이 발생할 수 있다는 점이 우려되나요?

  많은 클라우드 네이티브 관리형 서비스가 일반적인 업계 표준 및 API를 지원하도록 빌드됩니다. 예를 들어 AWS Glue 및 Amazon EMR과 같은 분석 서비스는 Apache Spark 및 Apache Parquet와 같은 업계 표준 처리 및 스토리지 프레임워크를 기반으로 빌드됩니다. AWS Lambda는 기본적으로 Java, Go, Microsoft PowerShell, Node.js, C#, Python 및 Ruby 코드를 지원합니다. Amazon Relational Database Service(Amazon RDS)는 SQL Server, Oracle, PostgreSQL, MySQL 등 여러 버전의 공통 데이터베이스 엔진을 지원합니다. 서비스에 독점 API가 있는 경우 클라우드에 구애받지 않는 공통 프로토콜을 사용하여 네이티브 또는 파트너 솔루션을 통해 API와 상호 작용할 수 있습니다. 예를 들어 Amazon Simple Storage Service(Amazon S3)에는 직접 통합을 위한 서비스별 API가 있지만 AWS Storage Gateway를 사용할 때 Network File System(NFS), Server Message Block(SMB), Internet Small Computer Systems Interface(iSCSI)와 같은 표준 스토리지 프로토콜을 사용하여 상호 작용할 수도 있습니다. 운영 오버헤드를 최대한 줄이면서 요구 사항을 가장 잘 충족하는 클라우드 네이티브 관리형 서비스를 선택하는 데 계속 집중해야 하지만 일반적인 사용 가능한 업계 표준 및 프로토콜을 만들거나 사용하는 서비스를 선호할 수 있습니다.

기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처 구현

대부분의 교육 기관은 엔터프라이즈 애플리케이션, 데이터 스토리지 솔루션, 최종 사용자 컴퓨팅(EUC) 환경 및 공유 컴퓨팅 리소스를 호스팅하기 위해 다양한 규모의 온프레미스 데이터 센터에 투자합니다. 이러한 데이터 센터의 모든 리소스에는 향후 성장을 고려하고 최대 규모를 수용할 수 있는 충분한 용량(한 해에 몇 번 정도만 필요할 수 있음)을 프로비저닝해야 하는 다양한 새로 고침 주기가 적용됩니다. 따라서 리소스는 다음 새로 고침 주기까지 유휴 상태로 유지되곤 합니다. 새 하드웨어에 대한 계획, 예산 책정, 조달 및 배포에 몇 주가 걸릴 수 있습니다. 아니면 몇 달 이상이 걸릴 수 있습니다. 이 긴 프로세스는 혁신을 방해하고 학습 및 연구를 지연시킬 수 있습니다.

클라우드 컴퓨팅은 이러한 많은 문제를 해결합니다. 클라우드는 온디맨드, 종량제 IT 리소스를 제공하므로 대규모 선결제 계획 및 투자 없이도 현재 용량을 실제 수요와 더 근사하게 맞출 수 있습니다. 그러나 온프레미스 하드웨어 및 리소스에 이미 상당한 투자를 한 경우 하이브리드 모델의 클라우드 기술을 사용하여 이러한 리소스를 효율적으로 활용하고 필요에 따라 강화해야 합니다.

성공적인 하이브리드 클라우드 전략은 기존 투자를 활용하면서 해당 투자만으로 지원할 수 있는 것보다 더 큰 민첩성, 확장성 및 신뢰성을 제공합니다. 다음 고려 사항은 시작하는 데 도움이 될 수 있습니다.

- 새 워크로드를 호스팅해야 하는 경우 클라우드를 우선적으로 고려하나요?

  퍼블릭 및 프라이빗 클라우드 인프라를 함께 사용하는 방법에서는 하이브리드 클라우드 전략을 정의합니다. 클라우드 우선 접근 방식은 클라우드가 모든 워크로드에 더 적합한 선택임을 의미하지 않습니다. 그러나 새 워크로드를 계획할 경우 클라우드를 첫 번째 옵션으로 평가합니다. 특히 새로운 기술이 필요하거나 온프레미스에서 사용할 수 있는 스토리지 및 컴퓨팅 용량을 초과하는 워크로드의 경우 더욱 그렇습니다. 일시적이고 일관되지 않은 사용 패턴이 있거나, 빠른 결과가 필요하거나, 쉽게 이동할 수 있거나, 최신 하드웨어가 필요한 워크로드는 클라우드의 확장성과 탄력성을 위한 이상적인 후보입니다. 또한 사용 가능한 용량이 있더라도 온프레미스에서 사용할 수 없는 클라우드 네이티브 관리형 서비스에서 워크로드가 이점을 얻을 수 있는지 고려합니다.
- 새로운 투자를 할 때 온프레미스 환경의 TCO를 이해하고 CFO와 협력하나요?

  자체 온프레미스 데이터 센터를 유지 관리하는 실제 총 소유 비용(TCO)을 이해하는 것이 좋습니다. 하드웨어, 소프트웨어 및 지원뿐만 아니라 시설, 유틸리티, 보험 및 직원 근무 시간을 포함하여 온프레미스 인프라 소유 및 운영과 관련된 많은 숨겨진 비용이 있습니다. 이러한 비용은 직원 생산성, 운영 복원력 및 비즈니스 민첩성에 부정적인 영향을 미칠 수 있습니다. 현재 라이선스 구조와 갱신 및 유지 관리 기간도 평가합니다. 최고 재무 책임자(CFO)와 협력하여 새로운 투자를 계획할 때 숨겨진 모든 비용을 식별할 수 있습니다. 일부 라이선스는 클라우드에서 Bring Your Own License(BYOL) 옵

션을 제공하거나 클라우드 서비스에 다소 유용할 수 있습니다. 현재 인프라의 실제 TCO를 이해하면 조직의 총 TCO에 가장 큰 영향을 미치는 워크로드에 대한 클라우드 채택의 우선순위를 정하는 데 도움이 됩니다. AWS 계정 팀은 온프레미스 TCO를 더 잘 이해하는 데 도움이 되는 도구를 즉시 사용할 수 있습니다.

- 하이브리드 배포를 지원하는 데 필요한 인프라는 무엇인가요?

  하이브리드 모델을 성공적으로 채택하려면 기본 네트워크, 보안 및 인프라 도구가 필요합니다. 클라우드 제공업체와 적절한 네트워크 연결을 유지할 수 있는지 확인합니다. 이는 기존 인터넷 연결, 가상 프라이빗 네트워크(VPNs), Direct Connect서드 파티 연결 공급자와 같은 전용 연결, Internet2 및 리전별 연구 및 교육 네트워크의 조합을 통해 이루어질 수 있습니다. 온프레미스 및 클라우드 환경에서 ID 및 액세스 관리를 통합했는지 확인합니다. 일관된 보안, 비용 및 사용 가드레일을 적용하기 위한 도구와 프로세스를 설정합니다.

- IT 직원이 하이브리드 배포를 운영할 준비가 되었나요?

  클라우드 서비스에는 팀에 없을 수 있는 특정 스킬 세트가 필요할 수 있습니다. 효과적인 클라우드 채택을 위해 IT 직원의 역량을 강화하는 데 필요한 교육과 지원을 줄이기 위해 클라우드 제공업체가 온프레미스 및 클라우드에서 기존 기술 세트를 재사용하고 이를 기반으로 빌드하는 서비스를 제공하는지를 고려합니다. 예를 들어 Kubernetes에 익숙하다면 Amazon Elastic Kubernetes Service(Amazon EKS) 또는 Amazon EKS Anywhere 사용을 고려할 수 있습니다. NetApp에 익숙하다면 Amazon FSx for NetApp ONTAP 사용을 고려할 수 있습니다. 마찬가지로 사용하는 기존 파트너 솔루션이 클라우드 환경에 대한 네이티브 통합 또는 지원을 제공하는지도 고려합니다.

- 온프레미스에서 클라우드로 장기 스토리지 또는 사용량이 적은 컴퓨팅을 오프로드할 수 있나요?

  클라우드 스토리지는 장기 데이터 스토리지를 위한 몇 가지 비용 효율적인 옵션을 제공합니다. 예를 들어 Amazon Simple Storage Service(Amazon S3)는 다양한 사용 사례에 최적화된 다양한 스토리지 티어를 제공합니다. 기관에서 특정 데이터를 장기간 보관해야 하는 경우 Amazon Glacier와 같은 콜드 스토리지 솔루션을 고려합니다. 이 데이터를 클라우드 스토리지로 오프로드하면 중요한 고성능 온프레미스 스토리지가 확보될 수 있습니다. AWS Storage Gateway와 같은 서비스를 사용하면 온프레미스 애플리케이션이 SMB, NFS 및 iSCSI와 같은 표준 프로토콜을 통해 클라우드 스토리지 계층에 쉽게 액세스할 수 있습니다. 마찬가지로 사용 빈도가 낮거나 사용량이 적은 컴퓨팅 작업을 오프로드하는 것이 좋습니다. 이러한 태스크 전용 온프레미스 서버가 있는 경우 확장 가능한 클라우드 컴퓨팅 서비스를 대신 사용할 수 있습니다. 이 서비스에서는 리소스가 온디맨드로 프로비저닝되고 사용한 만큼만 비용을 지불합니다. 이러한 저비용, 장기 스토리지 및 사용량이 적은 컴퓨팅 옵션도 백업 및 재해 복구에 클라우드를 이용할 경우의 이점입니다. 클라우드에서 안전하고 내구성이 뛰어나며 확장 가능한 스토리지 및 컴퓨팅을 사용하여 필요한 스토리지 및 컴퓨팅 인프라를 직접 유지 관리할 필요 없이 재해 발생 시 데이터를 보호하고 신속하게 복구할 수 있습니다.

- 온프레미스에서 실험하고 혁신할 수 있는 충분한 용량이 있나요?

고정 크기의 온프레미스 환경에서 탄력성과 민첩성이 부족하면 사용자가 사용할 수 있는 서비스와 기술이 제한될 수 있습니다. 새로 고침 주기가 엄격한 경우 새 워크로드는 구현을 위해 다음 주기까지 기다려야 할 수 있습니다. 이 운영 모델은 실험을 제한하고 혁신을 늦출 수 있습니다. 테스트해야 하는 새 워크로드 또는 새로운 워크로드가 있는 경우 확장 가능하고 탄력적인 클라우드 서비스를 사용하는 방법을 고려합니다. 클라우드 리소스는 온디맨드로 프로비저닝 및 프로비저닝 해제할 수 있으며 사용한 만큼만 비용을 지불하면 되므로 조직의 위험을 최소화하면서 빠르게 실패하고 실험하고 실패할 수 있습니다.

- 온프레미스에서 데이터를 유지해야 하는 고유한 규정 준수 또는 성능 요구 사항이 있나요?

  데이터 레지던시 또는 지연 시간 요구 사항이 엄격한 워크로드의 경우 데이터를 온프레미스에 보관하거나 사용자에게 최대한 가깝게 유지해야 할 수 있습니다. 이러한 사용 사례의 경우 기존 온프레미스 리소스의 사용을 우선할 수 있습니다. 그러나 클라우드 제공업체가 온프레미스에서 클라우드 기반 기술을 사용하기 위한 엣지 서비스 또는 메커니즘을 제공하는지를 고려합니다. 엣지 서비스는 자체 엔드포인트에 더 가까운 위치에서 데이터 처리, 분석 및 스토리지를 제공하며 표준 클라우드 제공업체 데이터 센터 외부에 도구를 배포할 수 있습니다. 예를 들어 AWS는 최종 사용자에게 더 가까운 특정 위치에 애플리케이션을 배포하기 위해 AWS 로컬 영역 및 AWS Wavelength와 같은 서비스를 제공합니다. AWS Outposts, AWS Storage Gateway, Amazon ECS Anywhere, Amazon EKS Anywhere와 같은 서비스를 사용하여 클라우드 서비스와 기능을 기존 데이터 센터로 가져올 수도 있습니다.

단일 클라우드 제공업체를 통해 기술 또는 비즈니스 요구 사항을 충족할 수 없는 워크로드에 대해서만 멀티클라우드 예약

멀티클라우드란, 둘 이상의 여러 클라우드 서비스 제공어체가 제공하는 클라우드 서비스를 사용하는 것을 말합니다. 멀티클라우드 전략을 사용하면 여러 클라우드 제공업체의 차별화된 기능을 잠금 해제하는 옵션 또는 단일 클라우드 제공업체가 수용할 수 없는 데이터 주권 요구 사항을 충족하는 기능과 같은 특정 이점을 제공할 수 있습니다. 그러나 사용하는 각 제공업체에 대해 해당 제공업체를 효과적으로 사용할 수 있는 적절한 사람, 기술, 교육 및 도구 세트가 있는지 확인합니다. 또한 특정 워크로드에 대해 멀티클라우드 전략을 사용하려면 각 클라우드 제공업체의 필수 서비스를 통합하고 상호 운용하기 위한 추가 리소스가 필요합니다. 이점이 증가한 투자보다 큰 경우에만 멀티클라우드를 고려하는 것이 좋습니다. 멀티클라우드 전략을 선택해야 하는지 여부를 결정하려면 다음 주요 질문을 고려합니다.

- 여러 클라우드 제공업체가 제공하는 서비스를 탐색할 수 있는 리소스와 기술이 있나요?

  여러 클라우드 제공업체가 다양한 제품과 서비스를 제공하는 경우 직원에게는 각 제공업체의 기능을 탐색하는 데 필요한 필수 기술이 필요합니다. 클라우드 제공업체 하나의 서비스만 사용하는 경우

사용 중인 서비스 및 기능에 따라 직원을 위한 기술 향상 및 교육이 필요할 수 있습니다. 멀티클라우드 전략을 고려하는 경우 기존 리소스를 평가하여 여러 클라우드 제공업체의 서비스를 효과적으로 사용하는 데 필요한 추가 기술 세트를 결정합니다. 단일 클라우드 제공업체에 필요한 것 이상으로 인력을 보강하거나 기술 향상 및 교육에 추가 시간과 비용을 투자해야 할 수 있습니다. 다른 클라우드 제공업체를 사용하는 개별 팀 또는 사용자가 이미 있는 경우 사례별로 기본 클라우드 제공업체에 통합할 때 얻을 수 있는 조직의 이점을 고려합니다.

- 특정 멀티클라우드 아키텍처로 인해 새로 생기는 추가 오버헤드는 무엇인가요?

  멀티클라우드의 일반적인 동인은 다른 클라우드 제공업체의 서비스와 차별화할 수 있는 기능을 갖춘 한 제공업체의 특정 관리형 서비스를 사용하려는 바람입니다. 예를 들어 인프라 요구 사항에 대해 하나의 클라우드 제공업체를 사용하고 도메인 및 디렉터리 서비스에 대해 다른 제공업체의 관리형 서비스를 사용할 수 있습니다. 그러나 단일 관리형 서비스가 관리 부담을 줄이고 해당 아키텍처 구성 요소의 관리를 단순화하더라도 코드 리팩터링, 프라이빗 연결 요구 사항 또는 수동 통합 작업과 같은 다른 워크로드에 추가 오버헤드가 발생할 수 있습니다. 이 추가 오버헤드를 미리 식별하고 차별화된 서비스를 통해 팀이 얻는 이점을 상쇄하거나 절충하지 않도록 하세요.

- 여러 클라우드 제공업체 사이에서 모니터링 및 관리를 중앙 집중화하려면 어떻게 해야 하나요?

  다양한 클라우드 제공업체의 리소스를 사용하여 애플리케이션과 기능을 배포하기 시작할 경우 이러한 리소스에 태그를 지정하고, 모니터링하며, 관리하는 방법을 고려합니다. 각 제공업체에는 다른 환경으로 확장할 수 있는 자체 도구가 있습니다. 예를 들어 Amazon CloudWatch를 사용하여 단일, 하이브리드 및 멀티클라우드 환경에서 주요 지표 및 로그를 모니터링하고, 경보를 생성하며, 애플리케이션 및 인프라를 시각화할 수 있습니다. 또한 AWS Systems Manager를 사용하여 리소스 가시성 및 제어를 개선하고, 운영 문제를 신속하게 진단 및 해결하며, 환경 전체에서 가상 머신 업데이트 및 패치 적용과 같은 프로세스를 자동화할 수 있습니다. 제공업체의 도구가 지원할 수 없는 요구 사항이 있는 경우 파트너 솔루션을 탐색할 수 있지만 이로 인한 추가 비용 또는 통합 노력이 추가될 수 있습니다.

- 다른 클라우드 제공업체를 사용할 경우 자동화를 통해 인프라를 코드로 관리하려면 어떻게 해야 하나요?

  클라우드에서 리소스를 실행하면 리소스의 자동화된 프로비저닝 및 관리를 통해 다양한 환경을 효율적으로 관리할 수 있습니다. API와 네이티브 자동화 도구는 클라우드 제공업체마다 다릅니다. 가능하면 여러 클라우드 제공업체 리소스를 수용할 수 있는 일반적인 오케스트레이션 및 배포 도구 세트를 사용하는 방법을 고려합니다. 이를 통해 유연성이 향상되고 여러 클라우드에서 작업이 단순화됩니다. 그러나 각 제공업체의 네이티브 자동화를 별도로 사용하고 적절한 사용을 보장하기 위해 조직 프로세스를 설정하는 과정이 더 간단할 수 있습니다.

- 각 클라우드 제공업체가 충족해야 하는 규정 준수 및 규제 요구 사항이 있나요?

데이터를 저장하고 처리하는 방법을 결정하는 규제 고려 사항이 있을 수 있습니다. 클라우드 제공업체의 각 클라우드 환경에 자동으로 적용할 수 있는 정책(예: 네트워크 트래픽, 스토리지 및 보안)을 표준화하는 데 중점을 둡니다. 애플리케이션이 데이터와 통신하는 방법을 고려하고 동일한 제공업체에 애플리케이션을 호스팅합니다. 애플리케이션과 해당 데이터가 여러 제공업체에서 분할된 경우 규정 준수 및 규제 요구 사항을 충족하는지 확인하기 어렵습니다. 네트워크 지연 시간을 최소화하고, 데이터 처리량을 극대화하며, 데이터 송신을 제한하는 동시에 보안 및 액세스 제어를 단순화하기 위해 애플리케이션을 가능한 한 데이터에 가깝게 두는 것이 가장 좋습니다.

- 클라우드 제공업체에 애플리케이션을 배포할 경우 TCO를 최소화하고 요금 할인을 극대화할 수 있나요?

  멀티클라우드를 염두에 둘 경우 총 소유 비용(TCO)을 고려하는 것이 중요합니다. 여러 클라우드 제공업체에서 애플리케이션을 실행하면 각 환경에서 리소스를 유지 및 관리하는 데 운영 비용과 관리 오버헤드가 증가할 수 있습니다. 또한 여러 제공업체에 사용량을 분산하면 특정 제공업체의 대량 구매 요금 할인 또는 엔터프라이즈 계약을 활용하기 더 어려워집니다. 멀티클라우드의 이점이 늘어난 TCO의 근거가 될 수 있는지를 판단할 때 이러한 요소를 고려합니다.

사용 사례 예제

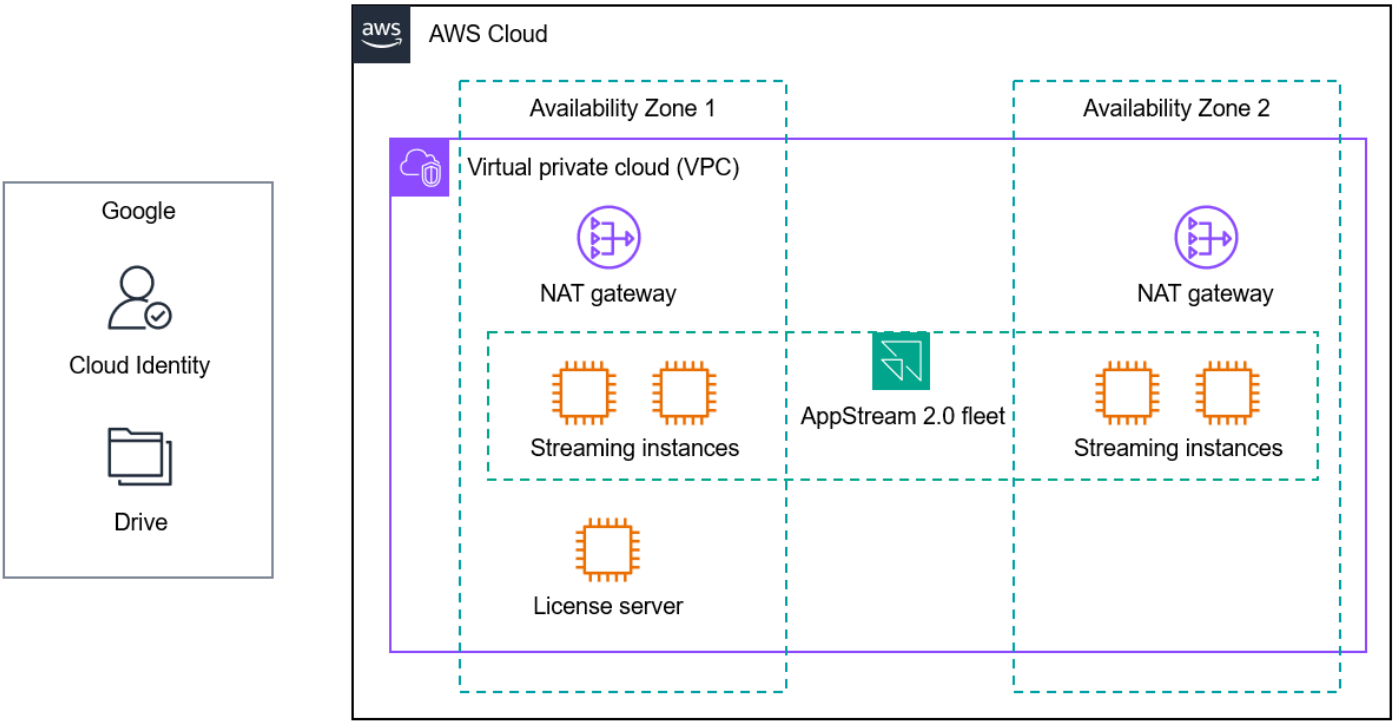
다양한 시나리오에서 이러한 원칙의 적용을 더 잘 이해하기 위해 몇 가지 사용 사례에 대해 살펴보겠습니다. 이러한 사용 사례는 실제 교육 기관이 클라우드 서비스를 채택하는 방식을 기반으로 합니다.

- 가상 컴퓨터 랩
- 학생 성공 예측
- ID 페더레이션 및 Single Sign-On
- 연구 컴퓨팅을 위한 클라우드 버스팅

가상 컴퓨터 랩

웹 기반 학습 도구의 인기와 노트북, Chromebook 및 태블릿과 같은 사용자 디바이스의 풍부함에도 불구하고 대부분의 교육 기관은 리소스 집약적 또는 레거시 애플리케이션을 위한 물리적 컴퓨터 실습을 유지합니다. 이러한 컴퓨터 랩은 종종 과학, 기술, 엔지니어링 및 수학(STEM), 직업 및 기술 교육(CTE), 미디어 및 아트, 엔지니어링 및 유사한 커리큘럼에 필요합니다. 학교는 물리적 컴퓨터 랩을 클라우드 기반 가상 데스크톱 또는 애플리케이션 스트리밍 서비스로 보강하거나 교체하여 모든 학생이 언제 어디서나 모든 디바이스에서 필요한 애플리케이션에 액세스할 수 있도록 할 수 있습니다. 이를 통해 디지털 형평성을 개선하고, 원격 학습을 활성화하며, 일관된 사용자 환경을 보장하고, 비용을 절감하면서 원격 액세스를 보호할 수 있습니다.

기본 및 보조(K12) 교육에서 많은 미국 학교는 완전 관리형 데스크톱 및 애플리케이션 스트리밍 서비스인 Amazon WorkSpaces 애플리케이션을 사용하여 가상 컴퓨터 랩을 제공하여 Adobe Creative Cloud, Autodesk 소프트웨어, STEM 및 Project Lead the Way(PLTW)와 같은 CTE 커리큘럼에 대한 액세스를 제공합니다. 많은 K12 조직이 이미 SaaS 애플리케이션인 Google Workspace 및 Google Drive를 통해 학생 Single Sign-On 및 파일 스토리지를 관리하고 있습니다. 이러한 기관은 SAML 2.0 페더레이션을 통해 Google Workspace와 WorkSpaces 애플리케이션 간에 Single Sign-On을 설정할 수 있습니다. 또한 학생이 기존 스토리지를 사용할 수 있도록 WorkSpaces 애플리케이션과 Google Drive 간의 기본 통합을 구성할 수 있습니다. 다음 다이어그램은이 사용 사례에 대한 WorkSpaces 애플리케이션 배포를 보여줍니다.



이 아키텍처는 다음 권장 사항을 따릅니다.

- 전략적 기본 클라우드 제공업체를 선택합니다. 이 아키텍처에서는 하나의 기본 클라우드 제공업체의 클라우드 서비스를 사용합니다. 동일한 제공업체에 호스팅되지 않는 SaaS 애플리케이션과의 통합이 포함되어 있지만 이러한 통합은 간단한 구성을 통해 수행됩니다. 클라우드 전문 지식과 기술 세트는 기본 클라우드 제공업체의 서비스를 배포하고 관리하는 데만 필요합니다.
- SaaS 애플리케이션과 기본 클라우드 서비스를 구별합니다. Google Workspace 및 Google Drive는 AppStream 2.0과 동일한 클라우드 제공업체에서 호스팅되지 않지만 이 배포는 필요한 통합을 제공하므로 이는 허용 가능합니다. Single Sign-On은 중앙 집중식 ID 관리를 지원하며 SAML 2.0을 통해 안전하게 구성됩니다. 학생을 위해 영구 클라우드 스토리지를 활성화하려면 Google Drive 및 WorkSpaces 애플리케이션에서 간단한 구성 변경이 필요합니다.
- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항을 설정합니다. 이 아키텍처에 사용되는 서비스 및 통합은 기관의 보안 및 거버넌스 요구 사항을 충족하는 데 도움이 됩니다. 스트리밍 트래픽은 암호화됩니다. Google Workspace를 통한 페더레이션을 사용하면 중앙 집중식 ID 관리를 수행할 수 있습니다. Amazon Virtual Private Cloud(Amazon VPC)와 같은 네트워크 서비스는 서브넷, 라우팅 및 방화벽의 구성을 지원합니다. DNS 구성, 에이전트, 가상 어플라이언스 또는 Amazon Route 53 Resolver DNS 방화벽과 같은 관리형 서비스를 사용하여 콘텐츠를 필터링할 수 있습니다. 와 같은 서비스를 사용하여 WorkSpaces 애플리케이션을 호스팅하는 AWS 계정이 표준 조직 가드레일 및 제어를 준수하도록 AWS Control Tower 할 수 있습니다.

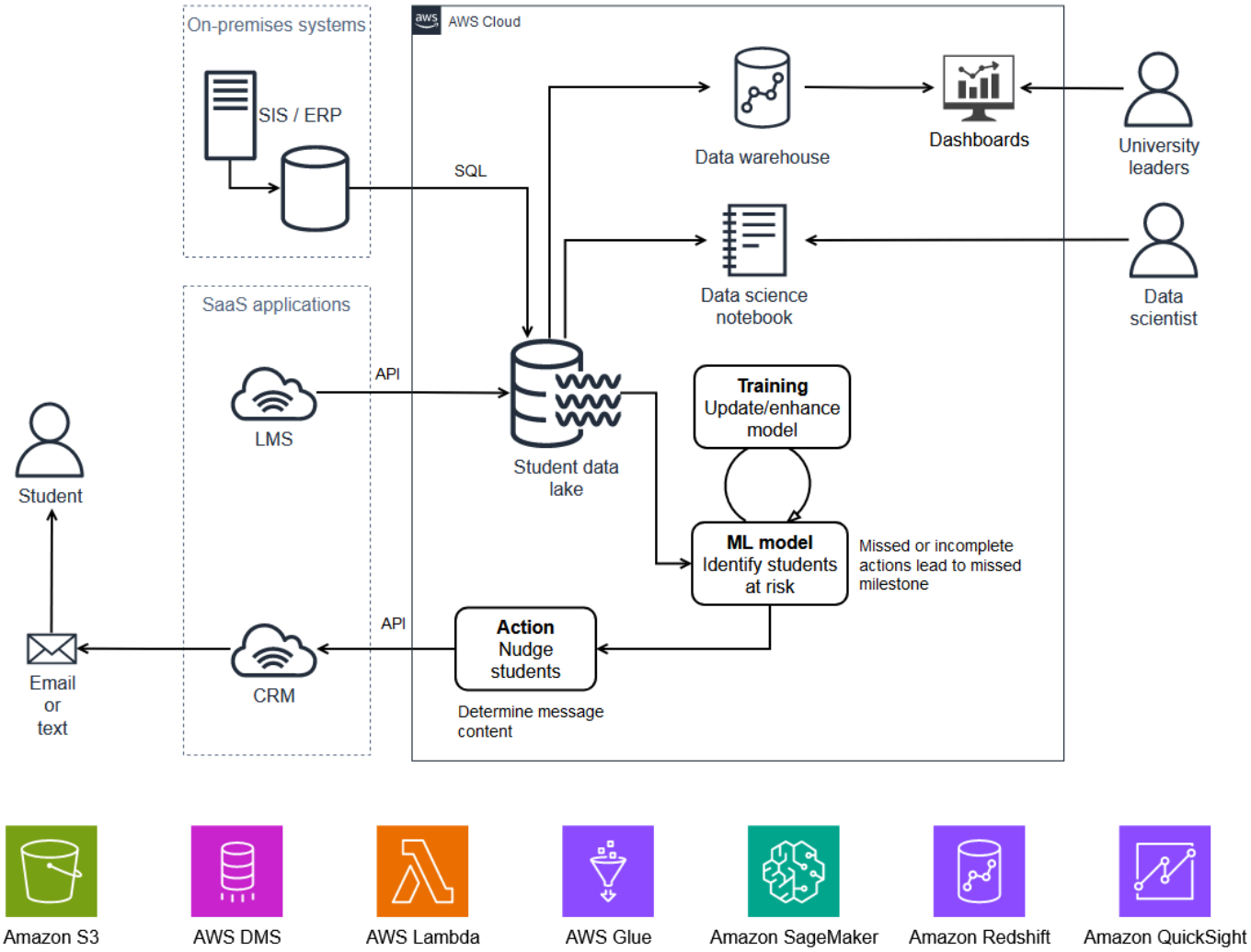
- 가능하고 실현 가능하면 클라우드 네이티브 관리형 솔루션을 채택합니다. WorkSpaces 애플리케이션은 데스크톱 및 애플리케이션 스트리밍을 위한 관리형 서비스입니다. 서버 프로비저닝, 규모 조정 또는 유지 관리에 대한 걱정 없이 데스크톱과 애플리케이션을 스트리밍할 수 있습니다. 애플리케이션을 설치하고 적절한 ID, 네트워크 및 스토리지 솔루션을 연결한 다음 해당 애플리케이션을 중앙에서 관리하고 사용자에게 스트리밍합니다. 그러면 자체 가상 데스크톱 스트리밍 솔루션을 관리하는 데 필요한 차별화되지 않은 많은 부담이 제거됩니다.

학생 성공 예측

미국의 한 중서부 대학에서 입학하는 1학년 학생의 몇 가지 주요 활동이 학생의 첫 번째 학기 및 학위 취득 모두에서 높은 성공 예측 지표로 사용할 수 있다는 사실을 발견했습니다. 이 대학은 이러한 활동의 완료를 감시하는 시스템을 구현하고 싶었고, 주요 기한이 다가오거나 경과했을 때 학생이 이러한 단계를 완료하도록 장려하고 싶었습니다.

SaaS 학습 관리 시스템(LMS) 데이터는 이 솔루션의 주요 입력 요소였지만, 해당 데이터는 대학 IT 팀의 데이터 웨어하우징 도구를 사용하여 액세스하고 처리하기가 어려운 것으로 나타났습니다. 또한 학생에게 보내는 메시지는 학교의 클라우드 기반 고객 관계 관리(CRM) 시스템을 통해 전송되어야 했습니다. 기능적 솔루션을 빌드하고 학생에게 표시하는 프롬프트의 효과를 평가하기 위해 대학은 CRM을 통해 메시지를 시작하고 여기에서 데이터를 수집해야 했습니다.

이 대학은 솔루션을 개발하여 단일 클라우드 환경에 배포했습니다. 솔루션은 클라우드 네이티브 관리형 서비스, 프로비저닝된 클라우드 서버, 온프레미스 시스템 및 클라우드 기반 SaaS 애플리케이션과의 통합을 조합하였습니다. 다음 다이어그램에서 볼 수 있듯이 솔루션은 학생 정보 시스템(SIS), LMS 및 CRM의 데이터를 데이터 레이크로 수집합니다. 이 데이터를 사용하여 주요 활동이 누락될 위험이 있는 학생을 식별하고, CRM을 통해 메시지를 시작하며, 대학 경영진에게 대시보드를 제공합니다.



이 아키텍처는 다음 권장 사항을 따릅니다.

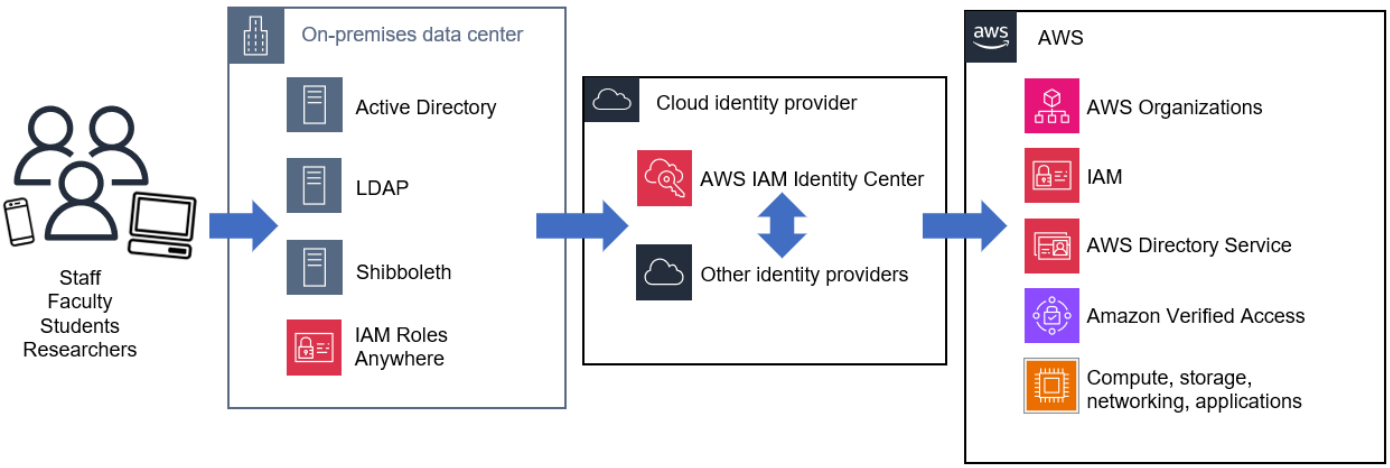
- 전략적 기본 클라우드 제공업체를 선택합니다. 대학의 전략적 클라우드 제공업체는 배포된 전체 솔루션을 지원합니다. 이를 통해 IT 및 비즈니스 직원은 통합된 단일 클라우드 기능 세트에서 기술을 개발하는 데 집중할 수 있습니다.
- SaaS 애플리케이션과 기본 클라우드 서비스를 구별합니다. 이 대학은 SaaS 애플리케이션과 핵심 클라우드 분석 서비스를 구별하고 SaaS 애플리케이션과의 통합을 사용하여 데이터를 수집하고 적절한 통신을 시작합니다.
- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항을 설정합니다. 대학은 학생 데이터를 적절하게 처리하기 위해 전송 중 및 유휴 시 암호화를 포함한 가드레일 및 제어를 적용하여 아키텍처의 모든 구성 요소를 안전하게 보호합니다.

- 가능하고 실현 가능하면 클라우드 네이티브 관리형 솔루션을 채택합니다. 클라우드 네이티브 관리형 서비스는 데이터 수집, 스토리지, 데이터베이스 및 추출, 전환, 적재(ETL) 기능에 사용되므로 포괄적인 데이터 처리 워크플로를 개발하는 데 걸리는 시간이 줄어듭니다.

ID 페더레이션 및 Single Sign-On

핵심 시스템에서 일관된 ID 관리를 보장하는 것은 모든 기술을 성공적으로 안전하게 채택하는 데 중요합니다. 교육 기관은 ID 관리를 단순화하고 운영 부담을 줄이며 다중 인증 및 최소 권한 액세스와 같은 모범 사례를 중앙에서 적용하기 위해 AWS IAM Identity Center, Microsoft Entra ID(이전 Azure Active Directory), Okta, JumpCloud, OneLogin, Ping Identity및 CyberArk와 같은 클라우드 기반 ID 및 Single Sign-On 솔루션을 점점 더 많이 채택하고 있습니다.

이러한 기관 중 다수는 여전히 온프레미스 환경에 대해 Active Directory 및 Shibboleth와 같은 ID 관리 및 디렉터리 서비스를 유지 관리합니다. 이를 클라우드 기반 솔루션과 통합하여 학생, 교직원 및 직원을 위한 중앙 집중식 ID 관리와 Single Sign-On을 활성화할 수 있습니다. 클라우드 솔루션 제공업체는 클라우드 ID 제공업체를 통해 기존 애플리케이션, SaaS 솔루션 및 클라우드 서비스에 자격 증명을 페더레이션할 수 있는 강력하고 통합하기 쉬운 ID 관리 플랫폼을 갖추고 있어야 합니다. 다음 다이어그램은 아키텍처 예제를 보여줍니다.



이 아키텍처는 다음 권장 사항을 따릅니다.

- 전략적 기본 클라우드 제공업체를 선택합니다. 이 아키텍처는를 기본 클라우드 공급자 AWS 로 사용합니다. 이 아키텍처는 클라우드 ID 제공업체 및 온프레미스의 기존 ID 관리 및 디렉터리 서비스와 통합하여 기본 클라우드 제공업체의 서비스와 다른 애플리케이션 및 SaaS 솔루션에 대한 액세스의 자동화된 프로비저닝 및 관리를 지원합니다. 이를 통해 기관의 기술 포트폴리오에 더 많은 애플리케

이션과 서비스가 추가될 때 일관되고 관리하기 쉬운 방식으로 보안 및 거버넌스 요구 사항을 충족할 수 있습니다.

- SaaS 애플리케이션과 기본 클라우드 서비스를 구별합니다. 이 아키텍처는 여러 유형의 클라우드 기반, SaaS 및 온프레미스 자격 증명 시스템을 통합하여 AWS 클라우드 서비스 및 기타 애플리케이션에 대한 액세스를 제공합니다. 많은 클라우드 기반 ID 제공업체 및 Single Sign-On 솔루션은 SaaS 애플리케이션이기도 하며, SAML과 같은 네이티브 통합 및 표준 프로토콜을 사용하여 여러 환경에서 작동할 수 있습니다.
- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항을 설정합니다. 이 아키텍처는 국립 표준 기술 연구소(NIST) 사이버 보안 프레임워크(CSF), NIST 800-171 및 NIST 800-53을 비롯한 다양한 보안 프레임워크에서 발행한 ID 및 액세스 관리에 대한 지침을 준수합니다. AWS Organizations, AWS Identity and Access Management (IAM) 및 기타 AWS 보안, ID 및 규정 준수 서비스와의 통합은 그룹 권한을 기반으로 안전하고 세분화된 액세스 제어를 제공하는 데 도움이 됩니다.
- 가능하고 실현 가능하면 클라우드 네이티브 관리형 서비스를 채택합니다. 이 아키텍처에서는 ID 관리 및 Single Sign-On을 위해 클라우드 기반 관리형 서비스를 사용합니다. 이렇게 하면 인프라 관리에 소요되는 시간과 노력이 줄어들고 이러한 중요한 시스템을 더 쉽게 유지 관리할 수 있습니다.
- 기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처를 구현합니다. 이 아키텍처는 Active Directory, Lightweight Directory Access Control(LDAP) 및 Shibboleth 워크로드를 호스팅하기 위한 인프라에 대한 기존 온프레미스 투자를 통합하고, 결국 핵심 ID 서비스를 클라우드 기반 인프라로 이전할 수 있는 경로를 제공합니다. 또한 온프레미스 워크로드에 AWS 리소스에 대한 인증서 기반 액세스가 필요한 경우 AWS Identity and Access Management Roles Anywhere를 사용할 수 있습니다.

연구 컴퓨팅을 위한 클라우드 버스팅

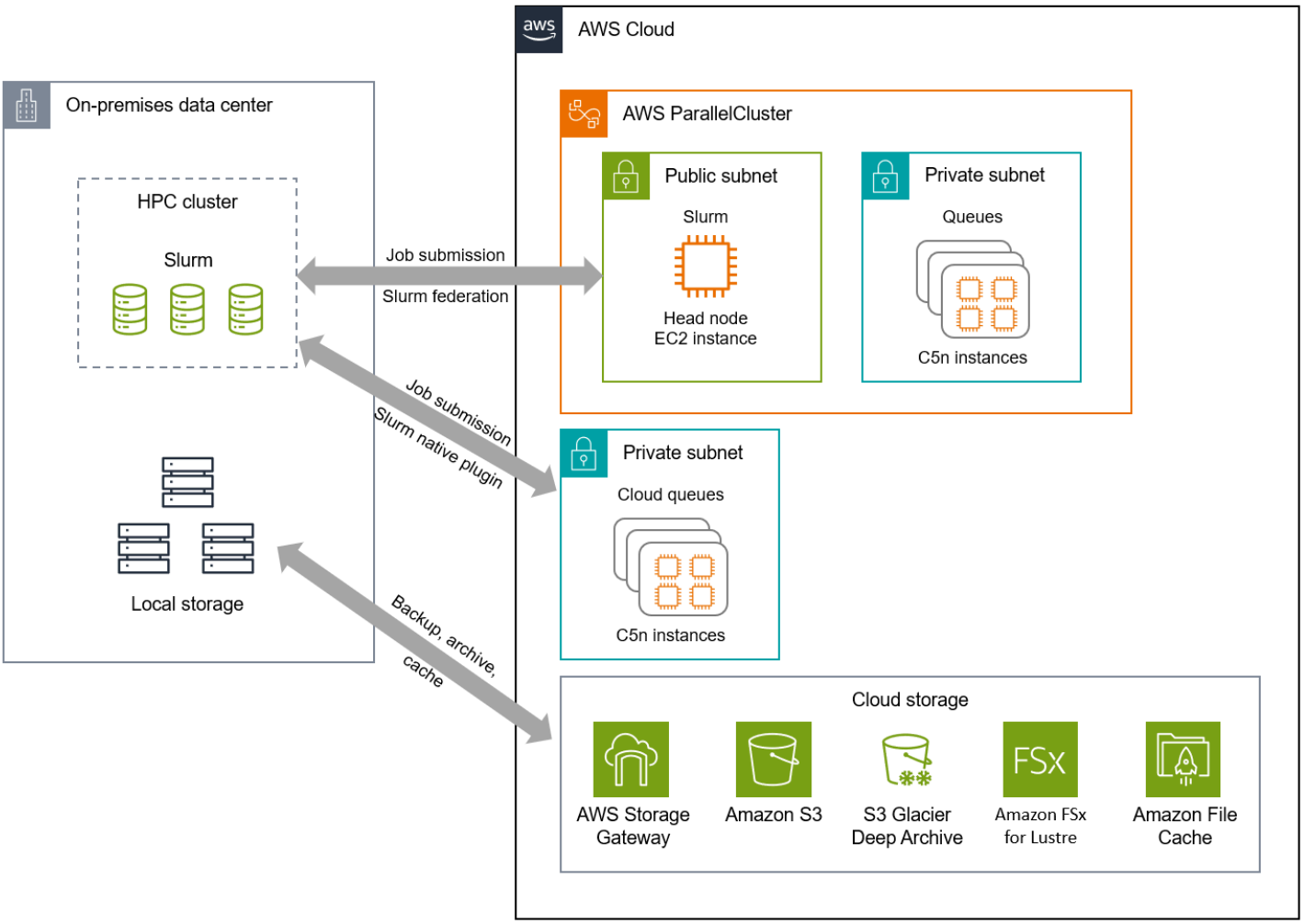
미국의 R1(Doctoral Universities – Very High Research Activity) 연구 기관에서는 수년간 Slurm 스케줄러를 사용하여 온프레미스 고성능 컴퓨팅(HPC) 클러스터를 실행해 왔습니다. 몇 주 동안 예약된 유지 관리를 제외하고 클러스터는 대부분의 대기열이 가득 찬 상태에서 80~95%의 사용률로 실행되었습니다.

기관의 연구 활동 수가 증가함에 따라 용량 및 역량 문제가 발생했습니다. 몇몇 주요 연구원은 항상 특정 대기열에서 장기 실행 시뮬레이션을 수행하여 다른 사용자의 대기 시간을 늘렸습니다. 새로 고용된 교직원은 기상 예측을 위한 새로운 인공 지능 및 기계 학습(AI/ML) 모델을 빌드하기 위해 많은 수의 기상 시뮬레이션을 실행해야 했지만 사용 가능한 것보다 더 많은 용량이 필요했습니다. 또한 이 연구 컴퓨팅 그룹은 기계 학습 모델을 훈련하기 위한 최신 그래픽 처리 장치(GPU)에 대한 요청을 더 많이 받고

있었습니다. 새 GPU에 대한 자금이 있더라도 팀은 데이터 센터에서 랙 공간을 확장하기 위한 승인을 받기 위해 몇 달을 기다려야 합니다.

많은 연구자가 이전 데이터를 삭제할 의향이 없었기 때문에 로컬 스토리지 용량도 문제가 되었습니다. 온프레미스의 중요한 고성능 스토리지를 확보하려면 더 확장 가능한 장기 스토리지 옵션이 필요했습니다.

클라우드는 온프레미스 용량이 충분하지 않을 때 연구 컴퓨팅을 클라우드로 버스트할 수 있는 하이브리드 컴퓨팅 및 스토리지 솔루션으로 이러한 문제를 해결합니다. 다음 아키텍처 다이어그램에서는 AWS ParallelCluster 및 AWS Storage Gateway와 같은 도구를 사용하는 몇 가지 컴퓨팅 및 스토리지 버스팅 접근 방식을 보여줍니다.



이 아키텍처는 다음 권장 사항을 따릅니다.

- 전략적 기본 클라우드 제공업체를 선택합니다. 이 아키텍처는 하나의 기본 클라우드 제공업체를 사용하여 가장 덜 일반적인 분모 접근 방식에 의해 제한되지 않도록 합니다. 그러면 기관은 기본 클라

우드 제공업체가 제공하는 혁신과 네이티브 컴퓨팅 및 스토리지 서비스를 활용할 수 있습니다. 연구 컴퓨팅 팀은 여러 클라우드 환경에서 작업하는 방법이 아니라 기본 클라우드 제공업체가 제공하는 환경에서 워크로드를 최적화하는 데 집중할 수 있습니다.

- 각 클라우드 서비스 제공업체에 대한 보안 및 거버넌스 요구 사항을 설정합니다. 이 아키텍처에 사용되는 각 서비스와 도구는 프라이빗 연결성, 저장 및 전송 중 데이터 암호화, 활동 로깅 등을 포함하여 연구 컴퓨팅 팀의 보안 및 거버넌스 요구 사항을 충족하도록 구성할 수 있습니다.
- 가능하고 실현 가능하면 클라우드 네이티브 관리형 서비스를 채택합니다. 이 아키텍처에서는 관리형 스토리지 및 컴퓨팅 서비스를 사용하는 기능과 클러스터 관리를 단순화하는 도구를 제공합니다. 그러면 연구 컴퓨팅 팀이 복잡하고 시간이 많이 걸릴 수 있는 클러스터 또는 기본 인프라를 자체적으로 관리하는 작업에 대해 걱정할 필요가 없습니다.
- 기존 온프레미스 투자가 지속적인 사용을 장려할 경우 하이브리드 아키텍처를 구현합니다. 이 아키텍처를 통해 기관은 온프레미스 리소스를 계속 사용하고 클라우드를 활용하여 용량을 늘리며 온디맨드로 컴퓨팅 성능을 확장할 수 있습니다. 클라우드를 사용하면 기관은 컴퓨팅 유형을 적절하게 조정하여 가격 대비 성능을 극대화하고 최신 기술에 액세스하여 추가 온프레미스 하드웨어에 대한 대규모 선결제 투자 없이 혁신을 촉진할 수 있습니다.

다음 단계

클라우드 워크로드에 적합한 배포 모델을 선택하려면 신중하게 고려해야 합니다. 이 문서에 설명된 권장 사항을 사용하여 의사 결정을 안내하고 불필요한 복잡성, 직원 요구 증가, 일관성 없는 거버넌스, 가장 낮은 공통 분모 접근 방식과 같은 일반적인 위험을 방지합니다. 이러한 모범 사례를 따르면 조직의 목표를 보다 효과적으로 충족하고 초과할 수 있도록 클라우드 채택을 가속화할 수 있습니다.

기본 전략 클라우드 제공업체를 선택하고, 조직의 성숙도를 높여 장기적인 성공을 보장하는 데 도움이 되도록 클라우드 혁신 센터(CCoE)를 구축해야 합니다. SaaS 애플리케이션과 기본 클라우드 서비스를 구분하고 각각에 대한 핵심 보안 및 거버넌스 요구 사항을 식별합니다. 가능하면 기존 데이터 센터 투자가 지속적인 사용을 장려할 때 클라우드 네이티브 관리형 서비스를 채택하고 하이브리드 아키텍처를 구현합니다. 마지막으로 실제로 필요한 워크로드에 대해서만 멀티클라우드를 예약합니다.

AWS 는 단일, 하이브리드 및 멀티클라우드 환경을 관리하는 데 도움이 되도록 잘 배치되어 있습니다. 기관은 AWS Systems Manager, 및 Amazon CloudWatch와 같은 AWS 관리 AWS Config및 관찰성 솔루션을 사용하여 환경에 관계없이 인프라 및 애플리케이션의 관리 및 모니터링을 간소화하고 중앙 집중화할 수 있습니다. Amazon Athena, AWS Glue 및 AWS DataSync와 같은 데이터 및 분석 서비스를 사용하면 데이터를 저장하면 항상 모든 데이터에서 인사이트를 얻을 수 있습니다. AWS Outposts, AWS Wavelength및와 같은 하이브리드 솔루션을 AWS Snow Family 사용하면 AWS 인프라와 서비스를 필요한 모든 곳으로 가져올 수 있습니다. Amazon EKS Distro와 같은 도구는 AWS온프레미스 또는 기타 클라우드에서 자체 관리형 Kubernetes 클러스터를 구축하는 데 도움이 됩니다.

클라우드 전략을 정의할 때 다음 단계를 고려합니다.

1. AWS Cloud Adoption Framework(AWS CAF)를 검토하여 혁신 기회를 식별 및 우선 순위를 지정하고, 클라우드 준비 상태를 평가 및 개선하고, 혁신 로드맵을 반복적으로 개선합니다.
2. 개념 증명으로 시작할 클라우드 구현 시스템을 식별합니다. 이를 통해 클라우드 기반 또는 프레임워크를 정의하여 가정을 검증할 수 있으며, 향후 클라우드 구현을 활성화할 수도 있습니다.
3. AWS 계정 팀을 참여시켜 클라우드 구현 목표를 논의합니다. AWS 계정 팀은 설명을 제공하고, 접근 방식을 제안하고, 종속성을 식별하고, 팀과 협력하여 초기 개념에서 구현까지 여정을 매핑할 수 있습니다.

기여자

이 가이드의 기여자는 다음과 같습니다.

- Kevin Arand, Senior Manager, Solutions Architecture, Education, AWS
- Kevin McCandless, Senior Solutions Architect, K-12 Education, AWS
- Craig Jordan, Principal Solutions Architect, Education, AWS
- Jesse Roberts, Principal Solutions Architect, SLG & K-12 Education, AWS
- Jianjun Xu, Principal Solutions Architect, Education, AWS
- Josh Badal, Senior Solutions Architect, Education, AWS
- Raj Chary, Senior Solutions Architect, Education, AWS

참조 자료

추가 정보는 다음을 참조하세요.

- AWS 아키텍처 센터
- Public Sector Cloud Transformation
- AWS Cloud Adoption Framework(AWS CAF)
- AWS Solutions for Hybrid and Multicloud

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	—	2023년 9월 15일

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