HashiCorp

클라우드 운영 모델 구축

최신 데이터센터 및 멀티클라우드 운영의 가치를 실현하는 가장 빠른 경로

백서

클라우드 운영 모델 구축

전체 요약

이제 클라우드가 제 역할을 해야 할 때입니다. 많은 기업들이 디지털 트랜스포메이션을 추진하면서 펼쳐진 멀티클라우드 아키텍처 시대에 성공하려면, 엔터프라이즈 IT는 ITIL 기반 게이트키핑(gatekeeping) 방식에서 탈피해 DevOps 탁월성(excellence)을 위해 공유 셀프서비스 프로세스를 활성화하는 방향으로 나아가야 합니다.

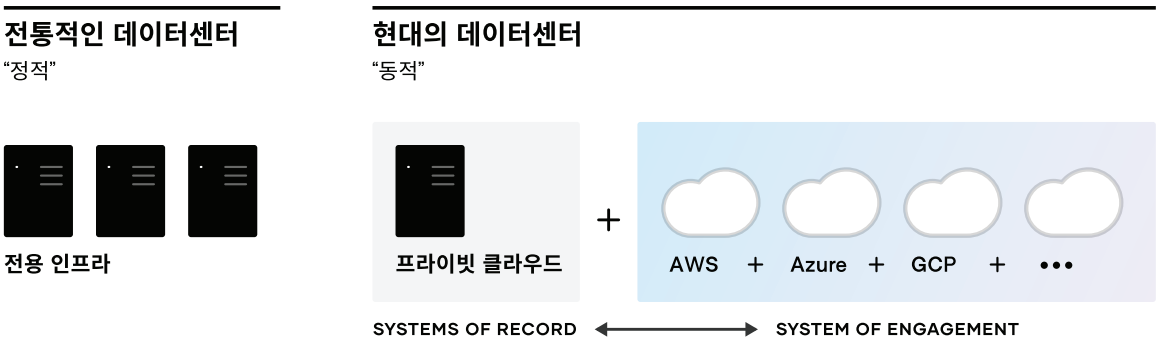
대부분 기업에서 디지털 트랜스포메이션 노력은 새로운 비즈니스 및 고객 가치를 보다 빨리, 그리고 대규모로 제공하는 데 목적을 두고 있습니다. 엔터프라이즈 IT에서 이는 비용 최적화에서 속도 최적화로의 전환을 의미합니다. 클라우드는 무한하게 확장할 수 있는 온디맨드 서비스를 신속하게 배포할 수 있는 기회를 제공한다는 점에서, 이러한 전환에서 필수적인 부분입니다.

클라우드의 가치를 신속하게 실현하기 위해 기업들은 클라우드 운영 모델을 수용하고 사람, 프로세스, 툴을 조정하는 등 클라우드의 각 계층 전반에서 애플리케이션 제공 프로세스를 산업화하는 방법을 고려해야 합니다.

이 백서에서는 클라우드 운영 모델의 의미를 살펴보고 IT 팀이 인프라, 보안, 네트워킹 및 애플리케이션 제공 전반에 걸쳐 이 모델을 채택할 수 있도록 돕는 솔루션을 제시합니다.

멀티클라우드 데이터센터로의 전환

클라우드 및 멀티클라우드 환경으로의 전환은 IT에게 있어 세대 간 전환입니다. 이러한 전환은 사설 데이터센터의 대규모 전용 서버에서 온디맨드로 사용 가능한 컴퓨팅 용량 풀로 전환하는 것을 의미합니다. 대부분 기업은 한 클라우드 제공업체로 시작하지만, 다른 회사의 서비스를 사용해야 하는 타당한 이유가 있습니다. 또한, 불가피하게 대부분의 글로벌 2000 기업들은 설계 또는 인수 합병을 통해 둘 이상의 서비스를 사용하게 될 것입니다.



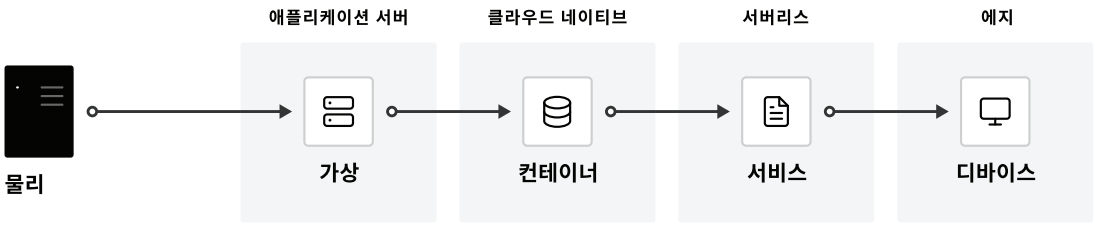
클라우드는 고객과 사용자를 참여시키기 위해 개발된 애플리케이션인 새로운 "참여 시스템(SoE: Systems of Engagement)"을 위한 속도 및 확장 최적화의 기회를 제공합니다. 이들 새로운 애플리케이션은 고객이 기업과 소통하는 주된 인터페이스로서, 다음과 같은 경향의 클라우드에서 제공하는 데 이상적입니다.

- 짧은 시간 동안 대규모로 부하를 확장 및 축소해야 하는 동적 사용 특성을 지닌 클라우드
- 빠르게 구축 및 반복해야 한다는 압력을 받고 있는 클라우드. 이들 새로운 시스템 중 상당수는 이벤트나 캠페인에 대한 특화된 사용자 경험을 제공하는 등 본질적으로 일시적인 것일 수 있습니다.

하지만, 대부분 기업에서 이러한 참여 시스템은 대개 기존 데이터센터의 인프라에 계속 상주하는 핵심 비즈니스 데이터베이스와 내부 애플리케이션인 기존 "기록 시스템(SoR: Systems of Record)"에 연결되어야 합니다. 이에 따라, 기업들은 여러 퍼블릭 클라우드와 프라이빗 클라우드가 혼합된 하이브리드 환경을 보유하게 됩니다.

대부분 기업들이 직면한 과제는 어떻게 이 애플리케이션들을 일관되게 클라우드에 제공하는 동시에 여러 개발 팀 간에 발생할 수 있는 마찰을 최소화하느냐 하는 것입니다.

이러한 문제가 심각해지면서, 독립적(self-contained) 환경의 가상 머신(VM)이 아니라, 공유 환경의 클라우드 '리소스'를 다루는 것으로 기본 원칙이 바뀌었습니다.
이에 따라, 기업들은 새로운 클라우드 인프라를 개발하면서, 기존 자산을 유지하는 경쟁력 있는 운영 모델을 갖게 됐습니다.



클라우드 컴퓨팅을 운영하기 위해서는 여러 클라우드 제공 업체에서 대규모로 재사용할 수 있는 일관된 워크플로우가 필요합니다. 주요 요구 사항은 다음과 같습니다.

- 프로비저닝을 위한 일관된 안내 방침
- 보안과 네트워크 접속을 위한 ID
- 배포와 실행을 할 수 있는 권한 및 권리

클라우드 운영 모델의 의미

클라우드 전환의 본질적 의미는 "정적" 인프라에서 "동적" 인프라로 전환한다는 것입니다. 즉, 정적인 IT 리소스의 구성 및 관리에서 온디맨드 방식으로 동적 리소스를 프로비저닝, 보안, 접속하고 실행하는 것으로 초점이 옮겨가는 것입니다.

	정적		동적
실행	전용 인프라	→	시스템 전반에 걸쳐 스케줄링
연결	호스트 기반, 정적 IP	→	서비스 기반, 동적 IP
보호	하이 트러스트, IP 기반	→	로우 트러스트, 자격증명 기반
프로비저닝	전용 서버, 동기종	→	CoD (Capacity on-demand), 이기종

이러한 의미를 각 스택에 따라 분석하면, 다음과 같이 다양한 변화를 의미합니다.

- **프로비저닝.** 인프라 계층은 제한된 규모로 전용 서버를 가동하는 환경에서, 수천 대의 서버를 spin up하고 사용하지 않을 때는 감축해 수요 증가에 쉽게 적응할 수 있는 동적 환경으로 전환됩니다. 아키텍처와 서비스가 분산될수록 컴퓨팅 노드의 볼륨이 크게 증가합니다.

- **보안.** 보안 계층은 강력한 경계와 방화벽으로 대표되는 근본적으로 "하이 트러스트(high-trust)" 환경에서, 명확하거나 고정된 경계가 없는 "로우 트러스트 (Low trust)" 또는 "제로 트러스트(zero-trust)" 환경으로 전환됩니다. 이에 따라, 보안에 대한 기본 가정은 IP 기반에서, 리소스에 대한 ID 기반 액세스를 사용하는 것으로 전환됩니다. 이러한 변화는 전통적인 보안 모델을 완전히 붕괴시키는 것입니다.

- **연결.** 네트워킹 계층은 서비스와 애플리케이션의 물리적 위치와 IP 주소에 주로 의존하던 형태에서 검색, 세분화 및 구성을 위해 **서비스의 동적 레지스트리**를 사용하는 방식으로 전환됩니다. 엔터프라이즈 IT 팀은 네트워크나 컴퓨팅 리소스의 물리적 위치에 대해 이전과 동일한 제어 권한이 없으며 서비스 기반 연결에 대해 생각해야 합니다.

- **실행.** 런타임 계층은 아티팩트를 정적 애플리케이션 서버로 배포하는 방식에서, 온디맨드로 프로비저닝되는 인프라 풀에서 스케줄러를 사용해 애플리케이션을 배포하는 방식으로 전환됩니다. 또한, 새로운 애플리케이션은 가상 머신부터 컨테이너에 이르기까지 동적으로 프로비저닝되고 다양한 방식으로 패키징되는 서비스의 모음이 됐습니다.

	정적		동적			
	전용		프라이빗 클라우드	AWS	AZURE	GCP
실행 배포	vSphere	→	vSphere	EKS / ECS Lambda	AKS / ACS Azure Functions	GKE Cloud Functions
연결 네트워킹	하드웨어	→	다양한 하드웨어	CloudMap AppMesh	전용	Google Istio
보호 보안	IP: 하드웨어	→	자격증명: AD/LDAP	자격증명: AWS IAM	자격증명: Azure AD	자격증명: GCP IAM
프로비저닝 운영	vCenter	→	Terraform	CloudFormation	Resource Manager	Cloud Deployment Manager

이들 과제를 해결하려면 해당 팀은 다음과 같은 질문을 해야 합니다.

- **사람.** 어떻게 대상 환경에 관계없이, 스킬을 일관되게 활용할 수 있는 멀티클라우드 환경을 위한 팀을 운영할 수 있습니까?
- **프로세스.** 중앙 IT 서비스에 대해 제어 위주의 티켓 기반 게이트키퍼(gatekeeper)가 아니라, 속도 위주의 셀프서비스 인에이블러(enabler)로서 포지셔닝하는 한편, 컴플라이언스(compliance)와 거버넌스를 유지하는 방법은 무엇입니까?
- **도구.** 보다 높은 고객 및 비즈니스 가치를 추구하며 클라우드 공급업체들이 제공하는 기능들의 가치를 최대한 실현하기 위해서는 어떻게 해야 합니까?

클라우드 운영 모델의 실제 구현

클라우드 운영 모델의 의미는 인프라, 보안, 네트워킹과 애플리케이션 전반의 팀들에 영향을 미치기 때문에, 성공적인 애플리케이션 제공을 위해 각 계층에 필요한 동적 인프라를 제공하는 중앙 공유 서비스(CoE: Centers of Excellence)를 구축한 기업들 사이에서 반복되는 패턴을 확인했습니다.

팀들이 클라우드 운영 모델을 위해 각 공유 서비스를 제공하면서 IT 속도가 증가합니다. 기업의 클라우드 성숙도가 높을수록 속도도 빨라집니다.

HashiCorp의 활용을 확대함에 따라 고객들의 성숙도와 속도 증가

프로비저닝/운영

Terraform

하이브리드 클라우드
인프라 자동화

IaC(Infrastructure as Code)

컴플라이언스 및 관리

셀프 서비스 인프라

보호/보안

Vault

하이브리드 클라우드
보안 자동화

자격증명 기반 보안

시크릿 관리

서비스형 암호화

Advanced Data Protection

연결/네트워킹

Consul

하이브리드 클라우드
네트워킹 자동화

공용 서비스 레지스트리

서비스 검색

네트워크 미들웨어 자동화

서비스 메시를 통한 제로 트러스트 네트워킹

실행/배포

Nomad

하이브리드 클라우드
애플리케이션 자동화

워크로드 오케스트레이션

컨테이너 오케스트레이션

이기종 오케스트레이션

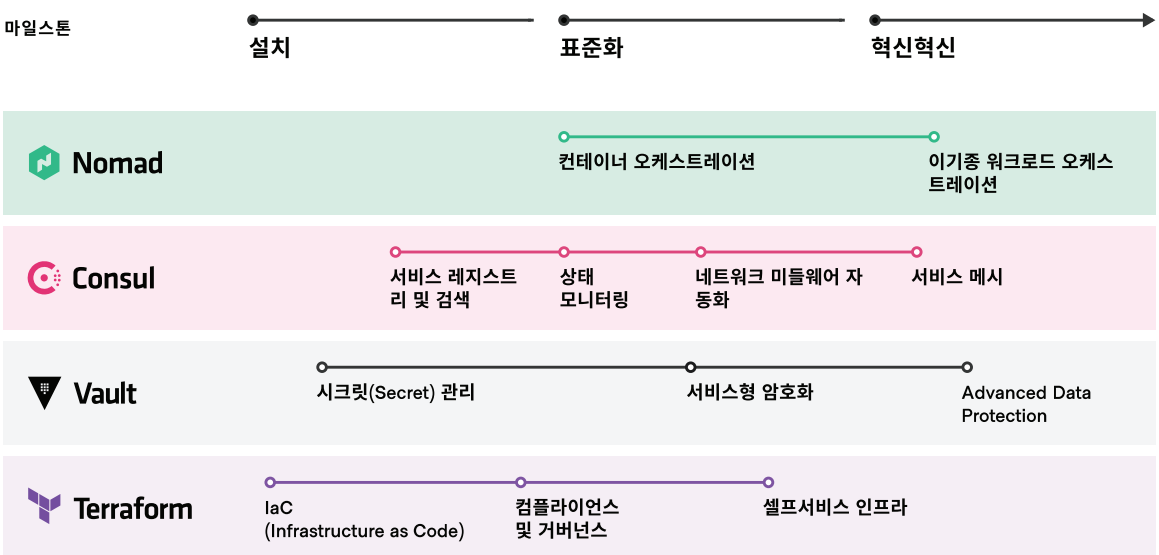
고객들이 클라우드 운영 모델을 실제 구현할 때, 채택한 일반적인 여정에는 다음 세 가지 주요 이정표가 포함됩니다.

1. **클라우드 필수 요소 설치** – 클라우드 여정에 착수하게 되면, 당면 요구 사항은 일반적으로 IaC(Infrastructure as Code)를 채택하고 시크릿(Secret) 관리 솔루션으로 이를 보호함으로써 클라우드 인프라를 프로비저닝하는 것입니다. 이는 미래에도 사용할 수 있도록 확장성이 뛰어난 진정한 의미의 동적 클라우드 아키텍처를 구축하는 데 필수적입니다.

2. **일련의 공유 서비스에 대한 표준화** – 클라우드 소비가 증가하기 시작하면 클라우드가 제공하는 이점을 최대한 활용할 수 있도록 일련의 공유 서비스를 구현하고 표준화해야 합니다. 또한, 액세스 제어 규칙을 설정하고 요구 사항을 추적해야 한다는 요구가 점차 중요해지면서, 거버넌스 및 컴플라이언스와 관련된 과제가 발생합니다.

3. **공통 논리(common logical) 아키텍처를 사용한 혁신** – 클라우드를 완전히 수용하고 클라우드 서비스와 애플리케이션을 기본 참여 시스템으로 사용하게 되면, 공통 논리 아키텍처를 만들어야 합니다. 이를 위해서는 클라우드 솔루션의 광범위한 에코 시스템과 연결하고 자체적으로 서비스와 여러 클라우드 전반에서 고급 보안 및 오케스트레이션 기능을 제공하는 컨트롤 플레인이 필요합니다.

클라우드를 위한 운영 모델의 실 구현을 위한 엔터프라이즈 환경 변화의 여정



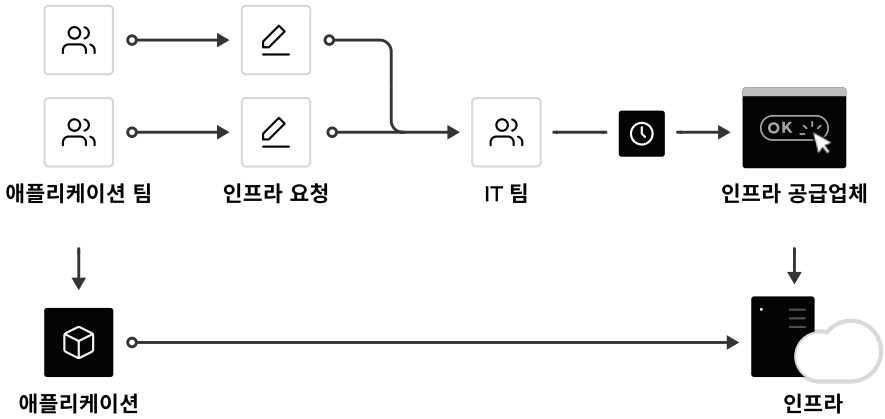
다음은 기업들이 성공적으로 채택한 단계별 여정입니다.

1단계: 멀티클라우드 인프라 프로비저닝

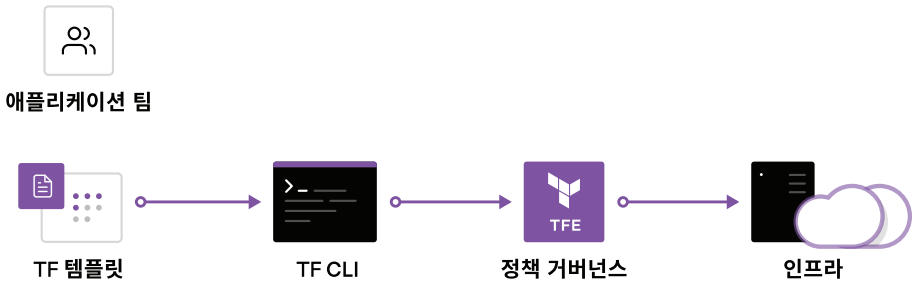
클라우드 채택을 위한 기반은 인프라 프로비저닝입니다. HashiCorp Terraform은 세계에서 가장 널리 사용되는 클라우드 프로비저닝 제품이며, 모든 대상 플랫폼을 위한 여러 공급업체를 활용해 모든 애플리케이션을 위한 인프라를 프로비저닝하는 데 사용될 수 있습니다.

인프라 프로비저닝을 위한 공유 서비스를 달성하기 위해 IT팀은 복제 가능한 IaC(Infrastructure as Code) 방식을 구현하는 것으로 시작한 다음, 컴플라이언스와 거버넌스 워크플로우를 계층화해 적절한 제어가 이루어지도록 해야 합니다.

Terraform 도입 이전



Terraform 도입 이후



복제 가능한 IaC(Infrastructure as Code)

인프라 프로비저닝을 위한 공유 서비스의 첫번째 목표는 복제 가능한 IaC(Infrastructure as Code)의 제공을 지원함으로써 DevOps팀에게 익숙한 툴을 사용해 CI/CD 워크플로우 내에서 리소스를 계획하고 프로비저닝할 수 있는 방법을 제공한다는 것입니다.

DevOps팀은 하나 이상의 클라우드 플랫폼에서 서비스 구성을 표시하는 Terraform 템플릿을 작성할 수 있습니다. Terraform은 모든 주요 구성 관리 툴과 통합되어 기본 리소스를 프로비저닝한 다음, 세분화된 프로비저닝을 처리할 수 있습니다. 마지막으로, 모니터링 에이전트, 애플리케이션 성능 모니터링(APM) 시스템, 보안 툴, DNS, CDN(Content Delivery Network) 등을 포함한 여타 많은 ISV 제공업체의 서비스를 통해 템플릿을 확장할 수 있습니다. 일단 정의되면, 템플릿은 필요에 따라 자동화된 방식으로 프로비저닝될 수 있습니다. 이러한 과정을 통해 Terraform은 퍼블릭 및 프라이빗 클라우드 전반에서 리소스를 프로비저닝하는 팀을 위한 공통의 워크플로우가 되는 것입니다.

셀프서비스 IT에서는 템플릿 작성 프로세스와 프로비저닝 프로세스를 분리하는 경우, 개발자들이 사전 승인된 템플릿을 사용하는 한, 더 이상 운영 승인을 기다릴 필요가 없기 때문에 애플리케이션을 운영 환경에 적용하는 데 걸리는 시간이 대폭 줄어들게 됩니다

컴플라이언스 및 관리

대부분 팀에서는 구축된 인프라 유형, 사용 방법과 사용하는 팀에 대한 정책을 적용해야 합니다. 코드 프레임워크로서 HashiCorp의 Sentinel 정책은 전체 팀의 워크플로우를 변경하도록 요구하지 않으면서 컴플라이언스와 거버넌스를 제공하며, 코드로도 정의되기 때문에 DevSecOps의 협업과 이해를 증진시키게 됩니다.

코드형 정책(policy as code)이 없는 경우, 기업들은 티켓 기반 검토 프로세스를 사용하여 변경을 승인합니다. 그 결과, 개발자들은 인프라 프로비저닝을 위해 몇 주 또는 그 이상 기다려야 하며 병목 현상이 발생합니다. 코드형 정책을 사용함으로써 정책 정의를 정책 실행에서 분리해 이 문제를 해결할 수 있습니다.

중앙집중화된 팀은 모든 클라우드 프로비저닝 전반에 보안, 컴플라이언스, 운영 모범사례를 적용하는 정책을 체계화합니다. 자동으로 정책을 적용함으로써 수동 검토 프로세스에 병목을 발생시키지 않으면서 변경 사항들이 규정을 준수하도록 보장합니다.

2단계: 멀티클라우드 보안

동적인 클라우드 인프라 환경은 명확한 네트워크 경계가 없이 여러 클라우드에 걸쳐 Low-Trust나 Zero-Trust 네트워크를 통해 호스트 기반 ID에서 애플리케이션 기반 ID로 전환하는 것을 의미합니다.

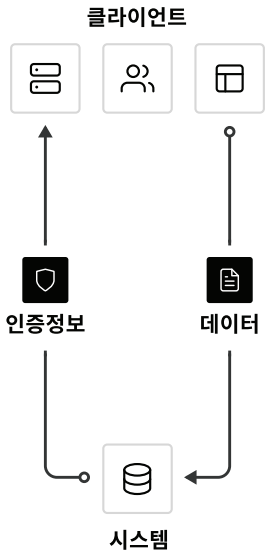
전통적인 보안 세계에서는 High-Trust(높은 수준의 보안환경)인 내부 네트워크를 가정했지만, 이로 인해 단단한 외부 보안에 비해 취약한 내부 구성을 갖게 됐습니다. 또한, 최근 "Zero-Trust" 접근 방식을 통해 내부도 강화하기 위해 노력하고 있습니다. 이를 위해서는 애플리케이션들을 명시적으로 인증하고, 시크릿(Secret)을 불러와서 민감한 작업을 수행할 수 있는 권한을 부여받아야 하며 엄격한 감사가 이루어져야 합니다.

HashiCorp Vault를 통해 사용자는 시스템과 애플리케이션을 보호하기 위해 토큰, 비밀번호, 인증서, 암호화 키에 대한 액세스를 안전하게 저장하고 엄격하게 제어할 수 있습니다. 이는 포괄적인 시크릿(Secret) 관리 솔루션을 제공합니다. 이외에도, Vault는 저장 데이터와 전송 중인 데이터를 보호합니다. Vault는 개발자들이 암호화 키를 노출하지 않고 민감한 데이터를 보호할 수 있도록 암호화를 위한 API를 제공합니다. 또한, Vault는 인증기관(CA)역할을 수행하며 SSL/TLS와의 통신을 보호하기 위해 짧은 유효 기간으로 자동으로 순환하는 동적 인증서를 제공할 수도 있습니다. 마지막으로 Vault는 온프레미스 환경의 Active Directory와 AWS IAM 등 서로 다른 플랫폼 간에 ID 브로커링을 지원하기 때문에 플랫폼 경계를 넘어 애플리케이션들을 실행할 수 있습니다.

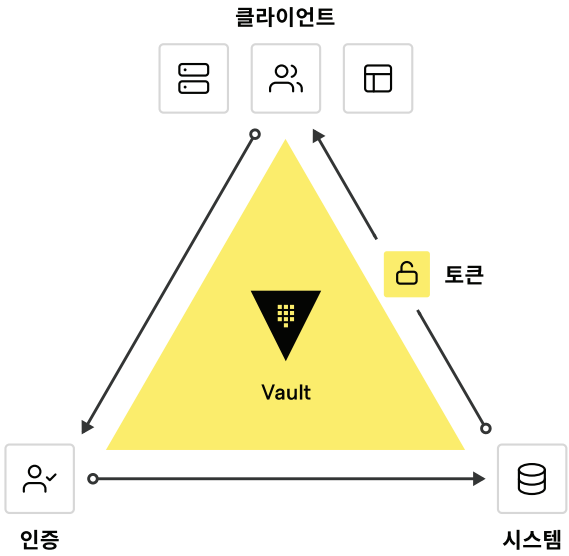
Vault는 클라우드 운영 모델에서 보안을 제공하기 위해 증권거래소, 대규모 금융사, 호텔 체인 등 기타 모든 산업 전반에서 널리 사용됩니다.

보안을 위한 시크릿이 공유되어야 하는 서비스를 운영하려면, IT 팀은 중앙집중식 시크릿(Secret) 관리 서비스를 활성화하고, 이 서비스를 사용하여 인증서와 키 순환, 전송 및 저장 데이터 암호화 등과 같은 보다 수준 높은 서비스형 암호화 사용 케이스를 제공해야 합니다.

Vault 도입 이전



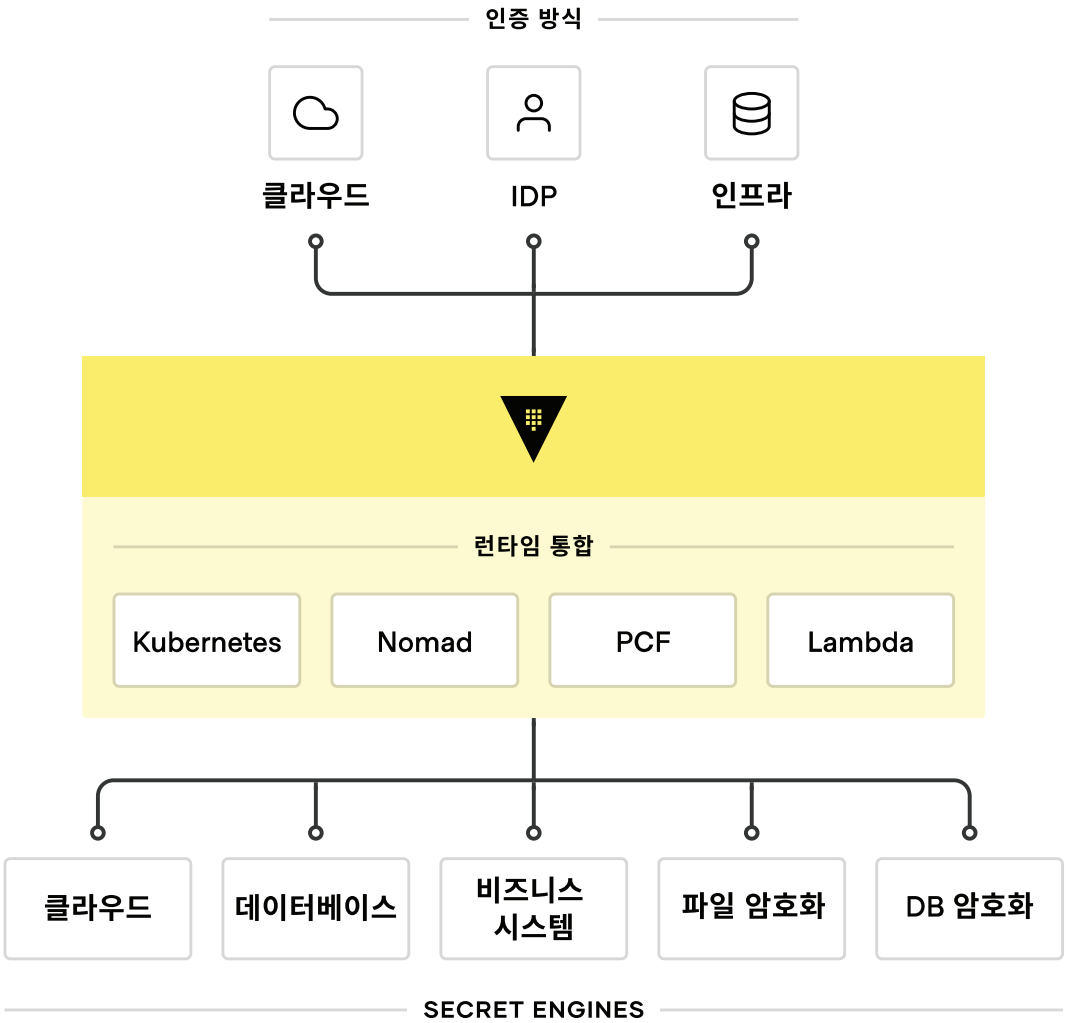
Vault 도입 이후



시크릿(Secret) 관리

클라우드 보안의 첫 번째 단계는 일반적으로 중앙 저장소, 접근 제어, 동적으로 생성되는 시크릿 생성과 같은 전반적인 시크릿 관리입니다. 고정 IP 주소에 의존하지 않고, AWS IAM 및 Azure AAD 등과 같은 ID 기반 액세스 시스템과 통합해 서비스와 리소스를 인증하고 액세스하는 것이 중요합니다.

Vault는 정책을 사용하여 애플리케이션 인증 방법, 사용 권한이 있는 로그인 정보와 감사 수행 방법을 체계화합니다. 클라우드 IAM(Identity and Access Management) 플랫폼, Kubernetes, Active Directory 및 인증을 위한 기타 SAML 기반 시스템 등 신뢰할 수 있는 일련의 ID 제공자와 통합할 수 있습니다. 이후, Vault는 신뢰할 수 있는 애플리케이션 소스와 사용자 ID를 기반으로 시크릿과 시스템에 대한 액세스를 중앙에서 관리하고 적용합니다.



엔터프라이즈 IT 팀은 일관되고 감사가 이루어지며 안전하게 보호되는 워크플로우를 통해 모든 시스템에 대한 시크릿을 요청할 수 있는 공유 서비스를 구축해야 합니다.

서비스형 암호화

또한 기업은 저장되거나 전송 중인 애플리케이션 데이터를 암호화해야 합니다. Vault는 서비스형 암호화를 제공해 키 관리와 암호화를 위한 일관된 API를 제공할 수 있습니다. 이를 통해 개발자들은 통합된 암호화 방식으로 수행하고, 여러 환경 전반에서 데이터를 보호할 수 있습니다.

Vault를 서비스형 암호화를 위한 기반으로 사용하면 인증서와 키 순환과 같은 보안팀이 직면한 어려운 문제들을 해결할 수 있습니다. Vault는 중앙집중식 키 관리 기능을 제공해 클라우드와 데이터센터 전반에서 전송 중인 데이터 및 저장 데이터의 암호화를 간소화할 수 있습니다. 이를 통해 고가의 하드웨어 보안 모듈(HSM: Hardware Security Modules) 관련 비용을 절감하고, 조직 전반에 일관된 보안 워크플로우와 암호화 표준을 통해 생산성을 높일 수 있습니다.

많은 기업들이 개발자에게 데이터를 암호화할 수 있는 권한을 제공하지만, 종종 "방법"을 제공하지 않아 개발자들이 암호화를 제대로 이해하지 못한 채 맞춤형 솔루션을 구축하는 경우가 많습니다. Vault는 개발자에게 쉽게 사용할 수 있는 단순한 API를 제공하며, 중앙 보안팀에는 필요한 정책 제어와 라이프사이클 관리 API를 제공합니다.

Advanced Data Protection

클라우드로 전환하거나 하이브리드 환경으로 확장하는 기업들은 저장 데이터 암호화와 같은 암호화 작업을 실행해야 하는 온프레미스 서비스 및 애플리케이션들을 계속 유지하고 지원합니다. 이들 서비스는 암호화 키 관리에 관한 로직을 반드시 구현할 필요는 없기 때문에, 외부 공급업체에 키 관리 업무를 위임하고자 합니다. Advanced Data Protection은 TDE(Transparent Data Encryption)를 사용해 MySQL, MongoDB, PostgreSQL 및 기타 데이터베이스의 데이터를 자동으로 보호하는 것을 비롯해 인프라와 Vault Enterprise 간의 고급 암호화 키, 운영 및 관리를 안전하게 연결, 제어, 통합을 할 수 있도록 합니다.

데이터 컴플라이언스(PCI–DSS, HIPAA 등), 데이터 보호, 개인식별정보(PII)의 암호화를 통한 익명성 보호 등에 대한 엄격한 보안 요구 사항이 있는 기업들의 경우 Advanced Data Protection을 통해 신용카드, 개인 정보, 계좌 번호 등과 같은 민감한 데이터를 보호하는 데이터 마스킹과 같은 토큰화 기능을 제공합니다.

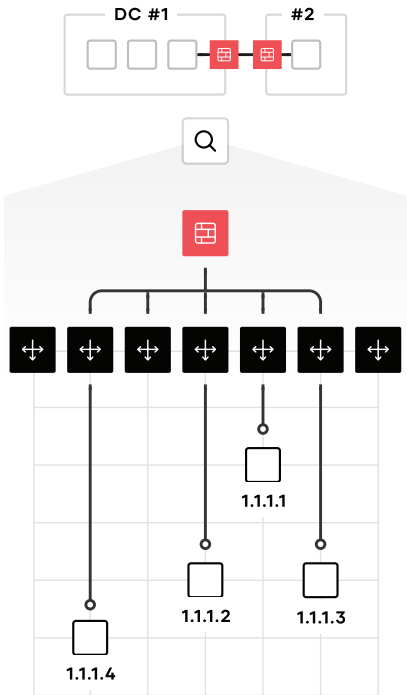
3단계: 멀티클라우드 서비스 네트워킹

클라우드의 네트워킹의 문제는 종종 엔터프라이즈를 위한 클라우드 운영 모델을 채택하는 데 있어 가장 어려운 측면 중 하나입니다. 동적 IP 주소의 조합, 마이크로서비스 패턴 채택에 따른 east–west 트래픽 급증, 명확한 네트워크 경계의 부재는 매우 심각한 문제입니다.

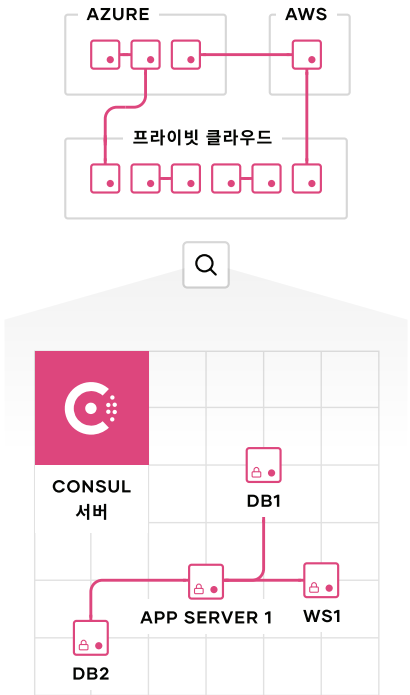
HashiCorp Consul은 서비스를 연결하고 보호하기 위한 멀티클라우드 서비스 네트워킹 계층을 제공합니다. Consul은 널리 사용중인 솔루션으로, 많은 고객들이 자신의 환경에서 100,000개 이상의 노드를 실행하고 있습니다.

네트워킹 서비스는 IT팀이 서비스 레지스트리와 서비스 탐색 기능을 제공하는 중앙에서 제공되어야 합니다. 공통 레지스트리는 실행중인 서비스, 서비스 위치와 현재 상태에 대한 "맵"을 제공합니다. 레지스트리를 프로그래밍 방식으로 쿼리해 서비스 탐색을 실행하고, API 게이트웨이, 로드 밸런서, 방화벽, 기타 중요한 미들웨어 구성 요소의 네트워크 자동화를 실행할 수 있습니다. 이들 미들웨어 구성 요소는 동일한 기능을 제공하기 위해 프록시가 엣지에서 실행하는 서비스 메시 접근방식을 활용해 네트워크 외부로 이동할 수 있습니다. 서비스 메시 접근방식을 통해 네트워크 토폴로지, 특히 멀티클라우드와 멀티 데이터센터 토폴로지를 단순화할 수 있습니다.

Consul 도입 이전



Consul 도입 이후



3단계: 멀티클라우드 서비스 네트워킹

클라우드 운영 모델에서 네트워킹의 출발점은 일반적으로 공통 서비스 레지스트리이며, 실행중인 서비스, 서비스 위치, 현재 상태에 대한 실시간 디렉터리를 제공합니다. 네트워킹에 대한 전통적인 접근방식은 로드 밸런서와 가상 IP를 활용해 정적 IP로 서비스를 나타내는 네이밍 추상화를 제공하는 것입니다. 서비스의 네트워크 위치를 추적하는 프로세스는 종종 스프레드시트, 로드 밸런서 대시보드 또는 구성 파일의 형태를 하고 있으며, 분리된 모든 수동 프로세스는 이상적이지 않습니다.

Consul의 경우, 각 서비스는 프로그래밍 방식으로 등록되고 DNS와 API 인터페이스가 제공되어 다른 서비스에 의해 모든 서비스들이 검색될 수 있습니다. 통합 상태 검사는 각 서비스 인스턴스의 상태를 모니터링하므로 IT팀은 각 인스턴스의 가용성을 분류하고 Consul은 트래픽이 비정상 서비스 인스턴스로 라우팅되는 것을 방지할 수 있습니다.

Consul은 전통적인 로드 밸런서 등 north–south 트래픽을 관리하는 여타 서비스와 Kubernetes 등 분산 애플리케이션 플랫폼을 통합해 멀티 데이터센터, 클라우드, 플랫폼 환경에서 일관된 레지스트리와 검색 서비스를 제공할 수 있습니다.

네트워크 미들웨어 자동화

다음 단계는 네트워크 자동화를 통해 기존 네트워킹 미들웨어의 운영 복잡성을 줄이는 것입니다. 서비스 네트워크 위치나 구성이 바뀔 때마다 로드 밸런서와 방화벽을 재구성하는 수동적인 티켓 기반 프로세스 대신, Consul은 이러한 네트워크 운영을 자동화할 수 있습니다. 이는 네트워크 미들웨어 디바이스가 서비스 레지스트리에서 서비스 변경 사항을 구독(subscribe)할 수 있도록 함으로써 구현되며, 정적 기반 접근방식보다 훨씬 높은 수준으로 확장할 수 있는 매우 동적인 인프라를 실현합니다.

운영 담당자들은 독립적으로 애플리케이션을 배포하고 Consul에 게시할 수 있으며, NetOps팀은 Consul을 구독(subscribe)해 다운스트림 자동화를 처리할 수 있어 팀 간의 워크플로우가 분리됩니다.

서비스 메시를 통한 제로 트러스트 네트워킹

기업들이 마이크로서비스 기반 또는 클라우드 네이티브 애플리케이션을 통해 계속 확장함에 따라, 기반 인프라는 더욱 커지고 동적으로 변화하고 있으며 east–west 트래픽이 급증합니다. 이로 인해 단일 장애 지점(single points of failure)이 있는 네트워크 미들웨어가 무분별하게 확산되고 IT팀에 상당한 운영 부담을 안겨주고 있습니다.

Consul은 라우팅, 권한 부여 및 기타 네트워킹 기능을 미들웨어를 통해 구현하는 대신 네트워크의 엔드 포인트에 관련 정책과 기능을 주입하는 분산된 서비스 메시를 제공합니다. 이는 네트워크 토폴로지를 보다 간단하고 쉽게 관리할 수 있도록 하고, east-west 트래픽 경로 내에 LB같은 고가의 미들웨어에 대한 필요성을 없애며, 서비스 간 통신의 신뢰성과 확장성을 크게 높여 줍니다.

Consul은 각 서비스 인스턴스(Envoy, HAProxy, NGINX와 같은 프록시)와 함께 사이드카 프록시와 통합되는 API 기반 컨트롤 플레인입니다. 이들 프록시는 분산 데이터 플레인을 제공합니다. 이들 두 플레인은 함께 자동 TLS 암호화와 ID 기반 인증을 통해 서비스 간 통신을 보호하는 제로 트러스트 네트워크 모델을 실현합니다. 네트워크 운영과 보안팀은 IP 주소 대신 논리적 서비스를 통해 보안 정책을 정의할 수 있습니다.

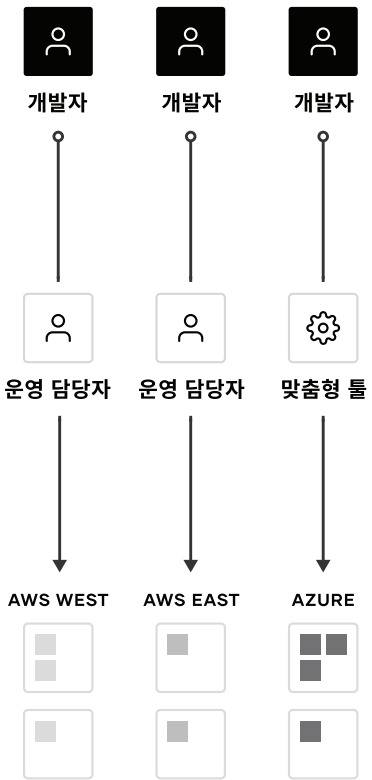
Consul은 자동 TLS 암호화와 ID 기반 인증을 통해 서비스 간 통신을 보호하기 위해 세분화된 서비스 세그먼트를 지원합니다. Consul은 중앙집중식 PKI와 인증서 관리를 위해 Vault와 통합할 수 있습니다. 서비스 구성은 환경을 가리지 않고 런타임에 서비스를 쉽게 구성하는 데 사용할 수 있는 API 기반 Key/Value 저장소를 통해 이루어집니다.

4단계: 멀티클라우드 애플리케이션 제공

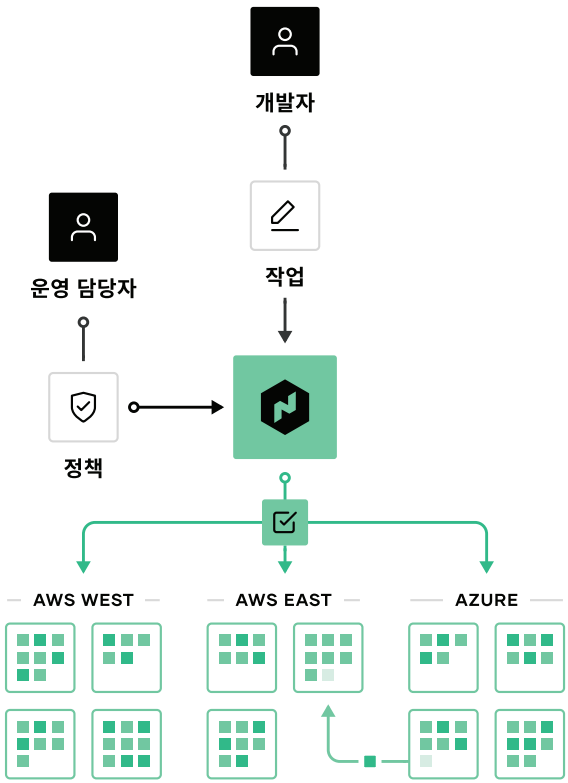
마지막으로, 애플리케이션 계층에서는 새로운 애플리케이션들이 분산, 배포되고 있고, 동시에 레거시 애플리케이션들도 보다 유연하게 관리할 필요성이 증가하고 있습니다. HashiCorp Nomad는 유연한 오케스트레이터로서, 기존 및 최신 애플리케이션을 배포하고 관리하고, 모든 종류의 워크로드(장시간 운영되는 서비스에서 단발성으로 실행되는 Batch, 시스템 에이전트 등)를 지원합니다.

애플리케이션 배포를 위한 쉐어드 서비스(Shared Services)를 위하여, IT팀은 Terraform, Vault와 Consul과 함께 Nomad를 사용하여 클라우드 인프라에서 애플리케이션을 일관되게 제공하고 필요한 컴플라이언스, 보안, 네트워킹 요구 사항은 물론, 워크로드 오케스트레이션과 스케줄링도 통합해야 합니다.

Nomad 도입 이전



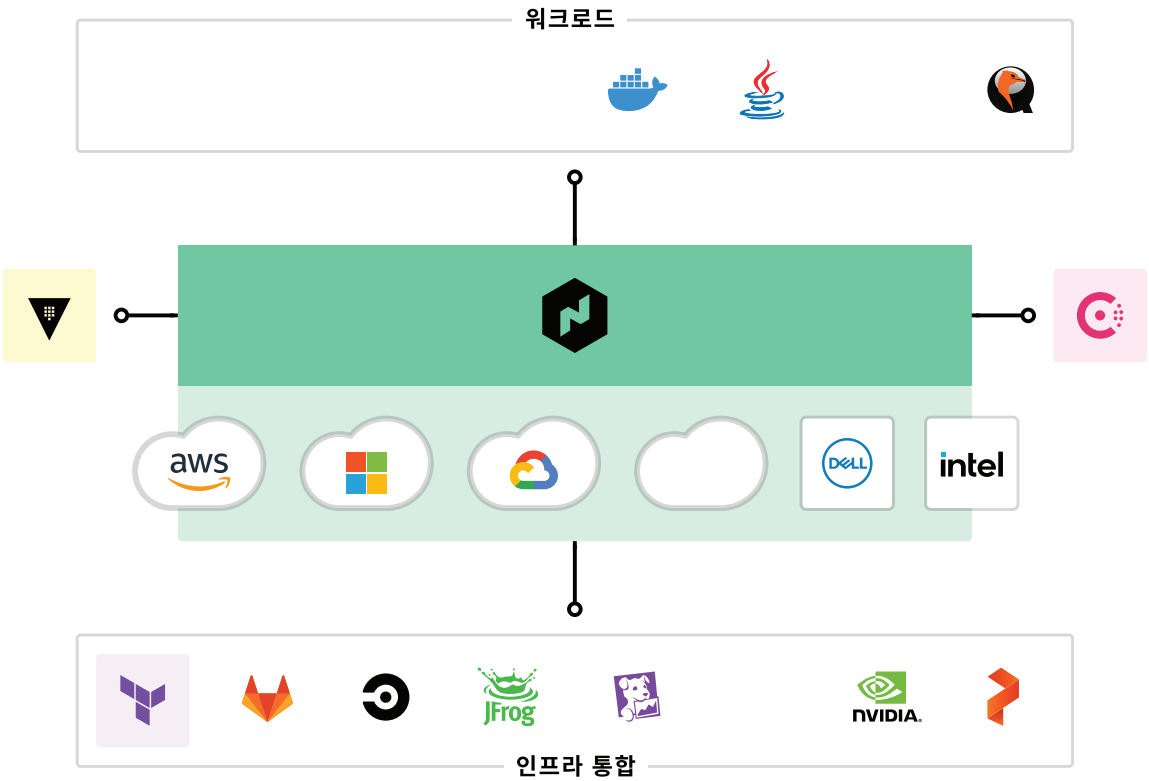
Nomad 도입 이후



다른 종류의 워크로드 오케스트레이션

많은 최신 워크로드는 Kubernetes 또는 기타 컨테이너 관리 플랫폼에 배포하기 위해 컨테이너로 패키징되어 개발됩니다. 그러나 많은 기존 워크로드는 이들 플랫폼으로 전환되지 않으며, 향후 Serverless 애플리케이션으로도 전환되지 않을 것입니다. Nomad는 독립 실행형 바이너리로 가상 머신에서 컨테이너에 이르기까지 모든 워크로드 배포를 위한 일관된 프로세스와 릴리스 자동화, 다중 업그레이드 전략, 빈 패킹(bin packing), 복원력 등 오케스트레이션의 주요 장점들을 제공합니다.

일반적으로 컨테이너에 내장된 최신 애플리케이션을 위해, Nomad는 다양한 환경과 운영 규모에서 동일한 일관된 워크플로우를 제공합니다. Nomad는 오케스트레이션과 스케줄링의 단순성과 효율성에 집중하여, 컨테이너 워크로드만을 운영하고 문제를 해결하기 위한 전문 기술이 필요한 Kubernetes와 같은 플랫폼의 복잡성을 미연에 방지합니다.



Nomad는 기존 CI/CD 워크플로우에 통합되어 레거시 워크로드와 현대의 워크로드를 위해 신속한 자동 애플리케이션 배포 기능을 제공합니다.

고성능 컴퓨팅

Nomad는 초대형 클러스터에서 지연 시간이 짧은(low latency) 애플리케이션을 스케줄링하도록 설계되었습니다. 고성능 컴퓨팅(HPC: High Performance Computing) 워크로드에서 흔히 그렇듯이, 이것은 대규모 배치 작업을 수행하는 고객에게 매우 중요합니다. 밀리언 컨테이너 챌린지(million container challenge)에서 Nomad는 데이터센터 세 곳에 있는 5,000대의 머신에 1백만 개의 Redis 인스턴스를 5분 안에 스케줄링하였습니다. 다수 Nomad 구축 환경은 훨씬 더 큰 규모로 운영되고 있습니다.

Nomad를 통해 고성능 애플리케이션들이 쉽게 API를 사용해 용량을 동적으로 조절할 수 있고, Spark처럼 데이터 분석 애플리케이션을 위한 리소스를 효율적으로 공유할 수 있습니다. 짧은 지연시간 스케줄링(Low latency Scheduling)은 빠른 시간 내 결과 제공을 보장하고, 낭비되는 유휴 리소스를 최소화할 수 있습니다.

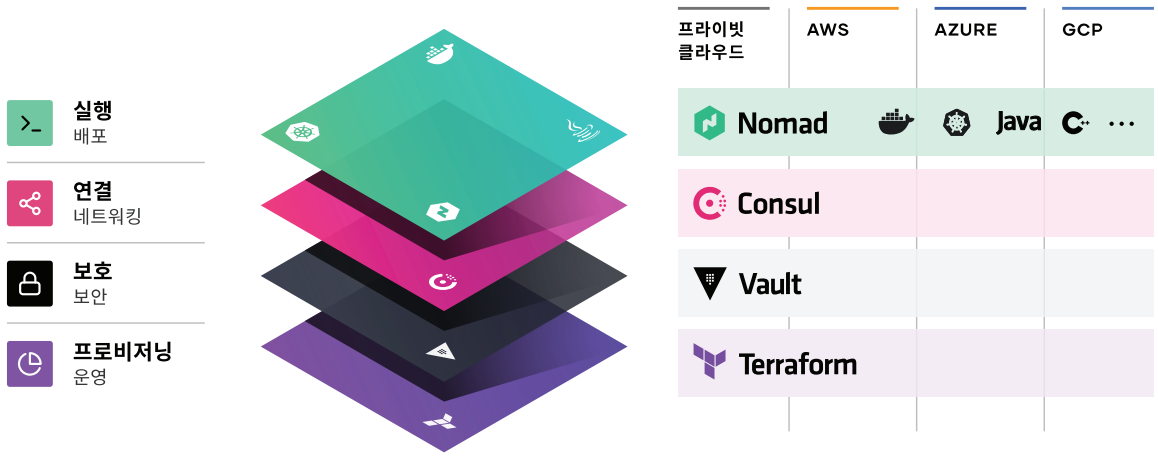
멀티 데이터센터 워크로드 오케스트레이션

Nomad는 멀티 리전, 멀티 클라우드를 위해 설계되었으며, 모든 워크로드를 배포하는 일관된 워크플로우를 제공합니다. 여러 데이터센터 또는 클라우드 경계를 넘어 글로벌 애플리케이션을 배포함에 하는 경우, Nomad는 애플리케이션들이 성공적으로 배포될 수 있도록 인프라, 보안, 네트워킹 리소스 및 정책의 지원을 받아 해당 애플리케이션을 오케스트레이션하고 스케줄링하는 기능을 제공합니다.

5단계: 기업용 애플리케이션 배포 프로세스

궁극적으로 인프라, 보안, 네트워킹 및 애플리케이션 런타임 전반에 걸친 이 쉐어드 서비스(Shared Services)는 애플리케이션 배포를 위한 기업용 프로세스를 제공하는 동시에, 클라우드 각 계층의 동적 특성을 활용합니다.

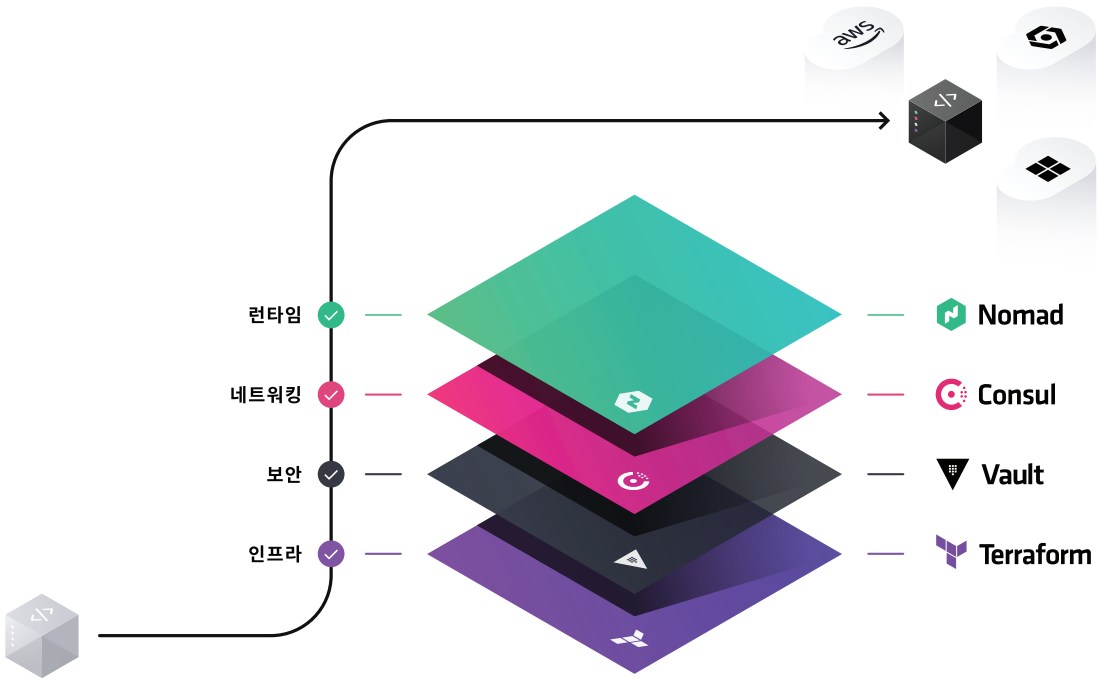
클라우드 운영 모델을 채택하면 완벽하게 규정을 준수하고 통제되는 셀프서비스 IT를 통해 팀은 더 빠른 속도로 애플리케이션을 배포할 수 있습니다.



결론

일반적인 클라우드 운영 모델은 디지털 트랜스포메이션 노력을 극대화하려는 기업들에게 필수적인 변화입니다. HashiCorp 제품들은 기업들의 클라우드 운영 모델 도입을 가능하게 하는 클라우드 서비스 계층별 솔루션 제공을 목표로 하고 있습니다.

엔터프라이즈 IT는 비용 최적화에 초점을 맞춘 ITIL 기반 통제에서 탈피해 속도 최적화에 초점을 맞춘 셀프서비스 인에이블러(enabler)로 진화해야 합니다. 새로운 비즈니스와 빠른 고객 가치 전달을 지원할 수 있도록 클라우드의 각 계층 전반에 쉐어드 서비스(Shared Services)를 제공함으로써 이를 구현할 수 있습니다.



공통 클라우드 운영 모델의 채택을 통해 최신 멀티클라우드 데이터센터에서 가치를 실현하는 가장 빠른 길로 들어선다는 것은 다음과 같이 엔터프라이즈 IT의 특성을 변화시키는 것을 의미합니다.

- **사람: 멀티 클라우드 스킬로 전환**
  - 내부 데이터센터 관리와 단일 클라우드 벤더의 스킬을 재사용하고 모든 환경에서 일관되게 적용합니다.
  - DevSecOps와 그외 애자일 실행 방식을 수용하여, 일회성, 분산형 시스템을 지속적으로 배포할 수 있습니다.

- **업무 프로세스: 셀프서비스 IT로 전환**
  - 중앙화된 IT를 애플리케이션 제공 속도에 초점을 맞춘 쉐어드 서비스(Shared Services)로 포지셔닝 합니다. 위험을 최소화하면서 매번 소프트웨어를 더 빠르게 제공할 수 있습니다.
  - 셀프서비스 역량 제공을 위해 클라우드 각 계층 전반에 CoE(Centers of Excellence)를 구축합니다.

- **도구: 동적 환경으로 전환**
  - 증가하는 인프라 및 애플리케이션의 일시성(ephemerality)과 분산성을 지원하며, 특정 기술에 종속되지 않으면서 중요한 워크플로우를 지원하는 툴을 사용합니다.
  - 셀프서비스 환경에서 리스크 관리를 위한 컴플라이언스와 배포 속도를 맞추기 위한 정책, 거버넌스 도구를 제공합니다.

HashiCorp 소개

HashiCorp은 멀티클라우드 인프라 자동화 소프트웨어 분야의 리더입니다. HashiCorp 소프트웨어 제품군을 통해 기업들은 일관된 워크플로우를 채택함으로써 애플리케이션 종류와 인프라에 관계없이 프로비저닝, 보안, 네트워크 및 애플리케이션 배포를 수행할 수 있습니다. HashiCorp의 오픈 소스 툴인 Vagrant, Packer, Terraform, Vault, Consul, Nomad는 매년 수천만 번 다운로드되며 글로벌 2000대 기업들에 의해 광범위하게 채택되고 있습니다. 이들 제품의 엔터프라이즈 버전은 오픈소스 툴을 향상시켰으며 협업, 운영, 거버넌스 및 멀티 데이터센터 기능을 한층 강화했습니다. 샌프란시스코에 본사를 두고 있으며 Mayfield, GGV Capital, Redpoint Ventures, True Ventures, IVP 및 Bessemer Venture Partners의 지원을 받고 있습니다. 더 자세한 내용은 **www.hashicorp.com**을 방문해 확인할 수 있습니다. 또는 Twitter **@HashiCorp**으로 HashiCorp를 팔로우하십시오.


HashiCorp