



귀사가 구상하는 미래에 클라우드가 있습니까?

*클라우드 마이그레이션을 계획해야
하는 이유와 그 방법*

- 2 서론
- 3 클라우드가 귀사에 적합한 솔루션입니까?
- 4 어떤 애플리케이션을 마이그레이션해야 합니까?
- 5 애플리케이션을 마이그레이션할 때 알맞은 방식은 무엇입니까?
- 9 클라우드상의 애플리케이션을 어떻게 보호합니까?
- 11 마이그레이션한 애플리케이션을 어떻게 관리하고 유지 보수합니까?
- 13 다음 단계

서론

많은 기업에게 클라우드 이전은 불가피한 선택입니다. 북미 지역의 기업들을 대상으로 한 설문 조사에서 응답자의 95%가 지난 1년간 중요 애플리케이션 및 IT 인프라를 클라우드로 마이그레이션했다고 밝혔습니다.¹ 또 다른 설문 조사에서는 응답자의 인프라 중 80%가 평균 14개월 내에 클라우드로 이전할 것으로 나타났습니다.²

이처럼 클라우드 열풍이 거세지는 이유는 무엇일까요? 클라우드를 통해 유연성과 확장성을 강화하고 설비 투자(CapEx) 중심에서 운영 비용(OpEx) 중심으로 비용 모델을 전환하는 등 여러 중요한 이점을 누릴 수 있다는 점에 기업들은 주목합니다.

그러나 안타깝게도 작업의 범위를 제대로 파악하지 않고 마이그레이션에 뛰어드는 경우가 너무 많습니다. 준비 부족으로 인해 심각한 사태가 벌어지고 결국 프로젝트가 교착 상태에 빠지거나 재작업에 막대한 비용이 들곤 합니다.

귀사의 애플리케이션도 클라우드로 마이그레이션해야 합니까? 그렇다면 클라우드 여정을 어떻게 시작하시겠습니까?

클라우드 마이그레이션에 나서기 전에 다음 사항을 우선적으로 고려해야 합니다.

- 클라우드가 귀사에 적합한 솔루션입니까?
- 어떤 애플리케이션을 마이그레이션해야 합니까?
- 애플리케이션을 마이그레이션할 때 알맞은 방식은 무엇입니까?
- 클라우드에서 각 애플리케이션과 해당 데이터를 어떻게 보호해야 합니까?
- 마이그레이션한 애플리케이션을 어떻게 관리하고 유지 보수합니까?



모든 선택 사항을 철저히 평가하고 충분한 시간을 투자하여 계획 프로세스를 완료한다면 마이그레이션에 성공하고 클라우드의 이점을 극대화할 가능성을 높일 수 있습니다.

성공적인 클라우드 마이그레이션의 단계



1. 선택 사항 평가
2. 귀사의 특별한 비즈니스 케이스에 따라 조기에 철저한 계획 수립
3. 마이그레이션 실시
4. 클라우드에서 계속 혁신에 주력
5. 운영 및 유지 보수

적용 사례를 포함하여 이 단계에 대한 자세한 내용은 ibm.com/cloud/migration에서 확인하십시오.

클라우드가 귀사에 적합한 솔루션입니까?

왜 귀사의 애플리케이션을 클라우드로 이전해야 할까요? 클라우드에서 애플리케이션을 실행하면 필요에 따라 온디맨드로 IT 리소스를 사용할 수 있어 더 민첩한 운영이 가능해집니다. 반면 온프레미스 솔루션에서는 이와 같은 리소스를 사용하려면 추가 단계를 거쳐야 합니다.

게다가 설비 투자의 부담을 줄일 수 있으며, 애플리케이션 실행을 위해 새 서버를 도입할 필요 없이 종량과금제 방식의 운영 비용 모델로 전환할 수 있습니다. 그리고 필요에 따라 확장하거나 축소 하면서 사용한 만큼만 지불하면 됩니다. 단기간 급증하는 사용량도 수용할 수 있습니다. 즉 새 서버를 구매했다가 수요 감소로 사용률이 저조한 수준에 머무르는 문제가 없습니다.

또한 새 장비를 도입하지 않고도 최신 하드웨어 기술을 활용할 수 있습니다. 클라우드 제공업체가 하드웨어를 업그레이드하면 귀사의 애플리케이션도 혜택을 누리게 됩니다.

뿐만 아니라 대개의 경우 보안 수준도 향상됩니다. 클라우드는 물리적 하드웨어와 네트워크부터 소프트웨어와 인력에 이르기까지 스택의 전 범위에서 다양한 보안 옵션을 제공할 수 있습니다.

애플리케이션을 클라우드로 마이그레이션할 경우 엄청난 가치를 누릴 수 있으나, 귀사의 기술 팀과 가깝게 일하지 않는 이해관계자에게 이러한 장점을 설명하는 것은 쉽지 않습니다. 먼저 [여기](#)서 귀사가 하나 이상의 애플리케이션을 클라우드로 마이그레이션하여 어떤 효과를 거둘 수 있는지 확인하십시오. 그리고 다시 이 백서로 돌아와 성공적인 마이그레이션을 계획하는 방법을 알아보십시오.

이 애플리케이션이 클라우드에서 더 진가를 발휘할까요?

클라우드 마이그레이션이 상당한 시간과 리소스가 집중되는 프로세스가 될 수도 있습니다. 애플리케이션을 이전하기 전에 과연 클라우드에서 호스팅하는 것이 실제로 유익할지 따져봐야 합니다. 포트폴리오의 각 애플리케이션을 평가하면서 이렇게 물어보십시오.

클라우드에서 더 우수한 성능을 발휘할까, 더 안전해질까, 아니면 더 효과적인 애플리케이션이 될까?

이 첫 질문에 대한 답이 아니라면 해당애플리케이션의 어느 부분이라도 클라우드 마이그레이션을 통해 나아질 수 있는지 생각해 보십시오. 그런 영역이 있으면 써드파티 SaaS(Software-as-a-Service) 오퍼링으로 대체할 수 있습니다. 이를테면 자체 개발한 메일 서버 또는 거추장스러운 온프레미스 데이터베이스를 클라우드 버전으로 대체하여 다른 온프레미스 애플리케이션을 뒷받침할 수 있습니다.

애플리케이션의 일부를 클라우드로 이전하면 단기적 확장의 효과를 누릴 수 있습니다. 1년 중 어떤 때는 사용률이 저조했다가 특정 시점에 사용이 집중되는 애플리케이션도 있을 것입니다. 이러한 경우 필요에 따라 클라우드 컴퓨팅 리소스를 추가하거나 제거할 수 있는 클라우드 확장 능력을 이용하면 됩니다. 이런 대안이 초기에는 비용 부담이 더 클 수도 있으나, 이미 확실한 기반을 가진 클라우드 벤더와의 파트너십으로 안정성과 신뢰성을 높이면 IT 부문의 마이그레이션 및 유지 보수 부담이 줄어듭니다.



클라우드가 해결책이 아닐 때



애플리케이션의 어떤 영역도 클라우드에서 큰 효과를 볼 수 없다면 무리해서 추진하지 마십시오. 매우 민감한 성격의 정보를 다루거나, 사용상의 제한 또는 규제 준수상의 제약 때문에 온프레미스 환경이 더 적합한 애플리케이션도 있습니다.

그러한 애플리케이션의 예는 다음과 같습니다.

- USB 키 또는 동글이 필요한 애플리케이션
- 인터넷 액세스가 차단된 환경에서 또는 에어갭 네트워크에서 사용해야 하는 애플리케이션
- 법적 요건 때문에 온프레미스를 벗어날 수 없는 데이터 세트

이러한 애플리케이션을 영원히 온프레미스 환경에 가둘 필요는 없습니다. 퍼블릭 클라우드의 보안, 성능, 경제성이 향상되면 굳이 온프레미스에 애플리케이션을 남겨야 하는 이유도 줄어들 것입니다.

어떤 애플리케이션을 마이그레이션해야 합니까?

마이그레이션을 시작하기 전에 무엇을 왜 마이그레이션하는지 이해해야 합니다. 기본 클라우드 마이그레이션 전략은 이전할 애플리케이션의 수를 기준으로 해야 합니다. 단일 애플리케이션이나 공유 리소스(데이터베이스, 메일 서버 등)를 이전할 것인지, 아니면 연관된 애플리케이션의 클러스터 혹은 포트폴리오 전체를 이전할 것인지 결정해야 합니다.

당장의 목표로 시야를 한정해서는 안 됩니다. 지금은 애플리케이션 하나만 마이그레이션하더라도 결국 모든 것을 클라우드로 이전하게 될 수도 있습니다. 동시에 마이그레이션하는 애플리케이션이 많을수록, 더 수고스럽겠지만 서비스 또는 데이터를 공유하는 애플리케이션을 한꺼번에 마이그레이션하면 재작업이 줄고 비호환성의 문제가 최소화됩니다. 모든 애플리케이션을 동시에 배치하면 클라우드에서 제대로 작동하고 있는지 확인하기 쉽습니다.

단일 애플리케이션 마이그레이션

성능 확장성의 이점을 누리하고자 단일 공유 리소스만 클라우드로 이전하고 포트폴리오의 나머지는 온프레미스에 두는 경우도 있습니다. 하이브리드 환경을 구성할 때 사용자와 다른 애플리케이션이 이 애플리케이션과 어떻게 상호 작용하는지 파악하면서 워크플로우가 끊기지 않게 하십시오. 또한 데이터 소스 누락, 종속성 미충족, 신규 액세스 프로토콜로 인한 혼란으로 어설픈 마이그레이션이 되는 것을 막을 수 있습니다.

단일 애플리케이션을 마이그레이션할 경우 그로 인해 생성되는 하이브리드 환경에서 2가지 기본 옵션을 통해 데이터 전송을 관리할 수 있습니다. VPN을 사용하여 클라우드 애플리케이션과 온프레미스 포트폴리오 간의 보안 회선을 구성하거나, 보안 API를 사용하여 두 플랫폼이 주고받는 데이터를 자동으로 읽고 기록합니다. 싱글 사인온(SSO) 페더레이션을 도입하면 사용자가 새 환경에서 문제 없이 연결할 수 있습니다.

연계 애플리케이션 마이그레이션

애플리케이션 제품군이나 단일 워크플로우 중심의 애플리케이션 세트를 마이그레이션해야 하는 경우 종속성 문제를 최소화하도록 애플리케이션 이전 순서를 관리하는 것이 관건입니다. 모든 애플리케이션을 마이그레이션할 때까지 서비스를 보류하는 것이 가장 안전한 방법이지만, 여의치 않을 때도 있습니다.

온프레미스 애플리케이션을 신속하게 폐기해야 한다면 종속 관계가 가장 많은 애플리케이션부터 시작하고 종속 관계가 가장 적은 애플리케이션을 맨 나중에 하십시오. 그러면 마이그레이션할 공유 서비스의 수가 모든 애플리케이션이 클라우드에 호스팅되는 시점까지 점차 감소하므로 재작업의 부담을 덜 수 있습니다.

포트폴리오 전체 마이그레이션

클라우드에 애플리케이션을 이전할 때 최대 과제는 작동중단시간(downtime)을 최소화하는 것입니다. 리스크 허용 한도와 속도 사이에서 아슬아슬하게 줄타기하는 셈입니다. 클라우드에서 가장 큰 효과를 거둘 것이므로 우선적으로 리소스를 투입해야 할 애플리케이션과 전략적 중요도가 상대적으로 낮고 리호스팅으로 비용과 수고를 절약할 수 있는 애플리케이션을 결정하려면 애플리케이션 포트폴리오를 프로파일링해야 합니다. 전환에 앞서 면밀한 테스트를 통해 대규모 마이그레이션의 전반적인 리스크를 줄여야 합니다. 하지만 혹시라도 어떤 종속 관계가 누락될 경우에 대비하여 비상 대응 계획을 마련해야 합니다.

American Airlines: 레거시 소프트웨어를 클라우드로 이전



도전과제: American Airlines는 안정적이면서 비용 효율적으로 디지털 환경을 확장하여 고객이 기대하는 신속한 정보 액세스를 제공하길 원했습니다.

해결책: American Airlines는 서비스 수명이 끝난 인프라 플랫폼에서 실행 중이던 애플리케이션을 IBM Cloud™ 기반 VMware HCX로 마이그레이션하여 곧바로 기술적 효율성과 경제적 효율성의 이점을 누리기 시작했습니다. 이 항공사는 이러한 효율성의 이점을 누리면서 레거시애플리케이션을 마이크로 서비스 아키텍처로 구성된 새로운클라우드 기반 애플리케이션으로 점차 대체해 나갈 것입니다.

이점: American Airlines는 비용을 줄이고 애플리케이션 개발 속도를 높이며 최종 고객 응대 시간을 단축했습니다.

[자세히 보기](#)

애플리케이션을 마이그레이션할 때 알맞은 방식은 무엇입니까?

애플리케이션과 데이터를 클라우드 마이그레이션하는 방법은 하나만 있는 것은 아닙니다. 다양한 경로와 클라우드 서비스 옵션이 있습니다. 먼저 얼마나 많은 백엔드 인프라를 지원할 것인지 결정해야 합니다. IaaS(Infrastructure-as-a-Service) 솔루션을 사용할지, 아니면 PaaS(Platform-as-a-Service) 솔루션을 사용할 것인지 결정합니다. 그런 다음 포트폴리오의 애플리케이션별로 마이그레이션 전략을 개발하되, 애플리케이션 고유 요구 사항에 부합하는 방식을 선택합니다.

백엔드 지원

클라우드에 애플리케이션을 이전할 때 IaaS 솔루션으로 온프레미스 서버를 대체하거나 PaaS 솔루션으로 운영 체제 및 서버 소프트웨어를 대체하여 애플리케이션을 가상화할 수 있으며, 혹은 이 두 가지 방법을 모두 적용할 수도 있습니다.

IaaS 솔루션

IaaS 솔루션은 100% 호스팅 클라우드 환경을 제공하며, 클라우드 제공업체가 모든 서버 유지 보수 및 프로비저닝을 맡습니다. 고객의 애플리케이션이 안전한 데이터 센터에 호스팅되고, 할당된 서버는 자동으로 확장되면서 필요에 따라 더 강력한 성능을 제공합니다. IaaS 솔루션은 대체로 종량과금지 방식입니다. 즉 고객이 실제로 사용하든 안 하든 여러 랙을 채울 만한 수의 서버를 구매하고 유지 관리 비용을 부담하는 것이 아니라 실제로 사용된 리소스에 대해서만 비용을 지불합니다. 이러한 접근 방식은 계절별 수요가 있거나 사용이 불규칙한 애플리케이션에 특히 안성맞춤입니다.

IaaS 제공업체가 정기적으로 서버를 최신 모델로 업그레이드하므로 고객은 새 장비를 계속 구매하지 않아도 첨단 기술을 활용할 수 있습니다. 제대로 유지 보수되는 최신 시스템을 사용하므로 고객의 가동시간(uptime)도 높은 수준으로 유지할 수 있습니다. 다만 IaaS 제공업체의 작동중단시간이 곧 귀사 애플리케이션의 작동중단시간임을 잊지 마십시오.

Think Research: 더 힘들일 필요 없는 스마트한 업무 환경



도전과제: 의사들이 이용하는 지식 기반 툴 및 첨단 임상 콘텐츠를 개발하는 기업, Think Research 는 더 빠르고 간단한 방식으로 IT 인프라를 관리할 방법이 필요했습니다.

해결책: Think Research 는 IBM의IaaS 및 PaaS 솔루션을 선택했습니다.

이점: Think Research 의 DevOps 팀은 일상적인 유지 보수 작업을 IBM Cloud 팀에 맡기고 더 우수한 툴 개발에 집중할 수 있게 되었습니다. 그 덕분에 솔루션 개발 속도가 빨라졌습니다.

[동영상 보기](#)

PaaS 솔루션

PaaS 솔루션이 운영 체제 및 모든 서버 소프트웨어를 관리하므로, 고객은 일상적인 운영 환경 유지 보수의 부담에서 벗어날 수 있습니다. 온프레미스 서버에 배치하거나, 대개는 IaaS 솔루션과 함께 배치합니다.

PaaS를 온프레미스 환경에 배치하는 경우 고객이 하드웨어를 선택합니다. 성능, 패치, 보안, 가동시간을 관리할 책임은 여전히 고객에게 있습니다. 이 방식으로 배치 속도를 높이고 효과적으로 비용을 관리할 수 있습니다.

우수한 PaaS 오퍼링을 선택하면 기존 플랫폼보다 더 효과적으로 서비스를 공유하고 업그레이드를 이행할 수 있습니다. 이 방식을 적용하려면 애플리케이션의 하이퍼바이저가 PaaS 플랫폼과의 호환성을 제공해야 합니다. 그렇지 않으면 클라우드에 맞게 애플리케이션을 다시 디자인해야 할 수도 있습니다. 가상 머신(VM) 모니터라고도 하는 하이퍼바이저는 가상 머신을 생성하고 실행하는 핵심 프로세스입니다. 하이퍼바이저는 메모리, 프로세싱 등의 리소스를 가상으로 공유하는 방식으로 단일 호스트 컴퓨터에서 여러 게스트 가상 머신을 지원할 수 있게 합니다. 이 방식으로 시스템 사용률 및 IT 가용성을 높일 수 있습니다.

이는 가상 머신이 하드웨어 독립적이어서 서로 다른 서버 사이클 수월하게 오갈 수 있기 때문입니다. 귀사의 제공업체가 호환 가능한 가상화를 제공하는지 확인하거나 VMware와 같은 업계 표준 하이퍼바이저를 사용하십시오.

CaaS 솔루션

가상 머신과 하이퍼바이저를 사용하는 대신 애플리케이션 컨테이너를 활용하여 모든 호스트 레벨 관리를 플랫폼 제공업체에 맡기는 방법도 있습니다.

각 컨테이너에 단일 애플리케이션과 그 애플리케이션 실행에 필요한 모든 소프트웨어가 들어 있습니다. 그러면 애플리케이션 레벨에서 격리가 이루어지므로 리소스 사용량이 많은 애플리케이션 때문에 다른 애플리케이션이 피해를 입을 염려가 없습니다.

컨테이너를 사용하면 배치 및 테스트가 간소화됩니다. 컨테이너를 재구성할 필요 없이 손쉽게 복사한 다음 즉시 실행 가능한 애플리케이션을 클라우드에 직접 보내면 됩니다.

IBM Cloud Kubernetes Service에서 제공하는 컨테이너에서 기존 클라우드 또는 온프레미스 호스팅보다 더 수준 높은 보안까지 실현할 수 있습니다(그림 1). 컨테이너 레벨에서 활동을 모니터링하므로 관리자는 허가받은 애플리케이션과의 상호 작용만 가능합니다. 이러한 제한 덕분에 악의적인 관리자에 의해 데이터가 손상될 위험을 줄이고 자동화된 암호화로 데이터를 안전하게 지킬 수 있습니다.

적합한 컨테이너 방식을 선택하면 성능 개선에도 도움이 될 수 있습니다. 예를 들어 IBM은 베어메탈에서 애플리케이션 컨테이너를 실행하는 것을 지원합니다. 하이퍼바이저나 운영 체제 없이 애플리케이션을 실행함으로써 애플리케이션에서 이용 가능한 프로세싱 리소스를 극대화합니다.

그러나 컨테이너 방식에는 잠재적 문제점이 있습니다. 이를테면 각 애플리케이션이 독립형 환경에 있으므로 업데이트나 패치를 컨테이너마다 배포해야 합니다. 컨테이너 방식을 활용할 경우 Docker(IBM Cloud Kubernetes Service의 필수 요소)와 같은 솔루션을 통해 업데이트 일정을 잡고 여러 컨테이너에 배포할 수 있습니다.

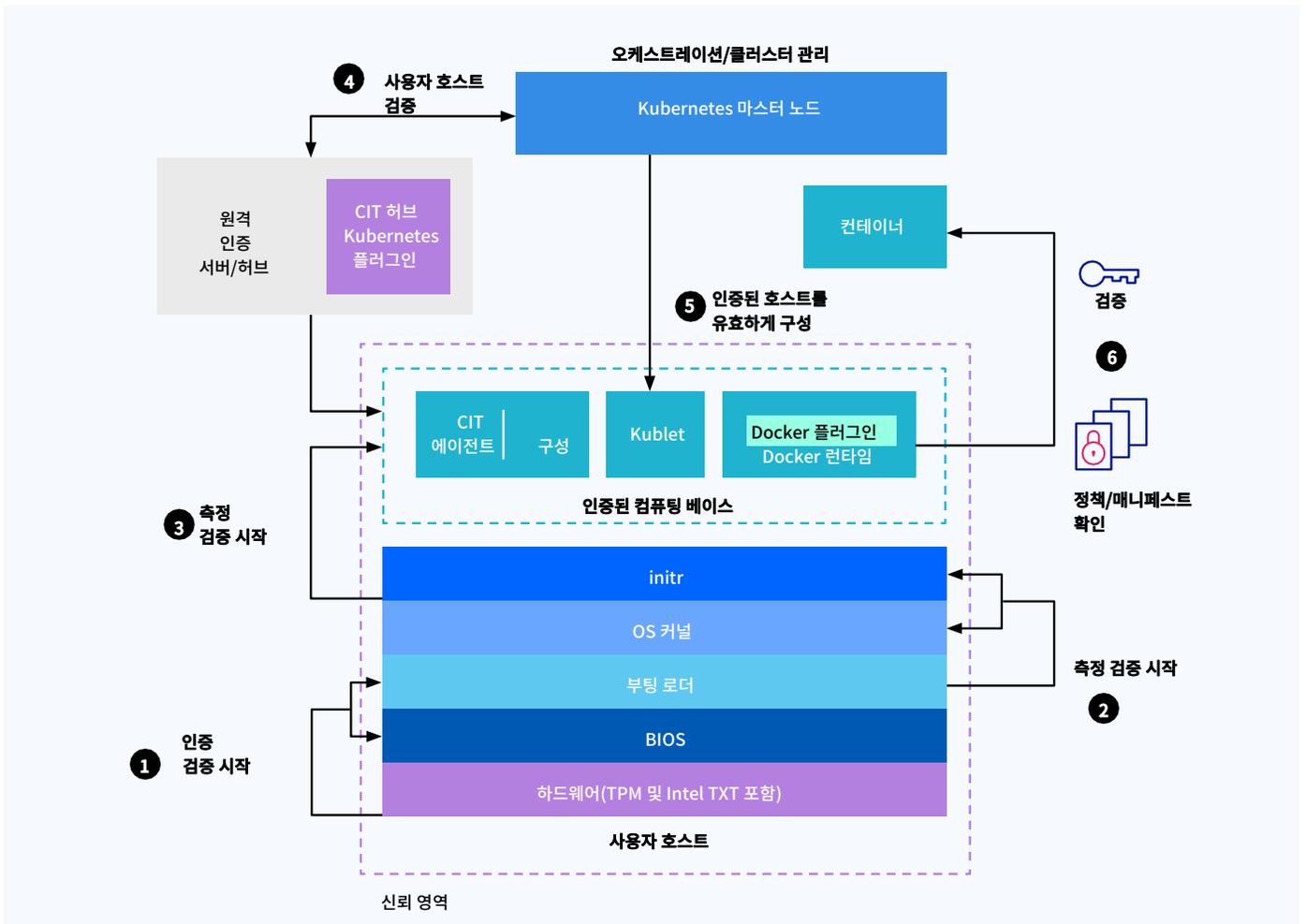


그림 1. IBM Cloud Kubernetes Service는 하드웨어 기반 신뢰 체인으로 컨테이너 보안을 실현합니다. 보안 정책을 토대로 컨테이너 플랫폼의 전 범위에 서 그 안전성이 확인된 호스트 및 컨테이너만 자동으로 실행합니다. 이 신뢰 체인은 클라우드 마이그레이션 도입의 최대 걸림돌인 보안 부실에 대한 우려 해 소에 핵심적인 역할을 합니다. 컨테이너 보안에 대해서는 [IBM 백서](#)에서 자세히 알아보십시오.

호스팅 형태의 퍼블릭 클라우드

퍼블릭 클라우드 데이터 센터에 애플리케이션을 호스팅할 수도 있습니다. 호스팅 형태의 퍼블릭 클라우드 솔루션은 확장 가능한 성능, 원격 액세스, 데이터 유출 차단, 종합적인 보안 및 하드웨어 제어 등 퍼블릭 클라우드의 여러 이점을 제공합니다.

많은 기업이 퍼블릭/프라이빗 하이브리드 클라우드를 구축하고 관리하면서 온프레미스에서 애플리케이션을 실행하다가 퍼블릭 클라우드로 확장하여 단기 수요를 해결하고 비용을 통제하거나 데이터 센터 환경을 통합합니다.

애플리케이션 준비

애플리케이션은 현재 상태로 이전할 수 있을까요 아니면 클라우드에 맞게 재개발해야 할까요? 클라우드 환경에 맞게 준비를 갖춘 일부 애플리케이션의 경우, 애플리케이션 변경 없이 클라우드의 가치를 극대화하도록 설계된 마이크로서비스를 기본 제공합니다. 그렇지 않다면 애플리케이션을 클라우드로 이전하여 클라우드의 확장성 혜택을 제대로 누리기 위해 어느 정도의 수고까지 감수할 것인지 결정해야 합니다.

현재 상태로 애플리케이션 이전

재개발 없이 애플리케이션 전체를 가상 환경으로 이전하는 방식의 가장 큰 장점은 속도입니다. 개발 시간을 확보하기 위해 마이그레이션을 늦출 필요 없습니다. 많은 클라우드 서비스가 배치 프로세스의 자동화를 지원하므로 간편하게 여러 애플리케이션을 리호스팅할 수 있습니다.

클라우드로 이전하면 다양한 이점을 누리게 됩니다. 대개 퍼블릭 클라우드 데이터 센터는 사내 데이터 센터보다 더 효과적으로 유지 보수되고 더 안전한 편입니다. 게다가 재해 복구와 같은 문제를 훨씬 더 강력하게 제어할 수 있습니다. 예컨대 IBM Cloud는 보안 슬라이싱(secure slicing)을 제공하는데, 이는 더 확실한 복구를 위해 자동으로 데이터를 세 곳의 데이터 센터에 나눕니다. 즉 이 무료 기능으로 세 곳의 데이터 센터에서 데이터를 리호스팅할 수 있으며, 이 기능은 아무리 비효율적인 애플리케이션이라도 유용하게 작용합니다.

OSRAM: 훨씬 더 민첩하게 업계의 변화에 대처



도전과제: OSRAM은 경쟁이 치열한 시장 환경에서 앞서 나가기 위해 더 민첩한 IT 인프라가 필요했습니다.

해결책: IBM과 함께 새로운 애플리케이션과 레거시 애플리케이션을 클라우드로 마이그레이션했습니다. OSRAM은 사내 IT 팀의 지원 부담을 줄이기 위해 IBM® 서비스를 선택했습니다.

이점: 이 마이그레이션으로 OSRAM은 연간 수백만 달러를 절감했을 뿐만 아니라 경쟁사를 제치고 여러 신규 계약을 체결하는 성과를 거뒀습니다. 그리고 이제는 일년 내내 하루 24시간 제공되는 인프라 지원 덕분에 안심할 수 있게 되었습니다.

[추가 자료](#)

단점도 있습니다. 클라우드 환경에 대한 준비가 되지 않은 애플리케이션은 더 많은 컴퓨팅 리소스를 사용합니다. 종량과금제 모델의 클라우드 제공업체를 이용하는 경우, 리호스팅할 레거시 애플리케이션이 너무 많으면 막대한 비용이 들 수 있습니다. 그럴 바에야 리소스를 많이 사용하는 애플리케이션을 서둘러 리팩토링하고자 할 것입니다.

애플리케이션 재작성 또는 리팩토링

시간과 리소스가 있다면 애플리케이션의 전체나 일부를 재작성(rewrite)하거나 리팩토링(refactor)할 수 있습니다. 오래된 레거시 애플리케이션은 완전히 새롭게 개발하면서 최신 기능을 추가하고 애플리케이션을 현대화하면 효과적일 것입니다. 그 밖의 애플리케이션은 클라우드를 제대로 활용하도록 약간만 변경하면 됩니다. 즉 특정 서비스를 SaaS 오피어링으로 대체하거나 더 효과적으로 리소스를 관리하도록 애플리케이션을 변경합니다.

그러면 애플리케이션에서 클라우드 컴퓨팅의 이점을 십분 누릴 수 있지만, 마이그레이션 전에 몇 가지 단계를 거쳐야 합니다. 더 많은 개발자, 디자이너, 아키텍트가 투입되어 클라우드에 맞게 소프트웨어를 최적화해야 하는데, 이러한 투자로 상당한 효과를 거둘 수 있습니다.

또 다른 지원이 필요한 고객을 위해 IBM은 [IBM Cloud Garage](#)에서 포괄적인 애플리케이션 디자인 서비스를 제공합니다. 이 서비스는 애플리케이션 구상부터 배치까지 8주 내에 완료할 수 있도록 뒷받침하며, 고객의 팀이 새롭게 클라우드에 준비된 애플리케이션을 관리할 수 있도록 교육 리소스도 제공합니다.

애플리케이션 대체

이 단계에서는 과연 현재 버전의 애플리케이션을 클라우드로 이전하는 것이 귀사가 원하는 바인지 심사숙고할 필요가 있습니다. 중요하게 여겨지는 애플리케이션의 상당수는 동일한 벤더 또는 유사한 벤더가 제공하는, 사전 구성된 SaaS 오피어링으로 대체할 수 있습니다. 그러면 초기 비용 부담이 다소 높더라도 개발, 호스팅, 마이그레이션 비용을 절약하고 가치 창출까지의 시간을 단축함으로써 투자한 만큼의 가치를 회수할 수 있습니다.

클라우드상의 애플리케이션을 어떻게 보호합니까?

일부 CPO(Chief Privacy Officer)와 CIO(Chief Information Officer)는 클라우드 보안에 대해 우려를 표합니다. 중요 데이터를 써드파티 데이터 센터와 같은 오프사이트에 보내는 것이 위험하게 보일 수 있기 때문입니다.

하지만 많은 클라우드 솔루션은 온프레미스 환경에 못지않게 안전하거나 더 안전합니다. 클라우드 마이그레이션 계획에 디지털 보안, 데이터 보안, 인증 톨, 액세스 제한을 포함시켜 함께 검토하십시오.

1. 디지털 보안

디지털 침입 위험으로부터 애플리케이션을 보호하는 것은 절대적으로 필요합니다. 특히 데이터가 원격 디바이스로 전송될 때 각별한 주의가 요구됩니다. 대다수 퍼블릭 클라우드 제공업체가 보유한 보안 및 규제 준수 기능은 일반 기업들이 자체적으로 제공할 수 있는 수준을 능가합니다.

예를 들어 IBM Cloud는 물리적 계층, 네트워킹 계층, 소프트웨어 계층의 3단계 보안을 제공합니다. 이러한 다층적 보안으로 단일 장애 지점을 방지합니다. 침입 탐지 및 차단 시스템의 영역을 인터넷으로 확장하여 외부 보안 위협을 막습니다. 운영 체제의 아래에서 작동하는 암호화 및 보호 기술, 즉 Intel TXT(Trusted Execution Technology), TPM(Trusted Platform Module) 등으로 BIOS 레벨에서도 무단 접근 및 변조 위험으로부터 데이터를 보호할 수 있습니다.

2. 데이터 보안

엄격한 개인 정보 보호 기준을 유지하고 적용하려면 추가적인 보증이 필요할 때가 있습니다. BYOK(bring-your-own-key) 보안이 해결책이 될 수 있습니다. BYOK에서는 고객이 직접 암호화 키를 생성, 관리, 저장합니다. 클라우드 서비스 제공업체가 그 키를 애플리케이션에 전달하여 고객 측의 최종 사용자를 위한 데이터를 암호화하고 해독하지만, 그 키나 데이터 자체에 직접 액세스할 수는 없습니다. 이러한 방식으로 보안을 한층 더 강화하고 고객에게만 데이터 액세스를 허용합니다.



IBM Cloud는 **Key Protect** 기능으로 고객이 관리하는 암호화를 지원합니다(그림 2). 고객이 Key Protect API에서 자신의 암호화 키를 애플리케이션에 가져와 데이터를 암호화하고 해독합니다. IBM에 키를 공개할 필요 없습니다. 이 키는 FIPS 140-2 Level 2이며, 삭제 시 복구 불가능한 방식으로 폐기되므로 서버의 데이터를 확실히 보호할 수 있습니다. 단순하게 마음의 평안을 가져다 주는 것에 그치지 않습니다. 암호화 키를 완벽하게 제어할 수 있다는 것은 CISO 감사에서 꼭 갖춰야 할 구성 요소 중 하나입니다.

IBM Cloud는 TLS/SSL(Transport Layer Security/Secure Sockets Layer) 프로토콜을 사용하여 전송 중인 데이터도 보호합니다. 이 기능으로 누군가가 고객의 귀중한 데이터를 가로챌 것을 막을 수 있습니다.



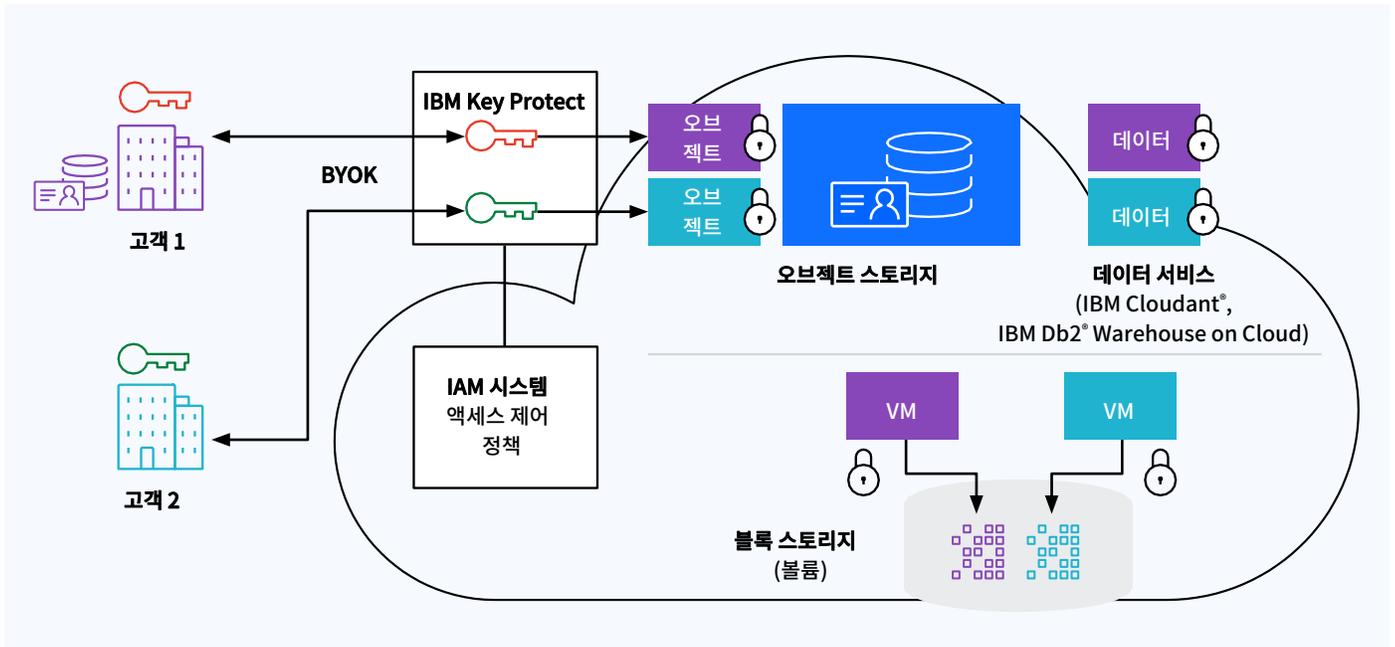


그림 2. Key Protect 클라우드 기반 보안 서비스가 제공되는 BYOK 솔루션의 아키텍처

3. 인증 틀

이제는 온프레미스의 특정 시스템에서만 애플리케이션을 사용하는 것이 아니므로, 액세스 제어가 더욱 중요해집니다. 워크플로우가 눈에 띄게 느려지는 일 없이 사용자를 정확히 인증할 수 있어야 합니다. 물리적 디바이스(예: 인증용 전화 앱, 동글)와 비밀번호를 함께 사용하는 이중 인증으로 무단 액세스를 훨씬 더 어렵게 만듭니다. SSO 프로토콜이 공유 ID 페더레이션을 지원하므로, 사용자가 동일한 로그인 정보로 여러 사이트에 액세스할 수 있으나 사이트 각각에 실제 ID 자격 증명을 공개할 필요 없습니다.

4. 액세스 제한

온프레미스 환경에서 클라우드로 이전한다면 직원들이 원격으로 애플리케이션과 관련 데이터에 액세스할 수 있게 됩니다. 데이터가 클라우드 서버에 안전하게 있더라도 직원들의 디바이스에 있는 데이터를 보호할 수 있는 더 강력한 보안이 필요합니다.

전체 디스크 암호화를 구현할 뿐만 아니라 어떤 디바이스가 클라우드 애플리케이션에 액세스할 수 있는지 결정하는 정책을 마련하여 시행하는 것도 고려해야 합니다. 관리자의 액세스 권한도 검토하고 조정해야 합니다. 관리자 레벨로 클라우드 환경에 접속할 수 있는 사람의 수를 제한함으로써 모든 사람의 데이터 및 애플리케이션에 영향을 미칠 만한 돌발적 활동이나 악의적 활동의 위험성을 최소화합니다.

마이그레이션한 애플리케이션을 어떻게 관리하고 유지 보수합니까?

최상의 클라우드 마이그레이션 및 개발 전략이라면 배치 후 유지 보수에 대해서도 다뤄야 합니다. 신중하게 계획된 클라우드 배치로 IT 및 시스템 관리자의 워크로드를 간소화할 수 있습니다. 클라우드 애플리케이션에서 온프레미스 애플리케이션과 다른 방식으로 확장, 패치, 업그레이드가 이루어진다는 점을 기억해야 합니다. 마이그레이션에 앞서 이러한 차이점을 제대로 이해하면 구현 후 워크플로우가 간단해집니다.

클라우드 성능 관리

기업이 클라우드로 애플리케이션을 마이그레이션하는 주된 이유 중 하나가 확장성입니다. 기존 온프레미스 환경에서는 프로세스 리소스를 추가하려면 새 서버를 구매, 구성 및 설치해야 합니다. 그러나 IaaS 환경에서는 탄력적으로 리소스를 확장하면서 예기치 않은 서버 수요도 수용할 수 있습니다.

이러한 확장은 배후에서 일어나므로 애플리케이션 성능을 계속 면밀하게 모니터링하면서 급격한 사용량 변동이 예상되면 이를 최소화하고 애플리케이션 작동중단을 야기할 만한 중대한 버그를 찾아내는 것이 여전히 중요합니다. 가장 손쉽게 원격 애플리케이션을 지켜보는 방법은 클라우드 서비스 모니터를 이용하는 것입니다. 클라우드 벤더가 급격한 사용량 변동을 추적하고 예측하는 툴을 제공하면서 비효율성 및 충돌 문제를 처리해야, 고객이 우수한 가용성 및 저렴한 사용 비용의 혜택을 누릴 수 있습니다.

애플리케이션 업그레이드 및 패치

클라우드에서 애플리케이션을 호스팅하면 훨씬 더 수월하게 애플리케이션 성능을 최고 수준으로 유지할 수 있습니다. 하지만 애플리케이션이 아무리 잘 설계되었다고 뭔가를 바꾸거나 개선하거나 바로잡아야 하는 때가 오기 마련입니다.

어떤 기업은 플랫폼, 서버 심지어 애플리케이션까지 클라우드 서비스 제공업체가 유지 보수하는 것을 선호합니다. 그러한 경우, 클라우드 서비스 구현 방식을 선택할 때 고객이 어느 정도로 애플리케이션에 대한 제어 권한을 행사할지 고려해야 합니다.

- **SaaS:** 고객이 패치 또는 업데이트를 관리하지 않습니다. 서비스 제공업체가 모든 유지 보수를 담당합니다.
- **PaaS:** 고객은 애플리케이션에 패치를 적용하고 서버를 업그레이드할 수 있으나, 운영체제나 하이퍼바이저에는 액세스하지 못합니다.
- **IaaS:** 고객은 애플리케이션, 운영 체제, 하이퍼바이저에 패치를 적용할 수 있으나, 서버에 대해서는 어떤 변경도 하지 못합니다.





클라우드는 SaaS 구현 외에도 배포 후 유지보수 측면에서 강력한 이점을 제공합니다. 온프레미스 애플리케이션은 전사적 범위에서 수천 대까지는 아니더라도 수백 대의 컴퓨터에 설치될 수 있습니다. 그러나 클라우드 애플리케이션은 다수의 사용자가 단일 설치 환경에 액세스하는 것입니다. 애플리케이션의 새 버전을 배치하면 모든 사용자가 자동으로 그 새 버전에 액세스하게 됩니다.

하지만 이 방식에서는 패치 또는 업그레이드 과정에서 상당한 주의를 기울여야 합니다. 패치 또는 업그레이드 적용 시 모든 사용자가 한꺼번에 클라우드 애플리케이션을 사용하지 못하므로 운영 전반이 중단될 수도 있습니다.

장시간의 작동중단 없이 클라우드 소프트웨어의 유지 보수를 수행하는 가장 쉬운 방법은 클라우드에 호스팅되어 있는 버전에 패치를 적용하지 않고 업데이트 버전을 새로 배치하는 것입니다. 그러면 테스트 시간을 대폭 단축하고 성능을 개선함과 동시에 모든 사용자가 가장 우수한 최신 버전에 액세스하게 할 수 있습니다. 즉, 업데이트 버전을 배치하는 즉시 새 버전으로 전환하면 되는 것입니다. 애플리케이션 컨테이너를 사용하는 경우, Docker나 Istio와 같은 관리 시스템을 사용하지 않는 한, 수정 프로그램을 복수의 애플리케이션에 적용할 때 컨테이너마다 별도로 패치를 적용하거나 배포해야 합니다.

클라우드에 적응하기



클라우드로 마이그레이션할 때 워크플로우, IT 정책 및 비즈니스 관행을 바꿔야 하는 경우가 많습니다. 귀사의 애플리케이션을 클라우드로 마이그레이션할 계획이 있다면 전사적 차원에서 클라우드식 사고로 전환할 수 있도록 다음 팁을 기억하고 실천하십시오.

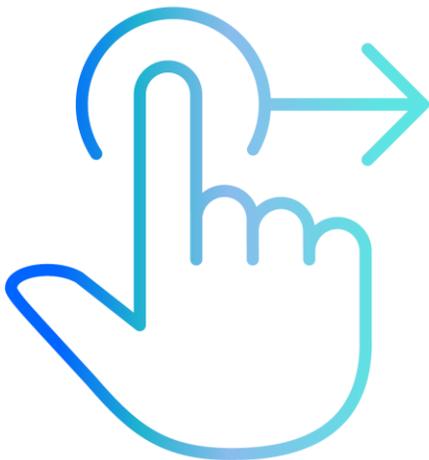
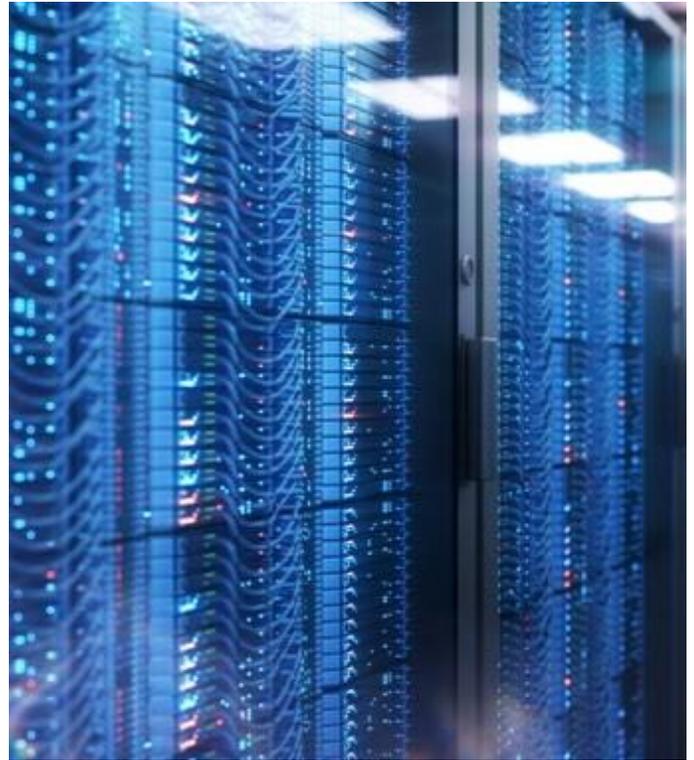
- **투명성 확보:** 경과 보고 및 문의 접수에서구심점이 될 마이그레이션 팀을 구성합니다. 다가가기 쉬운 프로젝트의 얼굴 역할을 부여하면 거시적 관점에서 마이그레이션의 원활한 진행을 뒷받침할 수 있습니다.
- **가치 입증:** 비교적 쉬운 목표, 즉 최소한의 개발작업으로 마이그레이션할 수 있는 애플리케이션을 찾아 배치함으로써 마이그레이션의 초기 단계에 성과를 거둬 클라우드 컴퓨팅의 이점을 입증합니다.
- **우려사항 해결:** 클라우드를 잘 모르는 이들은 보안문제 또는 워크플로우 차질을 과대평가하곤 합니다. 보안 장치가 마련되어 있음을 입증하여 이러한 우려를 미리 잠재웁니다.
- **차질 최소화:** 가급적 워크플로우에 영향을 주지 않도록 이전 일정을 계획합니다. 세일즈 킥오프 시점에 CRM을 마이그레이션하는 것은 바람직하지 않습니다. 회계 연도 마감 시점에 재무 소프트웨어를 교체해서는 안 됩니다. 가능하다면 온프레미스 환경을 폐기하기 전에 모든 애플리케이션을 배치하십시오. 그러면 애플리케이션의 연동을 테스트하고 사용자에게 완전한 경험을 제공할 수 있습니다.
- **지원 활용:** IBM Services가 원활한 마이그레이션 준비에 필요한 리소스와 컨설팅을 제공할 수 있습니다.

다음 단계

마이그레이션 계획을 수립했다면 이제 구현할 차례입니다. 마이그레이션 팀을 조직하고 애플리케이션별로 정한 전략을 이행하십시오. 마이그레이션 가능한 애플리케이션이면 마이그레이션하고 그렇지 않은 것은 교체하십시오. 가장 쉬운 애플리케이션부터 마이그레이션을 진행하여 추진력을 얻고 클라우드의 가치를 입증한 다음 점차 더 까다로운 마이그레이션으로 진행합니다.

클라우드에 애플리케이션을 옮기든, 클라우드 환경에서 바로 쓸 수 있도록 준비된 새로운 애플리케이션을 개발하든, 아니면 레거시 소프트웨어를 SaaS 솔루션으로 대체하든 상관 없이 어떤 경우라도 신뢰할 수 있는 기술, 툴, 전문성 및 서비스의 4박자를 모두 갖춰야 마이그레이션을 완료할 수 있습니다.

IBM은 1960년대 시분할 메인프레임으로부터 현재의 고성능 인프라 및 API에 이르기까지 수십 년 동안 클라우드 컴퓨팅 분야에서 신뢰받는 파트너의 자리를 지켜 왔습니다. IBM Services와 함께라면 아무리 복잡한 배치 시나리오라도 설계하고 계획을 세운 후 실행에 옮길 수 있습니다. [IBM Cloud 사이트](#)에서 여러 IaaS, PaaS, SaaS 마이그레이션 옵션에 대해 자세히 알아보십시오.





추가 정보

클라우드 마이그레이션 및 IBM에서 제공하는 관련 기술/서비스에 대해 ibm.com/cloud에서 자세히 알아보십시오.

새로운 소식

IBM Cloud 블로그

IBM 팔로우

@IBMcloud

Facebook

직접 만나는 IBM

LinkedIn

YouTube

© Copyright IBM Corporation
2018

IBM Cloud
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2018년 8월

IBM, IBM 로고, ibm.com, Cloudant, Db2, IBM Cloud 및 IBM Cloud Managed Services는 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹(ibm.com/legal/copytrade.shtml)에 있습니다.

이 문서는 최초 발행일을 기준으로 하며, 통지 없이 언제든지 변경될 수 있습니다. IBM이 영업하는 모든 국가에서 모든 오퍼링이 제공되는 것은 아닙니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 타인의 권리침해에 대한 보증이나 조건을 포함하여(단, 이에 한하지 않음) 명시적이든묵시적이든 일체의 보증 없이 "현상태대로" 제공됩니다. IBM 제품은 제품이제공되는 계약의 조건에 따라 보증됩니다.

법적 요구사항을 준수하는지 확인해야 할 책임은 IBM 고객에게 있습니다. 고객의 영업에 영향을 줄 수 있는 모든 관련 법률 및 규정과 이러한 법률을 준수하는 데 필요한 모든 조치를 식별하고 해석하기 위해 적절한 법률 고문의 자문을 구하는 것은 전적으로 고객의 책임입니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스 및 제품은 고객이 관련 법률을 준수하고 있음을 진술하거나 보증하지 않습니다.

¹ SolarWinds, "IT Trends Report: Portrait of a Hybrid IT Organization", North America 2017; <http://it-trends.solarwinds.com/reports/2017/portrait-of-a-hybrid-it-organization/north-america.pdf>.

² McAfee, "Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security", 2018년 4월 <https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html>.