COHESITY

백서

최신 데이터 보안 및 관리 토폴로지: IT 리더를 위한 가이드

위험을 줄이고 비즈니스 레질리언스를 강화하기 위한 청사진 및 모범 사례

목차

서론

세 가지 요인으로 인해 데이터 보안 및 관리에 대한 새로운 접근 방식이 필요합니다. 첫 번째는 디지털 전환과 API 기반 인프라의 필수 요소입니다. IT 리더는 IT 자산의 모든 측면을 현대화하여 더 큰 자동화, 확장성, 클라우드 규모, 소프트웨어 정의 아키텍처 및 "시프트 레프트(shift left)" 보안 원칙을 지원하고 있습니다.

둘째, 사이버 위협 환경은 복잡하고 예측할 수 없는 방식으로 진화하고 있습니다. 많은 조직의 기존 데이터 자산은 사일로화되어 사이버 공격으로 인한 운영 위험이 커집니다. 최근 조사에 따르면, 조직의 32%는 구식 백업 및 복구 시스템으로 인해 빠른 복구 시간이 방해받고 있다고 생각하는 것으로 나타났습니다. 마찬가지로, 34%는 IT 팀과 보안 팀 간의 통합 부족으로 인해 복구 시간이 길어진다고 답했습니다.

셋째, AI의 등장으로 인해 리더들은 생성형 AI 기술이 기업 데이터에 접근할 수 있도록 하는 최신 데이터 플랫폼을 검색하게 되었습니다.

데이터 현대화 프로젝트를 주도하는 모든 IT 경영진은 "거인의 어깨에 서서" 이익을 얻을 수 있습니다. 이 백서에서는 가장 중요한 설계 고려 사항과 일반적인 기업 요구 사항을 고려할 때 최상의 데이터 레질리언스 접근 방식을 달성하는 방법을 설명합니다. 수천 건의 배포에 걸친 경험과 모범 사례에 대한 지식을 통해 우리의 관점이 형성되었습니다.

다음 지침은 공급업체에 구애받지 않지만, 단순화를 위해 Cohesity 브랜드 이름을 사용합니다.

주요 설계 요소

가치 있는 모든 현대화 프로젝트는 위험을 수반합니다. 이는 기업 데이터 보안 및 관리 프로세스와 도구를 전환할 때 확실히 적용됩니다. 하지만 좋은 소식이 있습니다. 다른 사람들이 전에 해 왔던 작업을 바탕으로 구축할 수 있습니다. 많은 조직이 데이터 자산을 성공적으로 현대화했으며, 이 백서에서 이러한 모범 사례를 정리했습니다.

IT 및 사이버 보안 리더는 IT 자산 전반에 걸쳐 민첩성, 위험 및 비용의 균형을 유지해야 합니다. 이 자산은 동적이며, 이제 온프레미스 데이터 센터, 퍼블릭 클라우드, 코로케이션 시설 및 엣지 위치에서 실행되는 데이터 및 앱을 포괄합니다. 앱, 데이터 및 데이터 소스의 엄청난 양이 혼합되면서 시간이 지남에 따라 현대화 노력의 규모와 범위가 증가합니다.

기업 데이터 자산의 현대화는 다음과 같은 이유로 더욱 복잡해집니다.

- 다양한 위치 및 여러 워크로드의 다양한 인프라 대상으로 인한 데이터 단편화 및 비효율적인 백업 및 복구 프로세스 발생
- 대부분의 조직 내에서 충분한 IT 및 사이버 보안 기술 부족
- 1분마다 수백 건의 공격이 발생하는 등 사이버 보안 환경이 급변하고 있습니다. 공격의 진화와 정교함으로 인해 조기 식별이 매우 중요해집니다.

그러나 명심해야 할 몇 가지 “첫 번째 원칙”이 있습니다.

3:2:1 규칙은 여전히 적용됩니다.

3:2:1 규칙에 따르면 데이터 사본을 최소 3개 이상 보관해야 하고, 이러한 백업은 두 가지 유형의 미디어 또는 플랫폼에 저장해야 하며, 사본 중 하나 이상을 외부에 보관해야 합니다.

3:2:1 규칙의 지속적인 가치는 클라우드 기반 시대에도 시스템 토폴로지 설계를 계속 추진하는 세 가지 개념에서 비롯됩니다.

- 비즈니스 요구 사항
- 장애 도메인
- 천재지변

이러한 각 개념에 대해 자세히 설명하겠습니다. 이들은 항상 업계의 핵심 중점 사항이었으며, 특히 사이버 공격에 대한 우려가 높아짐에 따라 오늘날에도 여전히 그러합니다. 사이버 공격이 항상 가장 중요한 것은 아니었지만, 지금은 확실히 그렇습니다.

이 세 가지 개념이 시간이 지남에 따라 백업 및 복구 설계에 영향을 미친 방법을 정의하고, 사이버 공격에 대한 우려로 인해 고객이 기존 배포 토폴로지가 여전히 충분한지(또는 충분하지 않은지) 자문해야 하는 방법에 대해 논의합니다.

하나씩 살펴봅시다.

비즈니스 요구 사항

기업은 광범위한 비즈니스, 규제 및 규정 준수 요건을 준수해야 합니다. 이러한 요구 사항 중 상당수는 현재 및 과거 데이터 사본의 보존 필요성을 뒷받침합니다. 예를 들어, 규정 준수 팀은 업계 규제 기관의 요청에 대응하기 위해 3년

된 계약을 철회해야 할 수 있습니다. 또는 세무팀이 진행 중인 감사를 위해 파일을 복구해야 할 수도 있습니다. 또는 좀 더 공감할 만한 이야기로, 중요한 파일이 실수로 삭제되어 복원해야 할 수도 있습니다.

장애 도메인

IT 업계에서는 소프트웨어와 하드웨어가 모두 장애가 있을 것으로 잘 알려져 있습니다. 하드웨어 및 소프트웨어 공급업체는 이러한 불가피한 상황을 중심으로 설계하기 위해 특별한 노력을 기울이지만, 장애는 계속됩니다. IT 팀은 장애에 대한 계획을 수립하고, 이러한 장애가 조직 또는 비즈니스에 부정적인 영향을 미치지 않도록 해야 합니다. 장애의 예로는 VM 또는 스토리지 볼륨 손상과 같은 워크로드 장애 또는 장애 OS 패치 구현이 있습니다. 두 경우 모두 IT 팀은 장애로부터 복구해야 하며, 복구의 일환으로 백업 및 복구 시스템의 데이터가 필요할 수 있습니다.

수십 년 전, 리더들은 악의적인 공격자로 인한 장애에 대해 걱정할 필요가 없었습니다. 오늘날 사이버 공격은 시스템 장애의 핵심 동인일 뿐만 아니라 가장 눈에 띄는 장애 원인이기도 하며, 이사회의 관심을 끄는 원인이기도 합니다.

천재지변

이 용어는 인간의 통제를 벗어난 자연재해 또는 기타 사건을 말하며, 합리적인 방법으로 예측하거나 예방할 수 없습니다. 화재, 지진, 홍수 및 케이블 절단과 같은 부작용은 모두 "천재지변"으로 간주될 수 있습니다. 장애 도메인과 마찬가지로, IT 조직은 천재지변의 가능성을 고려하고 이에 대한 레질리언스가 갖춰진 설계 시스템을 구축해야 합니다.

3:2:1 규칙은 천재지변에 직면하여 실질적인 지침을 제공합니다.

시스템에 장애가 발생할 수 있으므로 여러 데이터 사본을 사용할 수 있는 것이 좋습니다. 장애 도메인으로 인해 백업을 두 가지 다른 미디어 유형 또는 시스템에 보관하는 것도 합리적입니다. 마지막으로, 천재지변으로 인해 이러한 사본 중 하나 이상을 재해 복구 사이트 또는 원격 데이터 센터의 일부로 원격 위치에 보관하는 것이 책임 있는 거버넌스입니다.

요구 사항은 다를 수 있지만 공통점이 존재합니다.

3:2:1 규칙은 견고한 관행이지만, 조직은 3개 미만의 사본을 배포하는 것을 선택할 수 있습니다. 다른 사람들은 3:2:1 규칙을 더 엄격하게 준수합니다. 3개 이상의 사본을 보관하는 사람도 있습니다. (이 백서의 뒷부분에서 이러한 설계 선택에 대한 근거를 설명하겠습니다.)

설계와 관련하여 배포 토폴로지("청사진")를 세 가지 유형으로 그룹화했습니다.

유형	설명
베이직	사본이 2개 이하인 배포 토폴로지
향상된 기능	3개의 사본이 있는 배포 토폴로지
미션 크리티컬	4개 이상의 사본이 있는 배포 토폴로지

익숙한 가용성 아키텍처는 오늘날에도 여전히 유효합니다

숙련된 IT 리더와 실무자들에게 보다 익숙할 용어인 가용성 아키텍처로 넘어가겠습니다.

가용성 아키텍처는 IT 팀이 하드웨어 및 소프트웨어 시스템을 구성하여 잠재적인 중단에 대한 레질리언스를 확보하는 방법을 설명합니다. 당사의 경험상 대부분의 기업 배포는 ***액티브-액티브, 액티브-대기, 허브 앤 스포크의 세 가지 고객 가용성 아키텍처 중 하나로 구성됩니다***.

이러한 각 접근법은 다음 페이지에 나와 있습니다.

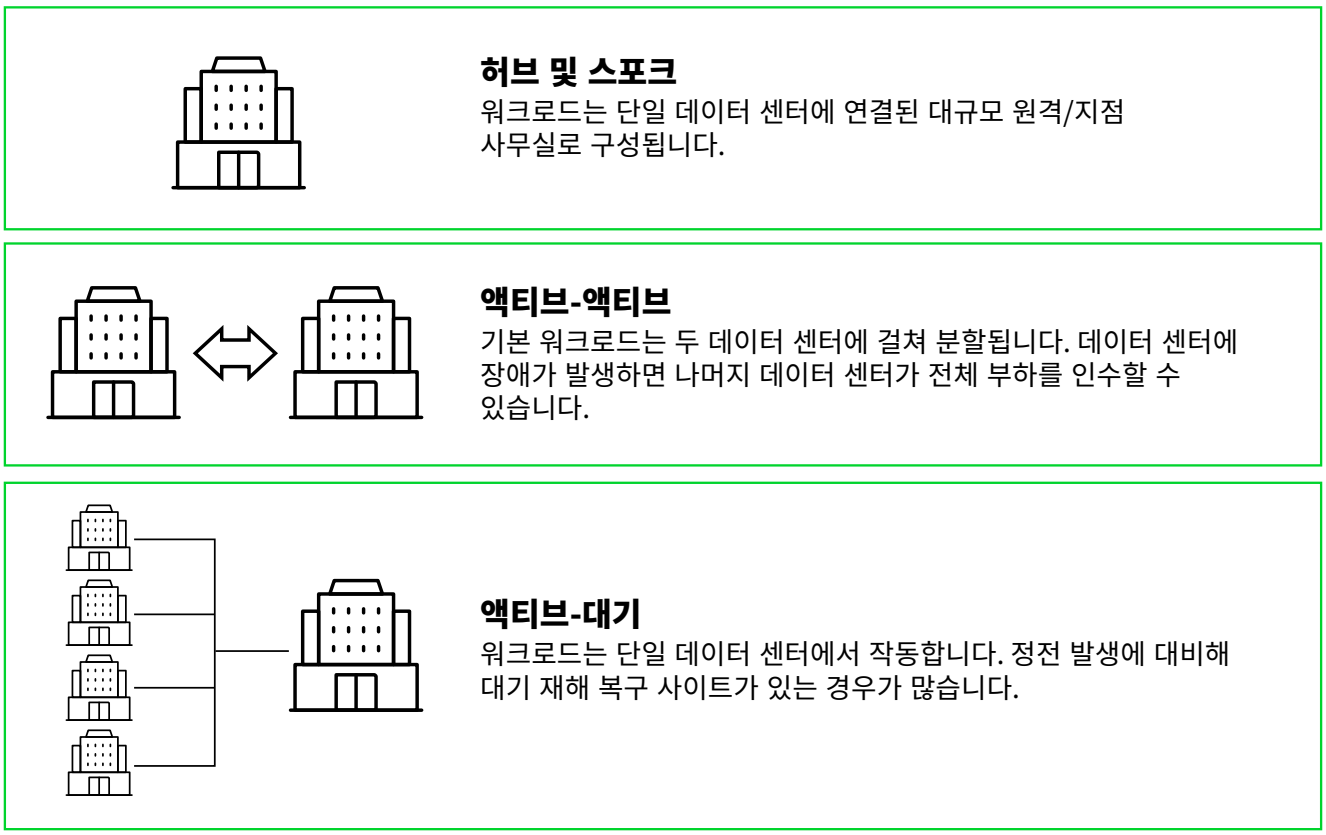


그림 1: 고객 가용성 아키텍처

각 경우에 가용성 아키텍처는 장애 발생 시 비즈니스 운영을 계속할 수 있도록 설계되었습니다. **액티브-대기** 아키텍처의 "액티브" 측에 장애가 발생하면 모든 처리가 다른 대기 시스템으로 전환됩니다. **액티브-액티브** 시스템의 어느 한 쪽에 장애가 발생하면 다른 쪽은 워크로드의 100%를 떠맡습니다. **허브 앤 스포크** 시스템에 장애가 발생하는 경우, 예를 들어 하드웨어 장애 또는 지점의 다른 문제로 인해 데이터가 파괴되는 경우, 장애의 원인이 해결되면 허브에서 시스템과 해당 데이터를 복원할 수 있습니다.

책임 있는 IT 팀은 이러한 가용성 아키텍처를 설계하고 정기적으로 테스트하여 레질리언스 메커니즘이 제대로 작동하는지 확인합니다.

당사의 모범 사례 청사진 세트는 이러한 입증된 가용성 아키텍처에 기반을 두고 있습니다. Cohesity에서는 백업 및 복구 시스템을 진공 상태로 배포하지 않습니다. 당사는 기본 IT 인프라와 긴밀하게 일치하도록 설계합니다. 이 백서의 뒷부분에서 다양한 백업 및 복구 토폴로지 및 이러한 토폴로지가 IT 가용성 아키텍처에 어떻게 매핑되는지에 대해 다룰 때 자세히 살펴보겠습니다.

최신 데이터 보안 및 관리를 위한 청사진: 유형 및 토폴로지

우리는 이미 기본, 강화 및 미션 크리티컬 백업 유형에 대해 논의했습니다. 이제 이러한 유형과 관련된 토폴로지를 소개합니다.

하지만 먼저 몇 가지 정의를 살펴보겠습니다. 데이터 보안 및 관리 시스템은 다양한 방법을 통해 데이터를 저장할 수 있습니다. 데이터 사본은 ***백업, 복제본*** 또는 ***아카이브로 보관할 수 있습니다***.

몇 가지 경험적 원칙은 다음과 같습니다.

- **백업**은 기본 복사본으로 구성되며 중복 제거, 압축 및 암호화된 데이터가 생성됩니다. 이러한 처리 작업은 데이터에 대해 한 번 수행한 다음 처리된 백업 데이터를 복제본 또는 아카이브에 복사할 수 있습니다.
- **복제본**은 일반적으로 단기 보관에 사용되며, 일반적으로 수개월이지만 수년은 아닙니다. 이러한 복제본은 액티브-액티브 또는 액티브-대기 등의 IT 가용성 아키텍처를 지원하는 경우가 많습니다.
- **아카이브**는 일반적으로 장기 보존에 사용되며, 수년 동안 보관되는 경우가 많습니다. 아카이브는 종종 규정 준수 및 규제 목적으로 사용되지만, 경우에 따라 IT 가용성 아키텍처에도 사용됩니다.
- **백업 또는 복제본에서 복원**하는 것은 1단계 프로세스이며, 2단계 프로세스인 아카이브에서 복원하는 것보다 빠릅니다. 아카이브는 IT 시스템으로 복원되기 전에 업체의 백업 및 복구 시스템에 다운로드해야 합니다.
- **랜섬웨어 공격으로부터 복원하는 것**은 가장 최근 백업이 아닐 가능성이 높은 깨끗하고 감염되지 않은 사본으로 복원해야 하기 때문에 복잡합니다. 조직은 단순히 천재지변으로 인한 도메인 장애 또는 중단으로부터 복원하는 것과 같은 방식으로 랜섬웨어 공격으로부터 복원할 수 없습니다. 영향을 받는 조직은 환경을 분석하고, 복구되는 사본에 애초에 공격을 유발한 악성코드 감염이 없는지 확인해야 합니다.

토폴로지 목록은 아래 표에 나와 있습니다. 모든 토폴로지에는 데이터가 중복 제거, 압축 및 암호화되는 단일 백업이 있습니다. 백업 외에도, 다양한 토폴로지는 하나 이상의 복제본 및 하나 이상의 아카이브 또한 유지할 수 있습니다. 각 토폴로지 유형에 설명자(B1, B2, E1, E2, M1, M2 등)를 제공하여 이를 추적하는 데 도움이 되도록 했습니다.

유형	사본	토폴로지/사본 유형
베이직	1	B1 - 백업
	2	B2 - 백업 및 아카이브
	2	B3 - 백업 및 복제
향상된 기능	3	E1 - 백업, 복제 및 아카이브
	3	E2 - 백업 및 이중 복제
미션 중요	4	M1 - 아카이브를 통한 백업 및 이중 복제
	4	M2 - 백업, 복제 및 이중 아카이브
	5	M3 - 백업, 이중 복제 및 이중 아카이브

유형/토폴로지 조합은 **사본 수와 해당 사본의 특성으로 정의됩니다**. 예를 들어, 항상 3개의 복사본을 포함하는 향상된 유형은 두 개의 고유한 토폴로지를 가질 수 있습니다. 한 토폴로지는 백업, 복제 및 아카이브이고, 다른 토폴로지는 백업 및 이중 복제입니다. 데이터 복사본의 모든 순열이 위에 나열되지는 않습니다. 이 목록은 단순히 가장 일반적인 배포를 나타냅니다. 일부 조합은 사업적으로나 기술적으로도 의미가 없습니다.

일반적으로 사용되는 토폴로지와 사용되지 않는 토폴로지를 이해하는 것이 도움이 됩니다. 각 패턴의 상대적 인기는 IT 팀이 데이터 자산에 대한 추가 보호를 고려할 때 유용한 "업그레이드" 경로를 제공할 수 있습니다.

청사진: 토폴로지의 전체 목록

이제 유형, 토폴로지 및 고객 가용성 아키텍처에 대해 설명했으므로 업계 청사진의 전체 목록을 살펴보겠습니다.

이 차트는 앞서 논의한 모든 개념을 함께 연결합니다. 모든 구성은 현실 세계에서 인기 있는 선택이며, 실제 기업들이 Cohesity를 통해 규모에 맞게 운영하고 있습니다.

유형	토폴로지/사본 유형	고객 가용성 아키텍처		
		액티브-대기	액티브-액티브	허브 앤 스포크
베이직	B1 백업(1)	•	•	
	B2 백업 및 아카이브(2)	•	•	
	B3 백업 및 복제(2)	•	•	
향상된 기능	E1 백업, 복제 및 아카이브(3)	•	•	•
	E2 백업 및 이중 복제(3)	•	•	
미션 중요	아카이브를 통한 M1 백업 및 이중 복제(4)	•		
	M2 백업, 복제 및 이중 아카이브(4)	•	•	
	M3 백업, 이중 복제 및 이중 아카이브(5)		•	

미션 크리티컬 토폴로지에는 한 가지 주의 사항이 있습니다. 이러한 토폴로지는 배포, 시연, 시험이 진행되었거나 기업 또는 기타 대규모 고객과 함께 장기간 논의되었습니다. 앞서 많은 고객이 배포에 대해 더 큰 레질리언스를 추구한다고 언급했습니다. 논의에는 추가 데이터 사본을 보호하는 실질적인 방법이 포함됩니다. 일반적인 솔루션은 사이버 볼트를 사용하여 배포를 개선하는 것입니다. 이러한 이유로, 미션 크리티컬 토폴로지의 대부분은 사이버 볼트로 구성된 아카이브를 포함합니다. (이 시나리오에서는 Cohesity FortKnox를 제공합니다.) 사이버 볼트를 추가하면 많은 토폴로지가 사이버 레질리언스를 높일 수 있습니다.

이제 한 번에 한 그룹씩 유형과 토폴로지에 대해 자세히 살펴보겠습니다.

베이직

토폴로지	기본 데이터 센터	액티브-액티브
B1 - 백업	✓	✓
B2 - 백업 및 아카이브	✓	✓
B3 - 백업 및 복제	✓	✓

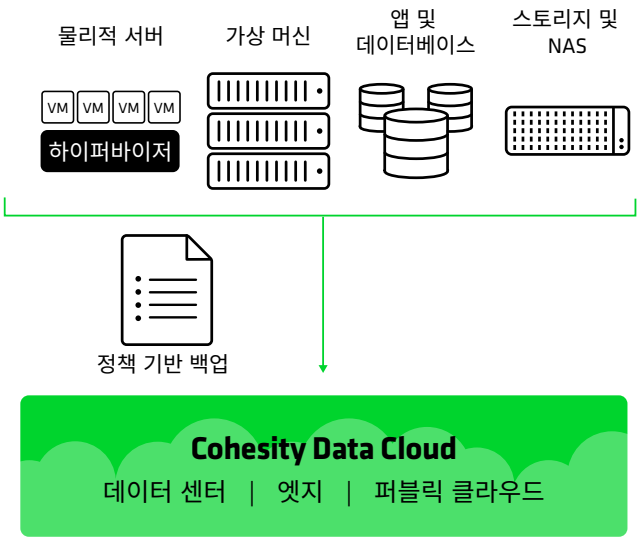
베이직은 가치가 낮거나 중간 수준인 데이터에 인기가 있거나, 고객이 이미 여러 데이터 복사본을 가지고 있는 경우 인기가 있습니다. 베이직 토폴로지는 단일 기본 데이터 센터가 있을 때와 액티브-액티브 접근 방식에도 사용됩니다.

사이버 볼트란?

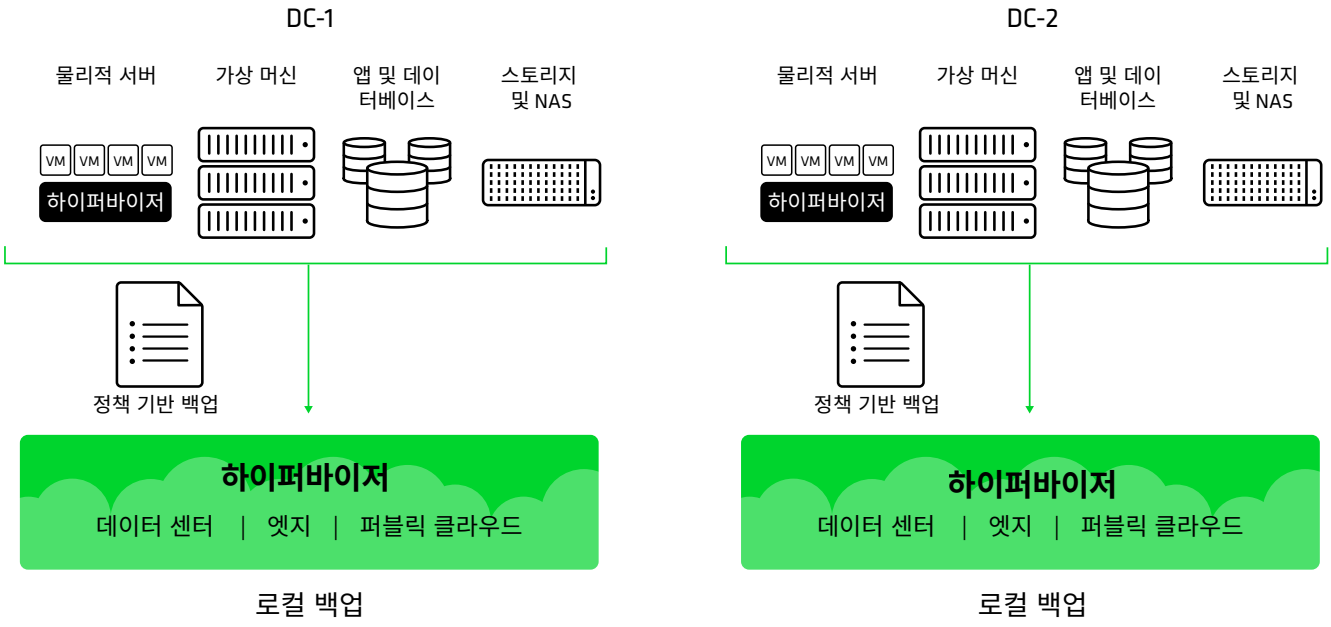
사이버 볼트는 종종 외부에 생산 데이터의 격리된 사본을 저장합니다. 항상 대기 상태로 유지되는 깔끔하고 분리되고 보호되는 데이터 복사본을 통해 랜섬웨어 공격이나 프로덕션 또는 기본 백업 시스템을 손상시키는 기타 사고가 발생할 경우, 조직에서 데이터를 원래 소스 또는 대체 백업 위치로 신속하게 복구할 수 있습니다. 최신 사이버 볼트 전략은 백업을 보호하지만, 매우 강력한 제어에도 불구하고 필요한 원격 액세스를 가능하게 하는 임시 네트워크 연결을 허용하는 "가상 에어갭" 기술을 사용하는 동시에 필요에 따라 클라우드에서 데이터를 추가로 격리합니다. 잘 설계된 사이버 볼트는 강력한 데이터 격리 및 사이버 레질리언스 전략의 효과적인 일부가 될 수 있습니다.

베이직: B1 - 로컬 백업

이것은 데이터의 단일 백업 복사본만 있는 기본적인 접근 방식입니다. 많은 IT 데이터 센터는 여전히 이 접근 방식을 사용하지만, 이 방법에는 재해 복구 또는 백업 데이터의 장기 보존을 위한 조항은 없습니다. 이 접근 방식은 일반적으로 가치가 낮은 데이터에 사용됩니다.



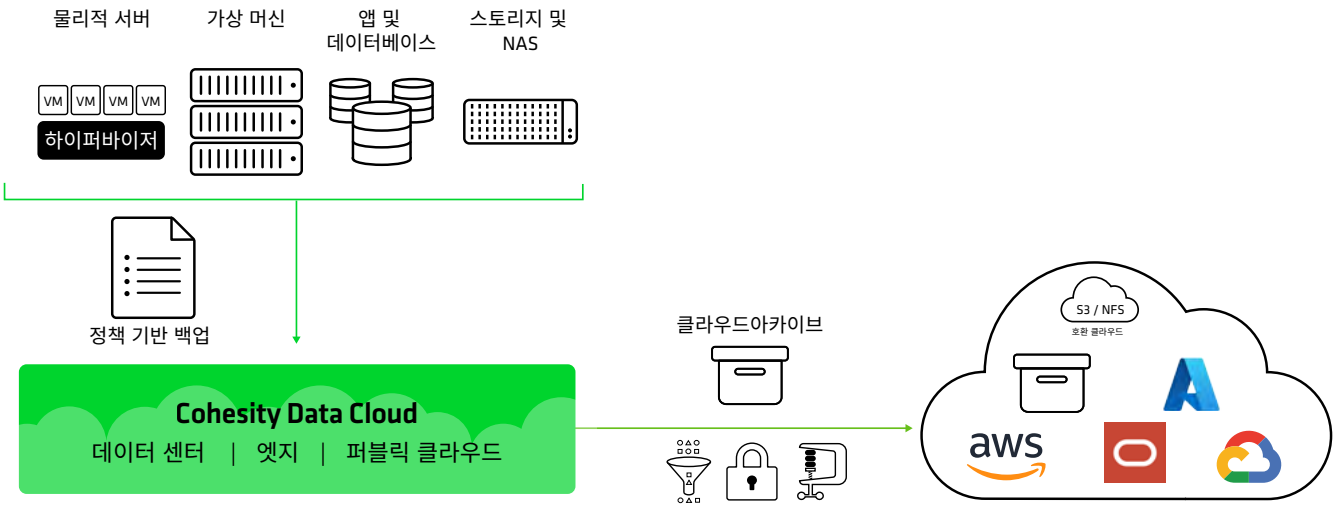
베이직: B1 - 백업(액티브-액티브)



로컬 백업 로컬 백업

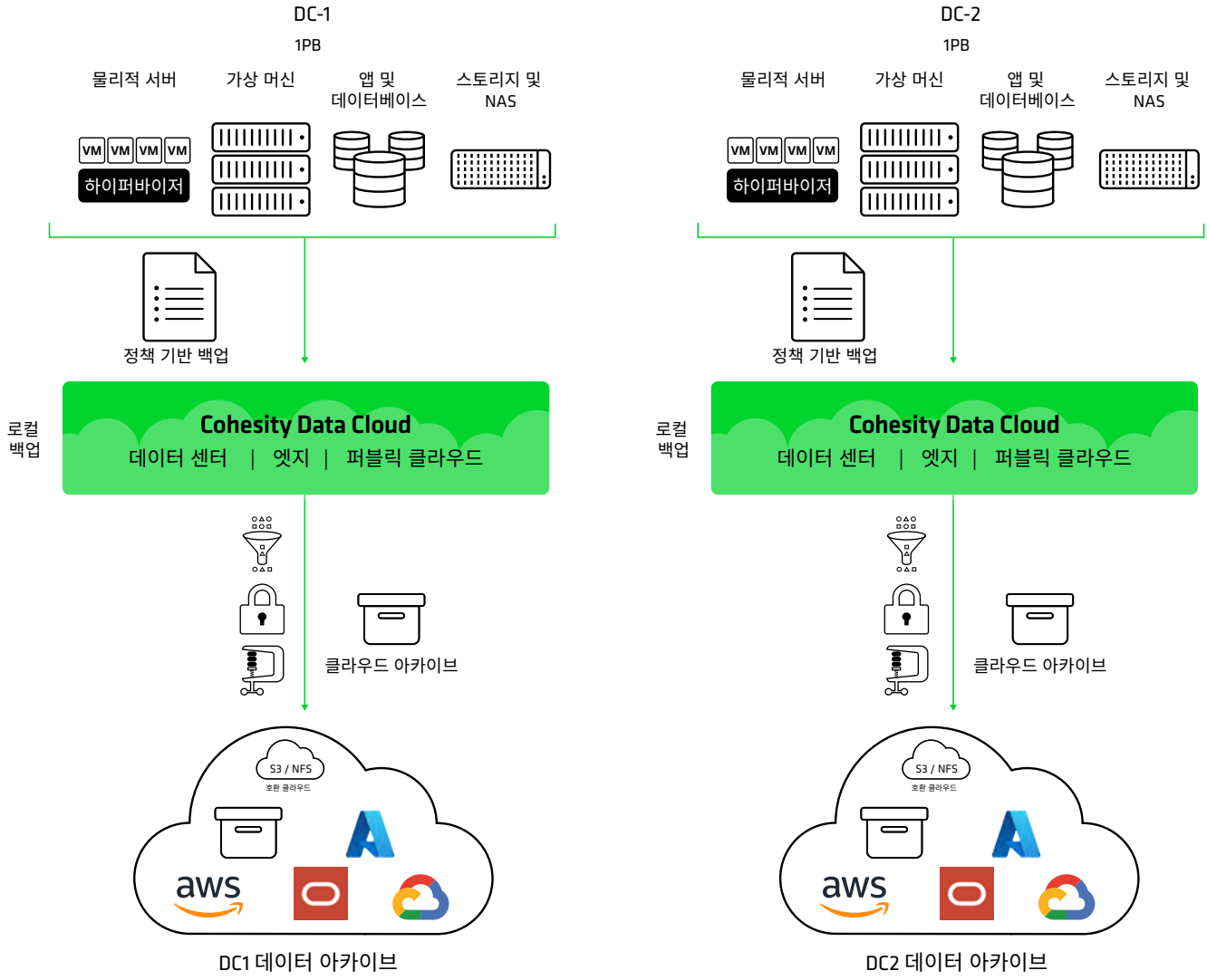
많은 유형과 토폴로지가 액티브-액티브 접근 방식에 적합합니다. 액티브-액티브 접근 방식은 사실상 두 가지의 단일 토폴로지 유형, 즉 미러링 및 백투백을 의미합니다. 이 토폴로지에는 각각 자체 백업이 있는 한 쌍의 액티브-액티브 데이터 센터가 있습니다. 어느 데이터 센터든 정전 시 다른 데이터 센터의 역할을 인수할 수 있습니다. 또한 각 데이터 센터에는 데이터와 워크로드에 대한 완전한 백업이 있습니다. 사용 가능한 WAN 대역폭이 많은 고객의 경우, 백업도 데이터 센터에서 지리적으로 분리하여 추가적인 재해 예방 기능을 제공할 수 있습니다. 워크로드 및 데이터의 모든 복제는 워크로드 계층에서 발생하므로 이 토폴로지는 복제가 필요하지 않습니다.

베이직: B2 - 백업 및 아카이브



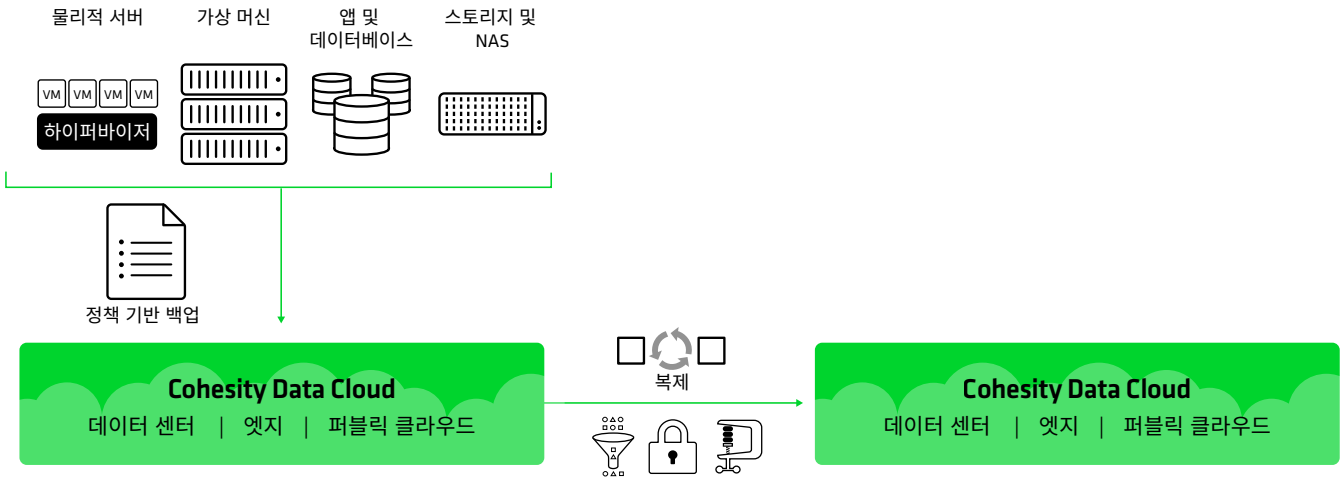
이 경우 백업은 백업보다 보존 기간이 훨씬 긴 아카이브와 결합됩니다. Cohesity FortKnox는 이 토폴로지에 대한 추가 보안을 제공하므로 여기에서 인기 있는 선택입니다. FortKnox는 격리된 아카이브이며 아카이브에 대한 쓰기 작업을 수행하거나 아카이브에서 복원이 수행되는 경우에만 연결됩니다. 아카이브는 온프레미스/오프프레미스 프라이빗 클라우드 또는 AWS, Google Cloud, Microsoft Azure, Oracle Cloud 또는 S3/NFS 호환 클라우드 서비스와 같은 퍼블릭 클라우드에도 있을 수 있습니다.

베이직: B2 - 백업 및 아카이브(액티브-액티브)



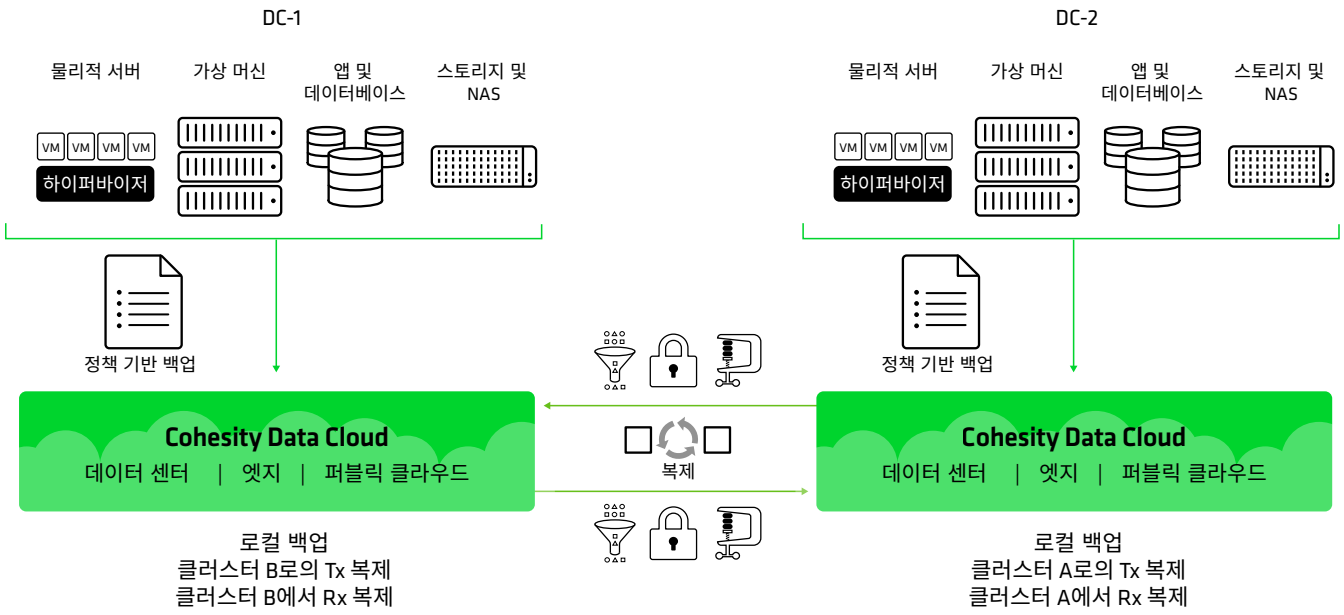
이 토폴로지에는 각각 자체 백업 및 아카이브가 있는 한 쌍의 액티브-액티브 데이터 센터가 있습니다. 어느 데이터 센터든 정전 시 다른 데이터 센터를 대신할 수 있으며, 각 데이터 센터는 아카이브를 통해 데이터와 워크로드를 완벽하게 백업합니다. 워크로드 및 데이터의 모든 복제는 워크로드 계층에서 이루어지므로 이 토폴로지는 복제가 필요하지 않습니다. FortKnox는 격리 및 추가 보안을 고려할 때 아카이브로 유용한 선택이 될 것입니다.

베이직: B3 - 백업 및 복제(재해 복구)



이 토폴로지에서 백업 및 복제본은 보존 기간에 따라 대략적으로 정렬됩니다. 복제본은 지리적으로 분산되어 재해 복구에 사용됩니다. 사용 가능한 WAN 대역폭이 많은 고객의 경우, 백업도 데이터 센터에서 지리적으로 분리하여 추가적인 재해 예방 기능을 제공할 수 있습니다. 이 토폴로지는 백업을 사용할 수 없는 경우 비즈니스 연속성에 중점을 둡니다. 복제본은 아카이브를 사용할 때 필요한 2단계 프로세스 없이 데이터를 직접 복원할 수 있습니다.

베이직: B3 - 백업 및 교차 복제(액티브-액티브)



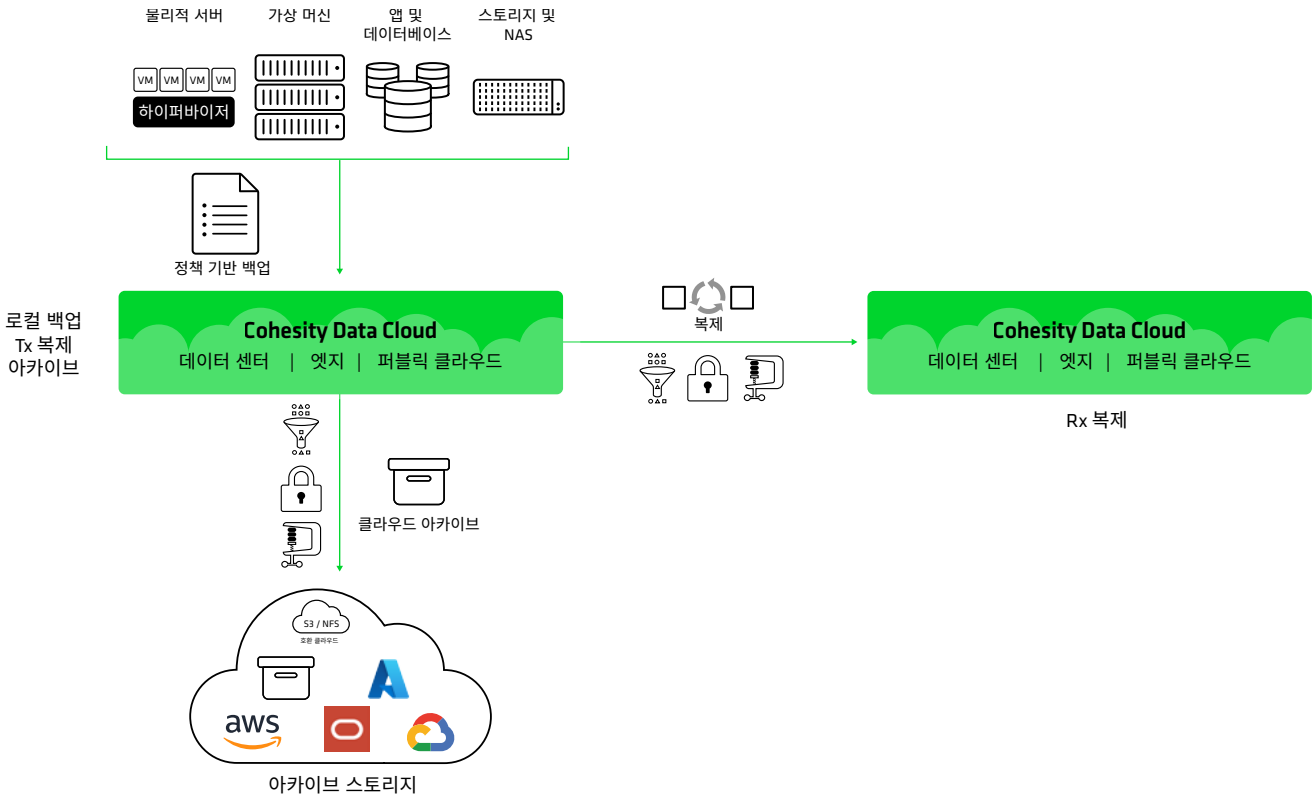
이 경우 백업 및 복제 클러스터가 교차 복제됩니다. 첫 번째 사이트의 백업은 두 번째 사이트의 복제본이며 그 반대의 경우도 마찬가지입니다.

향상된 토폴로지(산업별 채택 포함)

향상된 토폴로지는 가치가 높은 데이터에서 널리 사용됩니다. 백업, 복제 및 아카이브(E1)가 가장 인기 있는 반면, 백업 및 이중 복제(E2)는 그다지 인기가 없습니다. 일반적으로 사용되는 토폴로지와 업계별 주목할 만한 선호되는 토폴로지는 아래에 표시되어 있습니다.

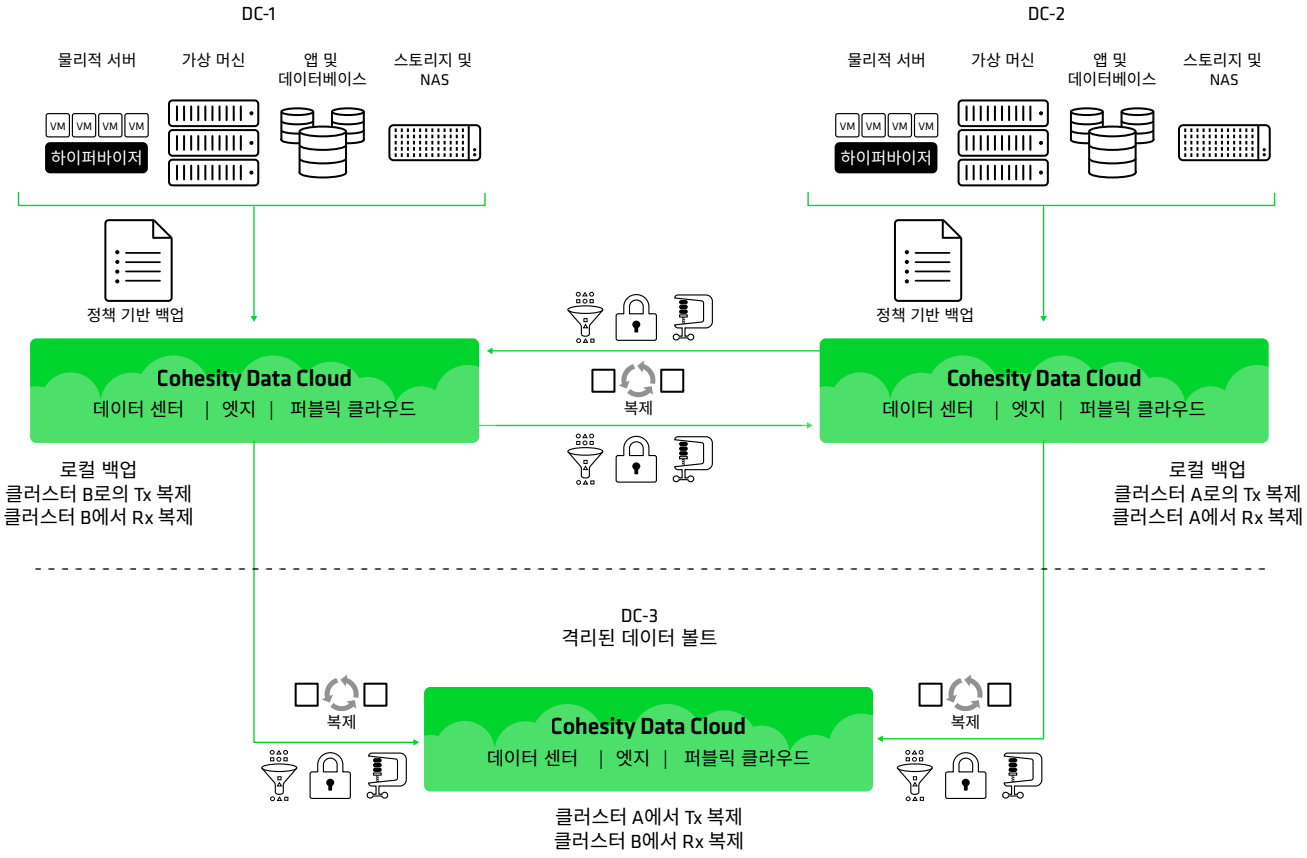
토폴로지	기본 데이터 센터	액티브-액티브	허브 앤 스포크
E1 - 백업, 복제, 및 아카이브	✓ 모든 유형	✓ 금융 기관	
E2 - 백업 및 이중 복제	✓ 정부 기관	✓ 소매 체인, 동서 모델을 사용하는 일부 정부 기관	

향상된 기능: E1 - 백업, 복제 및 아카이브



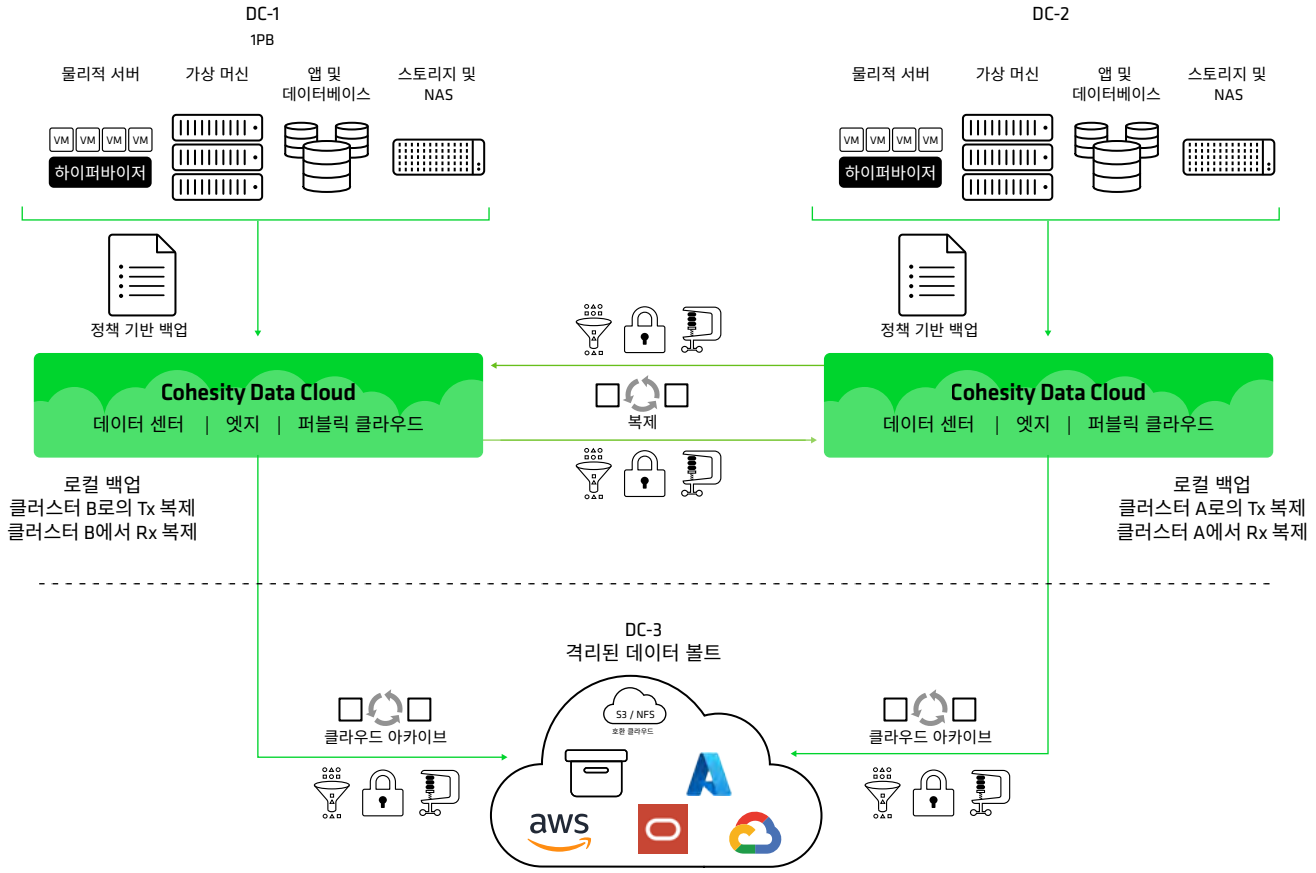
백업 및 복제본은 대략적으로 정렬되어 있지만(예: 90일 동안 1일 2회), 아카이브는 몇 달 또는 몇 년을 포함할 수 있습니다. 백업 또는 복제본에서 복구하는 것은 1단계 프로세스인 반면, 아카이브에서 복구하면 두 단계가 복구됩니다. 즉, 아카이브에서 읽은 다음 데이터를 복원하는 것입니다. 아카이브는 온프레미스/오프프레미스 프라이빗 클라우드 또는 AWS, Google Cloud, Microsoft Azure, Oracle Cloud 또는 S3/NFS 호환 클라우드 서비스와 같은 퍼블릭 클라우드에 있을 수 있습니다. FortKnox는 또한 격리 및 보안이 추가되었다는 점을 고려할 때 이 토폴로지에 탁월한 선택이 될 것입니다. Cohesity Data Cloud를 사용하면 기본 클러스터 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다.

향상된 기능: E1 - 데이터 볼트를 사용한 액티브-액티브



이 토폴로지는 또 다른 **액티브-액티브** 접근 방식입니다. 여기서 교차 복제된 데이터 센터는 격리된 단일 데이터 볼트를 공유합니다. 격리는 물리적으로 이루어지며, 사용하지 않을 때는 데이터 볼트가 네트워크에서 분리됩니다. 볼트는 복제본이므로 복제본에서 두 데이터 센터 중 하나를 한 번에 복구할 수 있습니다. 이 아키텍처는 여러 개의 액티브-액티브 쌍이 모두 동일한 데이터 볼트를 사용하여 확장될 수도 있습니다.

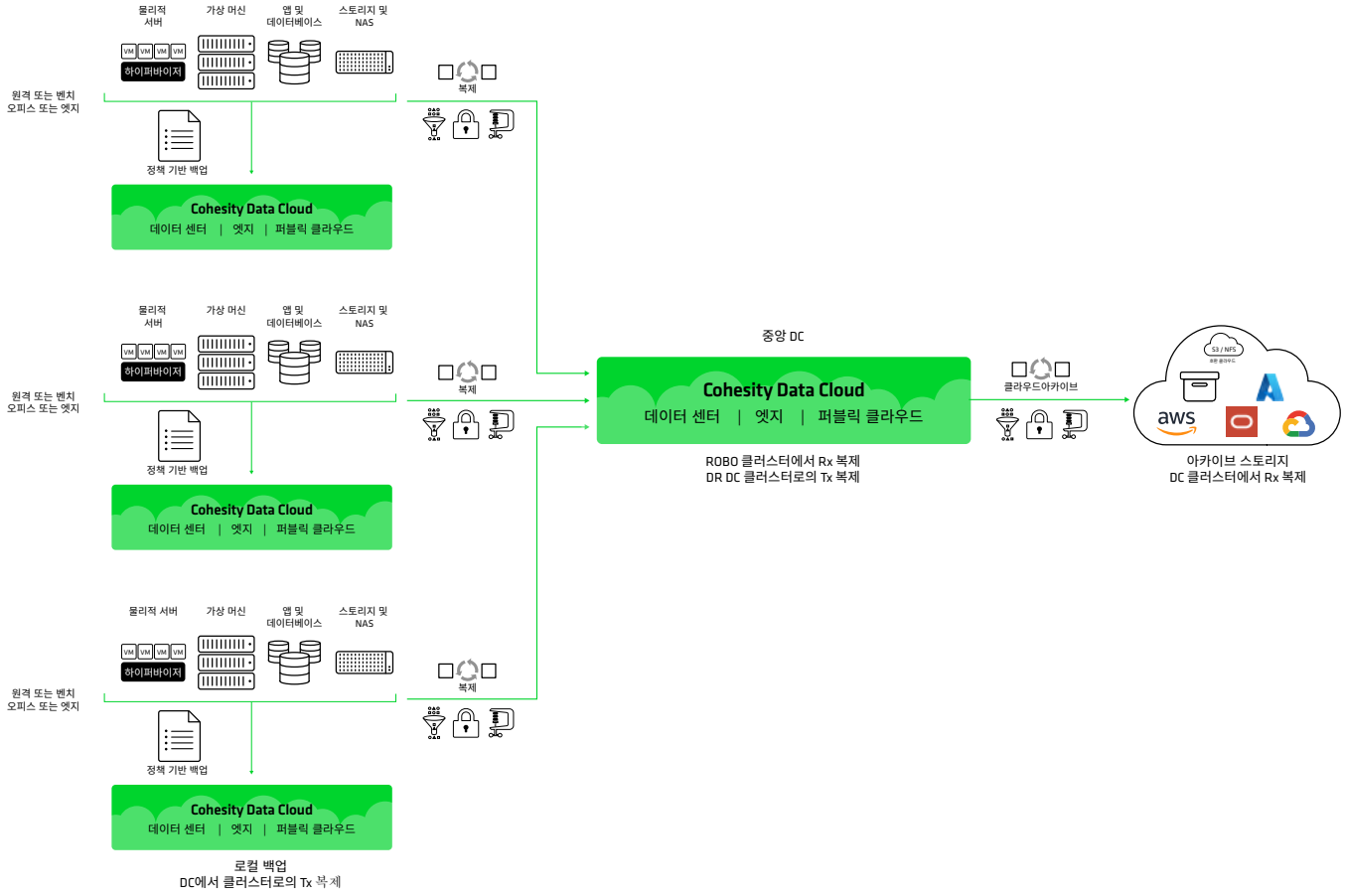
향상된 기능: E1 - 격리된 아카이브가 있는 액티브-액티브



위의 그래픽은 또 다른 **액티브-액티브** 접근 방식입니다. 이 경우 교차 복제된 데이터 센터는 단일 격리된 아카이브를 공유했습니다. 이 사용 사례는 격리 및 추가 보안을 고려할 때 FortKnox 아카이브 접근 방식과 잘 작동합니다.

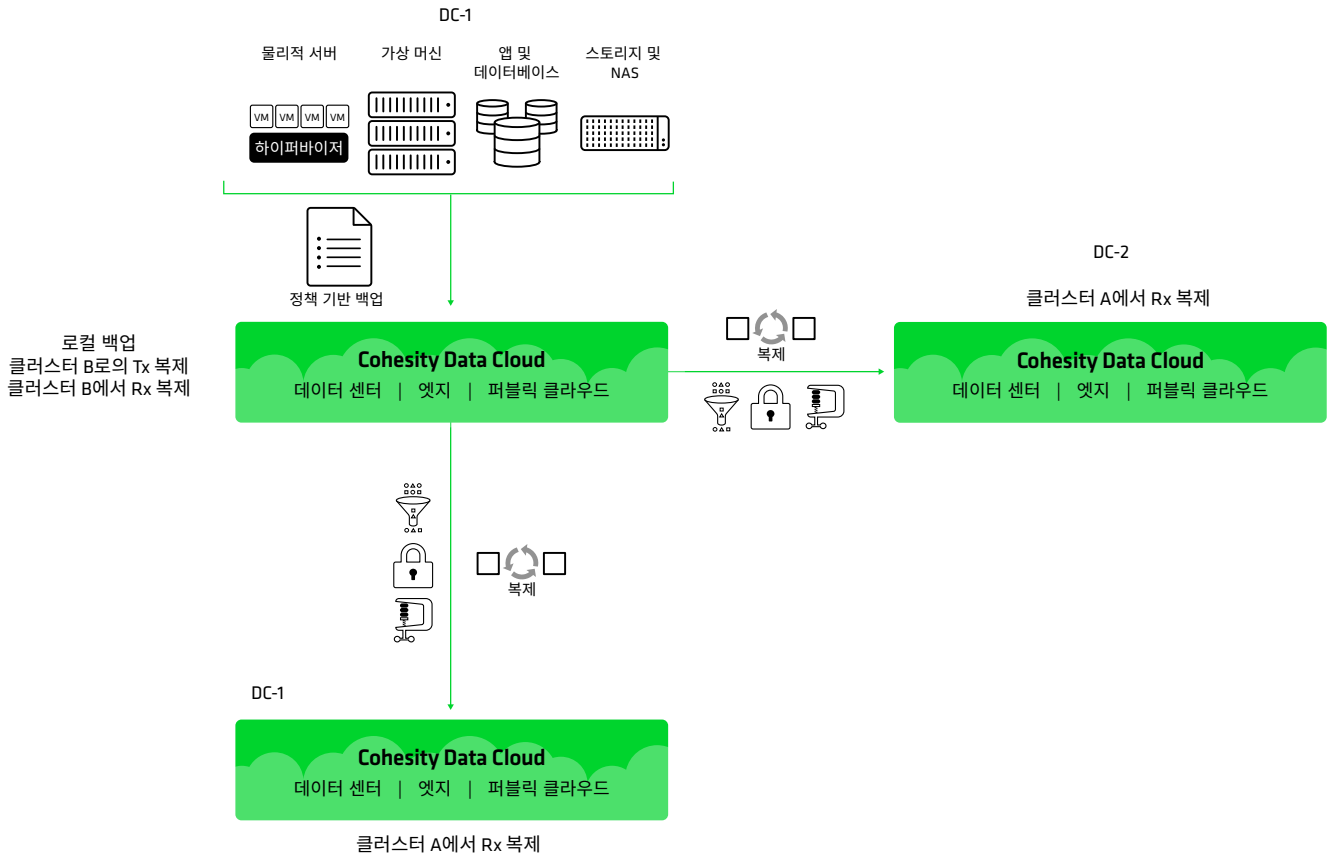
이 아키텍처는 동일한 격리된 아카이브를 사용하는 여러 개의 액티브 액티브 쌍으로 확장할 수도 있습니다. Cohesity Data Cloud를 사용하면 아카이브를 백업 또는 복제본으로 복원할 수 있습니다.

향상된 기능: E1 - 백업, 복제 및 아카이브(허브 앤 스포크)



또한 많은 토폴로지를 **허브 앤 스포크**로 확장할 수 있으며, 이를 팬-인 토폴로지라고도 합니다. 허브 앤 스포크 모델에서는 각 지점에 자체 백업이 있으며, 이러한 백업은 중앙 데이터 센터의 단일 통합 Cohesity Data Cloud로 복제됩니다. 중앙 데이터 센터에서 복제본은 FortKnox를 통해 보관되거나 다른 개인 또는 공용 아카이브로 보관됩니다. FortKnox는 백업과 복제본이 모두 손상된 경우 완전한 격리를 제공하므로 여기에서 훌륭한 선택이 될 것입니다. Cohesity Data Cloud를 사용하면 기본 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다.

향상된 기능: E2 - 백업 및 이중 복제



이 토폴로지는 아카이브의 2단계 복원 프로세스를 수행해도 충분히 낮은 RTO를 제공하지 않는 경우에 사용됩니다.

이 구성에서 3개의 복사본(백업 및 두 복제본 모두)을 모두 사용하여 1단계 프로세스로 데이터를 복원할 수 있습니다.

향상된 기능: E2 - 액티브-액티브 허브를 갖춘 허브 앤 스포크

이 토폴로지는 여러 가지 모델을 결합합니다. 원격 지점은 각각 자체 백업을 수행하며 이러한 백업은 중앙 데이터 센터에 복제됩니다. 이 중앙 데이터 센터에는 백업으로 재해 복구 데이터 센터도 있습니다. 이 모든 것이 미러링되어 왼쪽의 기본 데이터 센터가 오른쪽의 데이터 센터의 재해 복구 사이트 역할을 하며, 그 반대의 경우도 마찬가지입니다.

미션 크리티컬

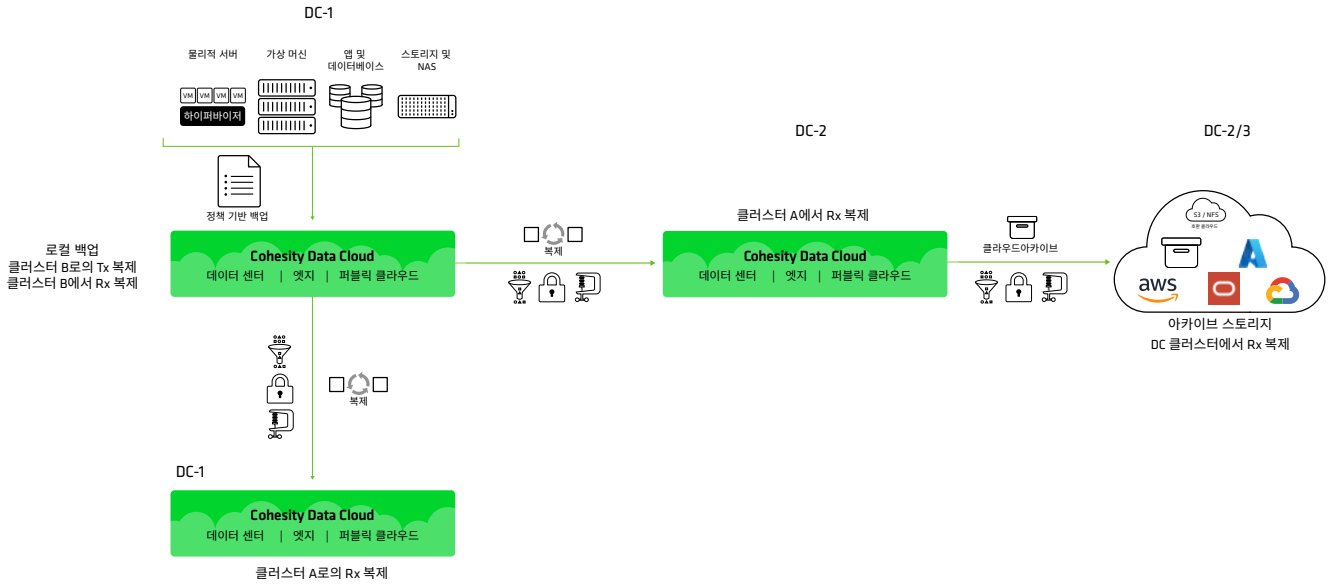
토폴로지	단일 데이터 센터	액티브-액티브	허브 앤 스포크
아카이브를 통한 백업 및 이중 복제본	✓		✓
백업, 복제 및 이중 아카이브	✓	✓	
백업, 이중 복제본 및 이중 아카이브		✓	

미션 크리티컬은 특정 회사에서 가장 가치 있는 데이터의 토폴로지로 부상하고 있습니다. 이는 최소 기능 기업(MVC)을 운영하는 데 필요한 데이터입니다.

귀하의 최소 기능 기업은 무엇입니까?

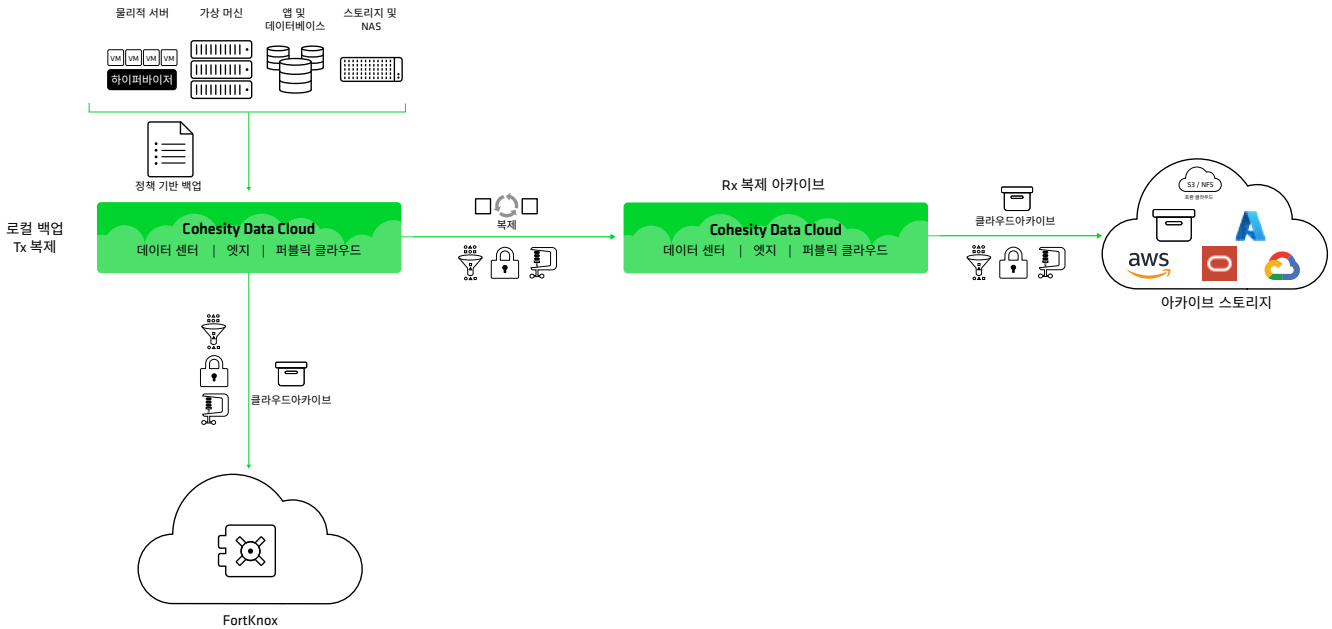
MVC는 기업이 최소한의 실행 가능한 수준에서 작동하도록 복원해야 하는 애플리케이션, 인프라 및 프로세스의 모음입니다. 이러한 시스템은 먼저 온라인 상태로 전환해야 하며, 다른 모든 시스템은 그 다음으로 우선 순위가 높습니다. IT 리더는 사고 대응 및 복구 전략과 데이터 토폴로지를 계획할 때 MVC를 사용해야 합니다.

미션 크리티컬: M1 - 아카이브를 통한 백업 및 이중 복제



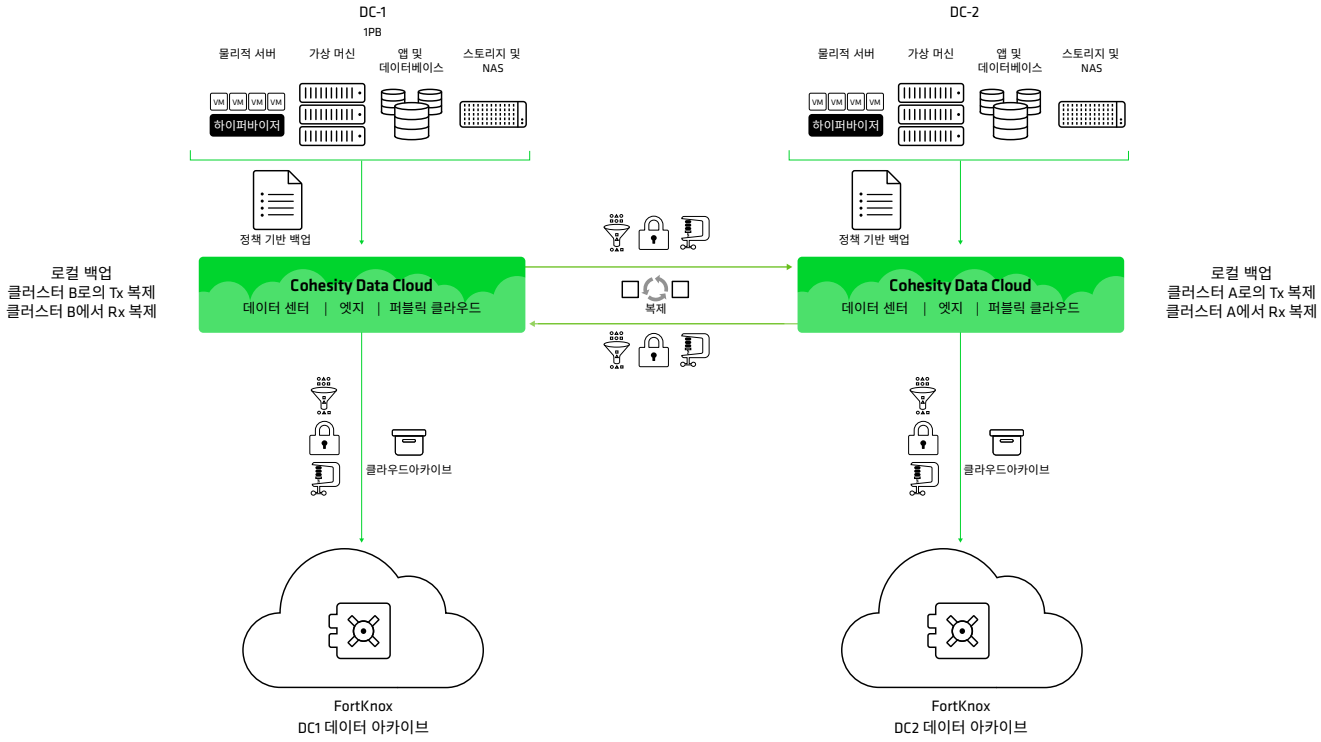
이러한 내결함성 아키텍처는 엄격한 RTO 및 RPO 요구 사항을 충족하며 장기 보존 요구 사항과 결합됩니다. 두 번째 복제본은 추가적인 재해 복구 및 랜섬웨어 보호 기능을 제공합니다. Cohesity Data Cloud를 사용하면 기본 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다. 두 번째 복제본에 에어갭을 추가하면 레질리언스가 향상됩니다.

미션 크리티컬: M2 - FortKnox를 사용한 이중 아카이브 백업, 이중 복제본(로컬 백업에서)



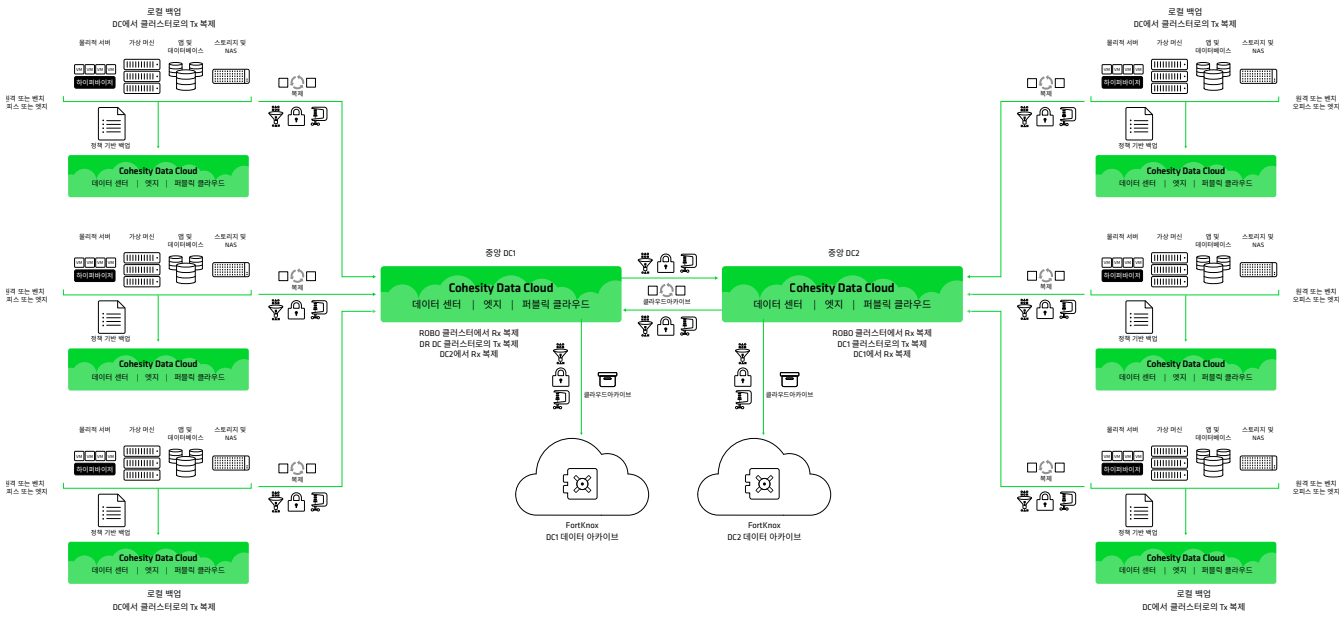
이러한 내결함성 아키텍처는 두 번째 복제본 대신 FortKnox를 사용하는데, 이는 FortKnox가 추가 보안 및 격리를 제공하기 때문입니다. 첫 번째 아카이브는 규정 준수 활동에 사용할 수 있으며, FortKnox 아카이브는 추가적인 랜섬웨어 방지 레질리언스를 제공합니다. Cohesity Data Cloud를 사용하면 기본 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다.

미션 크리티컬: M2 - FortKnox와 로컬에서 교차 복제 및 아카이브



이는 **베이직** 토폴로지에서 본 **액티브-액티브** 모델에 이중 FortKnox 아카이브를 추가한 것입니다. 각 클러스터에는 DC1 및 DC2 복사본이 모두 포함되어 있으므로 각 FortKnox 인스턴스에는 DC1 및 DC2 복사본도 포함되어 있습니다. Cohesity Data Cloud를 사용하면 기본 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다.

미션 크리티컬: M3 - 액티브-액티브 허브 및 FortKnox 아카이브를 사용한 허브 앤 스포크



이는 **향상된 기능** 유형에서 본 것과 유사하지만, 이 경우 각 복제본은 장기 아카이브로 FortKnox에 연결됩니다. 복제본에는 왼쪽 및 오른쪽 스포크의 복사본이 모두 있으므로 각 FortKnox 아카이브에는 두 복사본의 세트가 모두 보관되어 있습니다. Cohesity Data Cloud를 사용하면 기본 또는 보조 클러스터를 통해 아카이브를 복원할 수 있습니다.

결론 및 다음 단계

많은 기업 리더들은 중요한 데이터의 보호를 강화하려고 합니다. 이러한 의사 결정권자들과 새로운 접근 방식에 대해 논의할 때 청사진은 중요합니다. 이 백서에서 논의된 설계는 경영진이 유사한 데이터 보호 요구 사항이 있는 유사한 상황에서 동료가 수행한 작업을 이해하는 데 도움이 될 것입니다.

데이터의 복사본과 관련하여 "더 많은" 것이 항상 좋은 것은 아닙니다. Cohesity와 고객 모두 더 많은 데이터 사본을 추가하면 운영, 라이선스 및 종종 하드웨어 비용이 추가된다는 것을 알고 있습니다. 경우에 따라 다른 사본을 추가하는 것을 권장하지 않고 다른 유형의 사본을 사용하도록 권장합니다.

회사 규정 준수 활동을 위해 아카이브를 사용하고 사이버 레질리언스를 촉진하는 것이 좋습니다. 따라서 고객은 종종 동일한 수의 데이터 사본을 보관하지만 사용한 사본의 유형을 변경합니다. 예를 들어, 보안이 취약한 현장의 아카이브를 FortKnox와 같은 격리된 아카이브로 교체하여 규정 준수 및 랜섬웨어 레질리언스 목적으로 모두 사용할 수 있는 사본을 제공할 수 있습니다.

청사진은 관련된 모든 입증된 옵션을 검토하고 배포에서 사용할 옵션에 대해 정보에 입각한 결정을 내릴 수 있기 때문에 강력합니다.

아래 차트는 장애 도메인, 천재지변 및 사이버 보호와 관련된 각 토폴로지의 이점에 대해 간단하고 종합적으로 보여줍니다.

유형	베이직		향상된 기능	미션 크리티컬	
사본	1	2	3	4	5
토폴로지	**백업 전용**	**백업 및 저장소** (복제본 또는 아카이브)	**백업 및 이중 저장소** (복제본 및 아카이브 또는 이중 복제본)	**백업 및 이중 복제본 및 아카이브**	**백업, 이중 복제본 및 이중 아카이브**
HW 및 SW 장애 도메인으로부터의 보호	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
"천재지변"으로부터의 보호		★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
사이버 보호	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

현대적인 데이터 보안 및 관리로의 전환은 어려워 보일 수 있습니다. 당사는 이 청사진 정보를 취합하여 위험과 비용을 줄이면서도 더 나은 비즈니스 성과를 얼마나 빨리 달성할 수 있는지 더 쉽게 만들고 가속화하는 데 도움을 드립니다.

여기에서 다음 단계를 수행하는 것이 좋습니다.

1. 귀하의 상황과 가장 관련이 있는 청사진을 결정합니다.
2. 기존 솔루션과 관련하여 최신 데이터 플랫폼의 ROI 및 TCO를 평가합니다. 비교의 핵심 사항은 다음과 같아야 합니다.
    a. 데이터 보호 효율성
    b. 운영의 효율성
    c. 위험 및 규정 준수
3. 제품 데모, 입증된 ROI 및 TCO 계산, 로드맵 우선 순위 지원을 기반으로 솔루션을 선택하십시오.
4. 가장 관련성이 높은 청사진에 따라 선택한 솔루션을 배포하고, 이전 단계에서의 로드맵을 실행합니다.

최신 플랫폼이 구축되면 사이버 레질리언스와 관련된 초기 KPI 세트를 생성하고 이 기준과 비교하여 진행 상황을 정기적으로 측정합니다. 거기에서 여정의 다음 단계로 넘어가야 할 시기를 알 수 있습니다.

Cohesity 소개

Cohesity는 AI 기반 데이터 보안의 리더입니다. Fortune 100대 기업 중 85개 이상과 글로벌 500대 기업 중 약 70%를 포함한 13,600개 이상의 기업 고객은 Cohesity를 통해 레질리언스를 강화하는 동시에 방대한 양의 데이터에 대한 Gen AI 인사이트를 제공합니다. Cohesity와 Veritas의 엔터프라이즈 데이터 보호 부문의 결합으로 구축된 이 회사의 솔루션은 온프레미스, 클라우드 및 엣지에서 데이터를 안전하게 보호합니다. NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud 등의 지원을 받고 있는 Cohesity는 캘리포니아주 산타클라라에 본사를 두고 있으며 전 세계에 지사를 두고 있습니다. 자세한 내용을 알아보려면 LinkedIn, X, Facebook에서 Cohesity를 팔로우하세요.

Cohesity에서 자세히 알아보기

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000050-002 KO 4-2025