aws re/start

대응

Security Fundamentals

보안 수명 주기 - 대응을 시작하겠습니다.

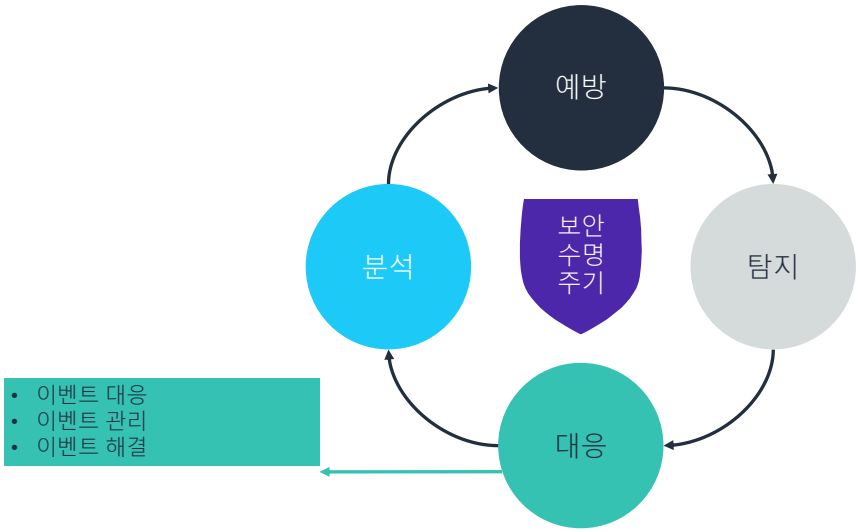
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 인시던트 조사 프로세스의 일반적인 단계를 나열합니다.
- 비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP)의 목적을 설명합니다.
- 백업 옵션을 파악합니다.
- 백업 모범 실무를 적용합니다.

보안 수명 주기: 대응



aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 위협을 탐지했을 때 취해야 할 조치를 설명합니다.
- **분석** - 향후에 인시던트가 다시 발생하지 않도록 예방하는 새로운 조치를 구현하면서 주기가 완료됩니다.

이 강의에서는 보안 수명 주기의 **대응** 단계를 배웁니다. 특히 보안 이벤트 관리, 대응, 해결과 관련한 방법과 기법을 배우게 됩니다.

이벤트 대응의 프로세스 및 계획

이벤트 조사 프로세스

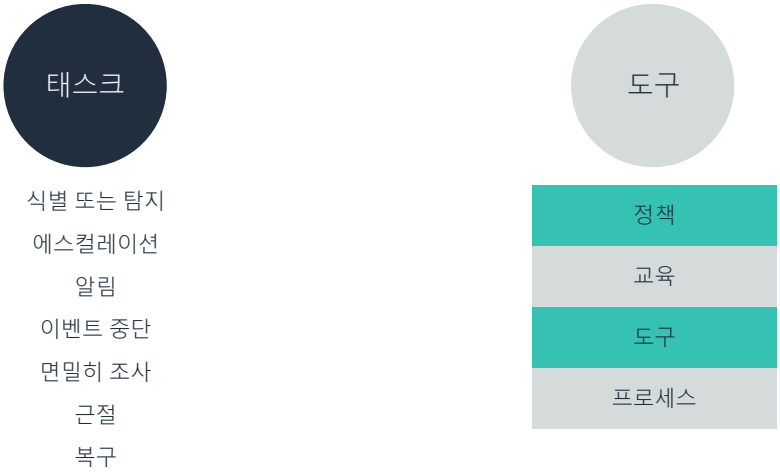
- 악성 **이벤트**에 대한 일반적인 대응 단계

aws re/start

그림에 보안 이벤트에 대응하고 보안 이벤트를 조사하는 데 사용되는 일반적인 단계가 나와 있습니다.

이벤트 조사: 준비 단계

준비는 이벤트를 해결하는 데 가장 중요한 단계입니다.



aws re/start

발생할 수 있는 모든 재해에 대비할 수는 없습니다. 그러나 비즈니스에 실질적인 위협이 될 수 있는 재해의 유형을 식별하고 문서화함으로써 상당한 주의를 기울일 수는 있습니다. 예기치 않은 이벤트는 사소한 불편함도 될 수 있고 조직이 최후를 맞이하게 되는 결과를 낳을 수도 있습니다. 이런 잠재적인 이벤트에 대비하지 못하면 실패를 겪게 될 것입니다.

비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP) 이해

앞으로 다룰 슬라이드에서는 비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP)에 관해 이야기합니다.

비즈니스 연속성 계획 및 재해 복구 계획

비즈니스 연속성 계획(BCP)

축소된 형태로
비즈니스 운영

재해 복구 계획(DRP)

중단 및 손실로부터
복구

aws re/start

이 두 계획의 목적은 다음을 하기 위한 것입니다.

- 중단이 있을 때 비즈니스가 계속해서 핵심적인 서비스를 지원하고 제공하도록 함
- 심각한 활동 중단을 이겨냄

비즈니스 연속성 계획

비즈니스 연속성 계획

축소된 형태로 비즈니스 운영

- 예방적 및 선제적 관리 도구
  - 다양한 재해 시나리오를 나열함
  - 중단 시 활성화되지 않음

비즈니스 연속성 계획(BCP)에서는 다양한 재해 시나리오를 나열합니다. 서비스 중단이나 하드웨어 파괴 등의 재해 또는 중단이 발생했을 때 핵심적인 서비스와 기능을 계속해서 운영할 수 있도록 비즈니스가 해야 할 일을 설명합니다.

BCP는 다음 행동을 하도록 합니다.

- 계속해서 평소처럼 비즈니스를 수행하기 위해 취할 다양한 재해 시나리오 및 작업 나열
  시나리오 예: 디스크 장애, 서버 장애, 데이터베이스 장애, 통신선 불안
- 일정 기간 동안 축소된 형태로 비즈니스 운영 유지
  예: 계속해서 실행해야 할 최소한의 온라인 시스템, 전화, 서버, 네트워크 연결, 네트워크 드라이브, 기타 리소스가 무엇인가?

BCP는 중단 시 활성화되지 않습니다.

재해 복구(DR) 계획

- 비즈니스가 재해 및 예기치 않은 인시던트로부터 복구하는 데 도움이 되는 전략
  - 복구 시간 목표(RTO): 얼마나 빨리 복구해야 하는가?
  - 복구 시점 목표(RPO): 잃어도 되는 시간과 데이터의 여유는 어느 정도인가?

재해 복구 계획

중단 및 손실로부터 복구

aws re/start

재해 복구 계획(DRP)은 비즈니스가 재해와 사이버 인시던트를 비롯한 예기치 않은 인시던트로부터 복구하는 데 도움이 되는 전략을 정의합니다. DRP에서는 두 가지 주요 파라미터를 사용합니다.

- **복구 시간 목표(RTO)**: 얼마나 빨리 복구해야 하는가?
- **복구 시점 목표(RPO)**: 잃어도 되는 시간과 데이터의 여유는 어느 정도인가?

이 파라미터의 값이 짧아질수록 백업 전략과 기타 복구 메커니즘은 비용이 더 커지고 더 복잡해집니다. 그러나 기술이 진화하면서 RTO와 RPO의 시간이 점점 더 짧아지고 있습니다.

DRP 목표

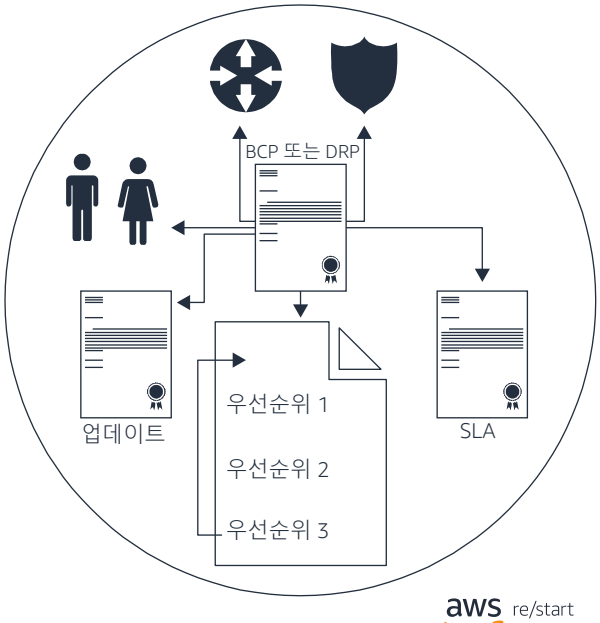
- 기본적인 목표:
  - 최소한의 영향으로 비즈니스 기능을 빠르게 복구함
- 보안 목표:
  - 적용된 제어 또는 안전 조치의 수준을 낮추지 않음
- 후속 작업 목표:
  - 이 위협, 불법 이용 또는 재해가 다시 일어나지 않도록 예방함

보안 목표:

- 비즈니스에서는 재해 또는 중단의 영향을 바탕으로 다양한 액세스 제어 해결 조치를 구현할 수 있습니다. 그러나 중단 이전과 같은 수준의 제한을 두고 보안 액세스 제어를 구현해야 합니다.
- 액세스 제어가 같은 수준으로 구현되지 않은 경우 비즈니스는 액세스를 허용하거나 리소스를 사용해서는 안 됩니다.

DRP 테스트

- 이 계획을 테스트해야 하는 이유:
  - 계획이 업데이트되었을 경우, 여전히 정확한지 확인
  - 환경, 하드웨어, 우선순위 변경
  - 인력 변경 시 현재 조직에서 일하는 사람이 계획을 구현할 수 있는지 판단
  - 규정 또는 계약에 테스트가 필요함



aws re/start

환경과 인력, 규정이 계속해서 변화하기 때문에 DRP를 주기적으로 테스트하고 필요에 따라 조정하는 것이 중요합니다.

RTO(복구 시간 목표) 및 RPO(복구 시점 목표) 이해

앞으로 다룰 슬라이드에서는 비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP)에 관해 이야기합니다.

RPO와 RTO 비교

RPO(데이터)

- 비즈니스에 어려움이 있기 전까지 얼마나 많은 데이터를 잃어도 괜찮은가?
- 재해가 발생했을 경우 심각한 해를 입히지 않는 선에서 데이터 백업까지 얼마나 시간이 흘러도 괜찮은가?
  - 데이터 백업의 고정된 간격 기반
  - 시간이 더 많이 흐를수록 비즈니스의 재정적 손실이 더 커짐

RTO(시간)

- 비즈니스 연속성을 유지하기 위해 IT 인프라를 얼마나 빨리 복구해야 하는가?
  - 온라인 상태로 더 빨리 되돌려야 할수록 비용이 더 커짐
  - 비즈니스 인프라 전체를 복구해야 함

RPO

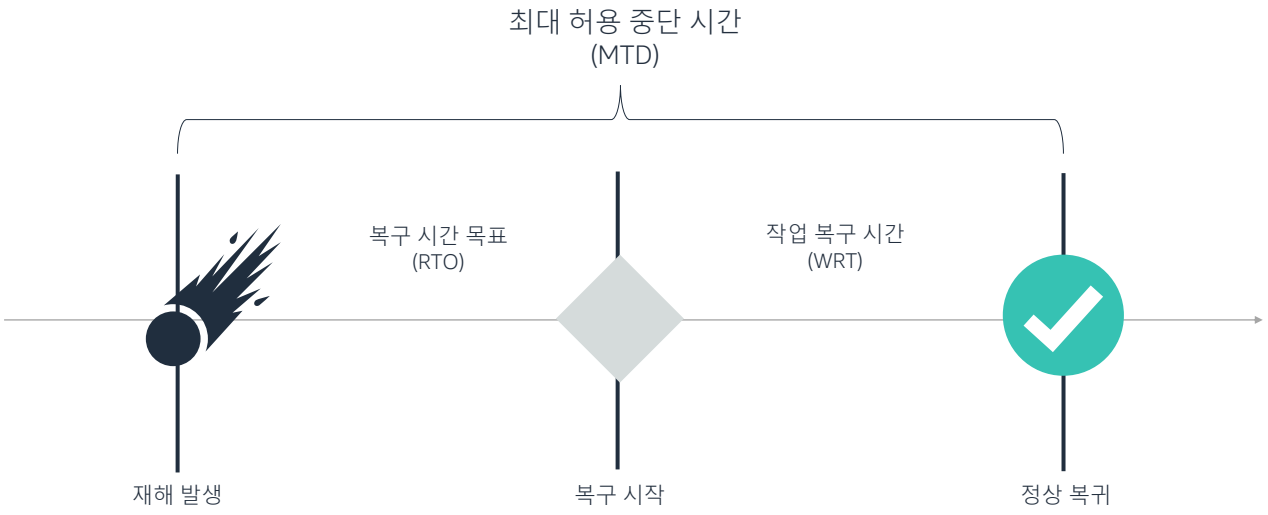
RPO는 데이터에 중점을 둡니다. RPO는 중단 이전의 시점으로, 중단 이후에 데이터가 복구될 수 있는 시점(데이터의 가장 최근 백업 사본)을 나타냅니다. RPO는 복구 프로세스 중에 비즈니스에서 용인할 수 있는 데이터 손실의 양을 나타내는 요소입니다.

RPO는 인프라의 데이터 계층에만 영향을 미치므로 RTO보다 구현이 쉽습니다.

RTO

RTO를 위해서는 데이터뿐만 아니라 비즈니스 인프라 전체를 복구해야 합니다. RTO는 다른 시스템 리소스, 지원되는 비즈니스 프로세스, 최대 허용 중단 시간(MTD)에 수용할 수 없는 영향이 있기 전까지 시스템 또는 리소스가 사용할 수 없는 상태로 유지되어도 괜찮은 최대 시간을 설정합니다.

중단으로부터 복구



aws re/start

작업 복구 시간(WRT)은 데이터를 복구 또는 복원하고, 프로세스를 테스트한 후, 시스템을 프로덕션용으로 작동시키는 것과 관련이 있습니다. 시스템 및 리소스 복구와 정상 프로세싱 시작 사이에 걸린 시간이 WRT에 해당합니다.

최대 허용 중단 시간(MTD)은 복구 시간 목표(RTO)와 WRT의 합입니다. 즉, MTD = RTO + WRT입니다.

MTD는 재해가 발생한 후 비즈니스 연속성을 중단시키는 수용할 수 없는 결과가 발생하지 않는 선에서 비즈니스가 중단되어도 되는 총 시간을 나타냅니다. MTD 값을 BCP와 DRP의 일부로 포함하십시오.

중단 복구 옵션

aws re/start

중단으로부터 복구하는 일은 일반적으로 이전에 구현한 백업 또는 복제 솔루션을 사용할 수 있는지에 따라 달려 있습니다.

복구 옵션의 유형

전통적인 테이프 스토리지

스냅샷 기반 복제

연속 복제

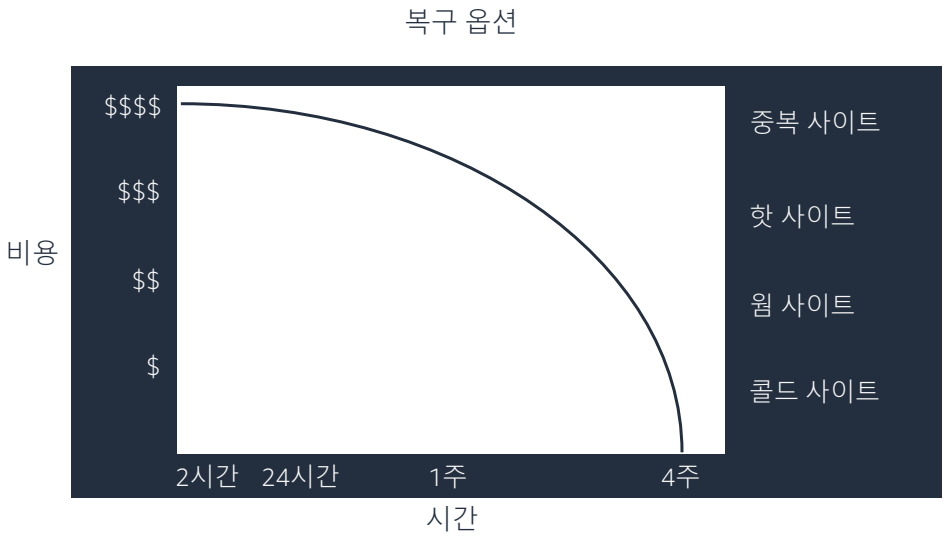
파일럿 라이트

백업과 복구 옵션의 유형:

- **전통적인 테이프 스토리지**
  - 대량의 데이터를 저장함
  - 신뢰성이 있으며 비용 효율적
  - 시간 효율적이지 않음. 가용성을 몇 시간 또는 며칠 동안 잃을 수 있음
- **스냅샷 기반 복제**
  - 특정 시점에 애플리케이션의 현 상태를 캡처함
  - 마지막 스냅샷 이후 변경된 데이터만 씀
  - 스냅샷이 얼마나 자주 생성되었는지에 따라 데이터를 보호함
- **연속 복제**
  - 디스크 또는 애플리케이션의 최신 사본이 지속적으로 클라우드 또는 다른 위치에 복제됨
  - 가중 중단 시간을 줄여줌
  - 더 세분화된 복구 지점을 제공함

- 파일럿 라이트
    - 환경의 최소화된 버전이 항상 클라우드에서 실행됨
    - 시스템에서 가장 핵심적인 요소를 구성하여 실행함
    - 복구가 필요할 때 핵심 코어를 중심으로 빠르게 완전한 프로덕션 환경을 프로비저닝함
    - 인프라 요소에 데이터베이스 서버와 기타 중요한 데이터가 포함됨

비용의 균형



허용되는 중단 시간이 길수록 비즈니스와 그 운영에 드는 비용이 더 커집니다.

핫, 웜, 콜드 사이트가 있는 비즈니스 시스템에 백업 솔루션을 결정해야 할 때는 시스템이 이 곡선의 어디에 있어야 하는지 자문하시기 바랍니다. 복구 속도와 비용 사이에 반대급부가 있습니다.

시스템마다 적절한 균형이 다릅니다. 예를 들어, 직원 데이터베이스는 며칠간 중단되어도 괜찮을 수 있지만 전자 상거래 사이트는 몇 분 만에 복구해야 합니다.

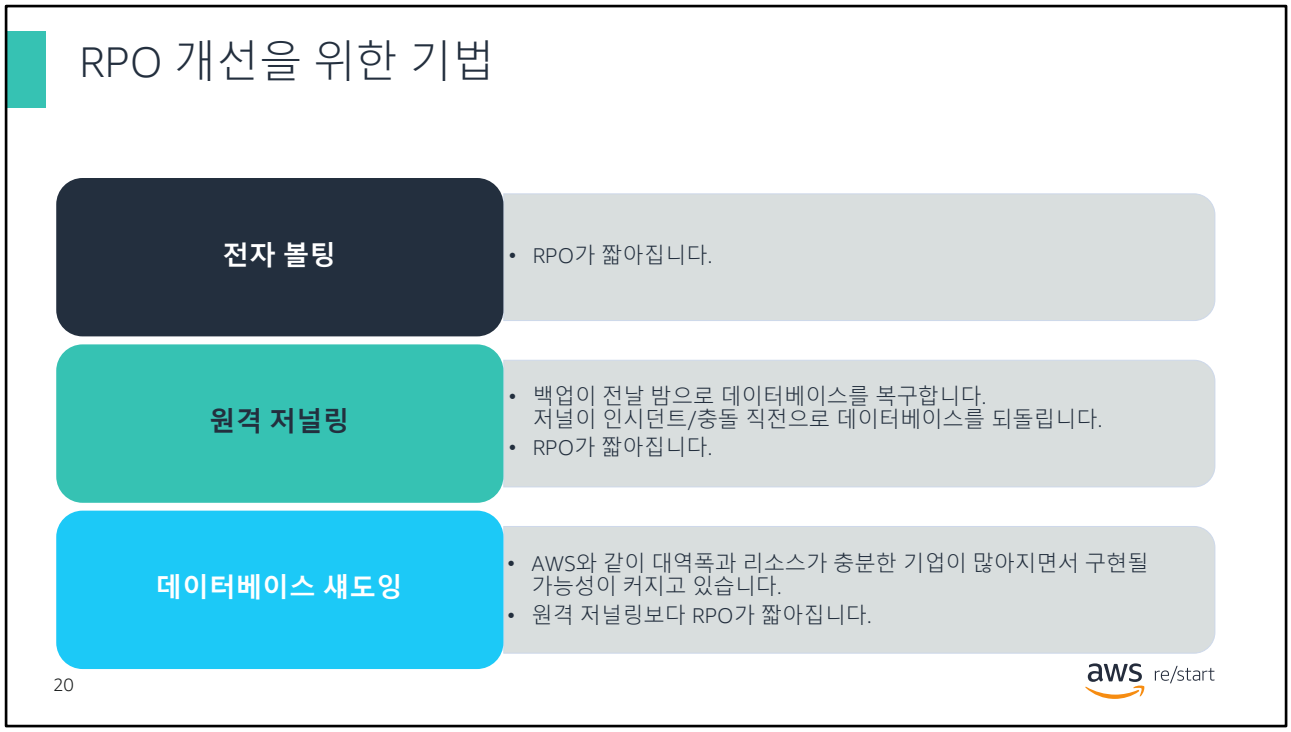
구독 서비스 및 외부 시설

구독 서비스는 대체 백업 및 처리 시설을 제공하는 제3자 공급 업체입니다.

핫 사이트	웜 사이트	콜드 사이트
몇 시간 만에 준비	더 저렴함	즉시 사용할 수 없음(최대 30일)
고가용성	기본 장비 및 연결	비용이 저렴함

Amazon Simple Storage Service(Amazon S3)는 클라우드 스토리지 서비스의 예로, 다양한 수준의 복구 속도와 비용으로 데이터를 백업하는 데 사용할 수 있습니다.

Amazon S3에 대한 자세한 내용은 Amazon S3 제품 웹 페이지를 참조하십시오.



전자 볼팅, 원격 저널링, 데이터베이스 섀도잉은 RPO를 개선할 수 있는 추가적인 데이터 관리 기법입니다. 특히 Amazon Relational Database Service(Amazon RDS) 및 Amazon DynamoDB와 같은 AWS 관리형 데이터베이스에서는 데이터베이스 섀도잉을 사용하여 데이터를 복제합니다. 데이터베이스 섀도잉은 동시에 업데이트되는 동일한 데이터베이스 두 개 이상을 사용합니다. 섀도우 데이터베이스를 로컬에 두어도 되지만 하나의 섀도우 데이터베이스는 외부에 호스팅하는 것이 모범 실무입니다.

전자 볼팅 - 전자 볼팅 솔루션을 사용하여 자동으로 가져오는 백업 데이터의 배치 덤프입니다. 데이터가 외부에 보호됩니다.
c- 각 트랜잭션이 완료될 때 항목이 저널(같은 시설에 있을 수 있음)에 써집니다.

데이터베이스 섀도잉 - 더 큰 중복성을 위해 서로 다른 위치에 있는 여러 개의 서버에 복제된 데이터베이스 세트를 생성합니다.

데이터 백업

백업 모범 실무

aws re/start

Redundant Array of Independent/Inexpensive Disk(RAID)는 여러 하드 디스크를 사용하여 데이터를 저장함으로써 성능을 최적화하고 중복성을 제공하는 스토리지 기술입니다.

데이터 백업 대체 방법

- 외부 및 현장
- 다양한 백업 유형:
  - 증분형
  - 미분형
  - 전체 백업
- 전자 볼팅(파일 백업)
- 원격 저널링(트랜잭션 로그)
- 데이터베이스 섀도잉
- 하드웨어 보안 모듈(HSM)

백업의 유형:

- **증분형 백업** - 마지막 증분형 백업 이후 새롭게 변경되거나 생성된 파일만 백업합니다. 이 옵션은 더 빠르고 스토리지 공간이 비교적 적게 필요합니다.
- **미분형 백업** - 마지막 전체 백업 이후에 변경되거나 생성된 파일만 백업합니다.
- **전체 백업** - 전체 파일을 백업합니다. 이 옵션은 더 많은 스토리지 공간이 필요하고 시간이 더 오래 걸립니다.
- **전자 볼팅** - 외부 위치에 물리적으로 백업하는 것이 아니라 전자적으로 백업 사이트에 데이터를 전송합니다.
- **원격 저널링** - 트랜잭션 로그의 사본을 전송합니다.
- **데이터베이스 섀도잉** - 대체 시설에 데이터베이스의 전체 사본을 유지 관리합니다.
- **하드웨어 보안 모듈(HSM)** - 디지털 키 보안 등 암호화 기능을 수행합니다.

아카이브 비트 백업

백업 유형	아카이브 비트를 기반으로 파일 선택	아카이브 비트 재설정
복사 함수		
전체		√
증분형	√	√
미분형	√	

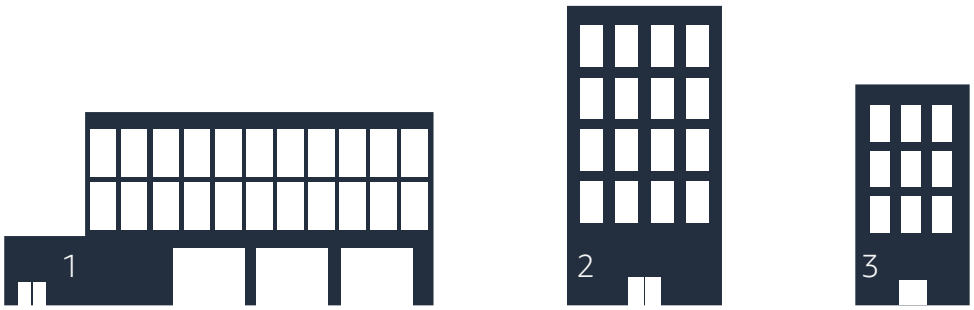
많은 백업 메커니즘이 파일과 관련된 **아카이브 비트** 속성에 의존합니다. 아카이브 비트 속성은 파일이 백업되었는지 나타냅니다.

이 테이블에는 백업 전략의 유형에 따라 이 아카이브 비트가 어떻게 사용되는지 나와 있습니다.

이벤트 관리 고려 사항

다중 센터

- 다중 센터(데이터 센터) 개념은 다음을 위해 설계되었습니다.
  - 여러 운영 센터로 프로세싱 분산
  - 중복성에 대한 분산된 아키텍처 접근법 생성



aws re/start

가장 중복성과 복원력이 높은 복구 솔루션에서는 여러 데이터 센터를 사용합니다.
예를 들어, AWS 클라우드 인프라는 가용 영역을 사용하여 네트워크와 장비를 물리적으로 격리함으로써 장애 조치와 중복성을 제공합니다.

장비 문서

비즈니스 하드웨어 및 유형의 자산에 관한 최신 문서는 BCP와 DRP 수행에 매우 중요합니다.

다음에 관한 장비 문서를 포함합니다.

- 네트워크 디바이스에 백업되는 구성 데이터
- 공급 업체 연락처
- 설명서
- 버전 정보
- 서버
- 최종 사용자 디바이스

이 외에도 조직에서 소유하는 자산에 따라 포함할 사항이 달라집니다.

BCP와 DRP 수행을 위해서는 장비와 유형 자산에 관한 문서를 유지 관리하는 것이 매우 중요합니다.

달성할 목표, 단계의 순서, 장비 문서를 명시한 계획에 더해 다음에 관한 문서를 유지 관리하시기 바랍니다.

- 연락처 정보
- 계약 정보
- 화면 캡처
- 설명서
- 양식
- 물리적 액세스
- 키(전자적 및 물리적)

핵심 사항

- 보안 이벤트에 효과적으로 대응하는 핵심 단계는 계획, 조사, 해결입니다.
- 비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP)을 통해 중단을 예방하고 최대한 빠르게 복구하는 방법을 식별하고 정의합니다.
- 백업의 주요 유형에는 증분형, 미분형, 전체 백업이 있습니다.
- Amazon S3와 같은 클라우드 서비스에서는 구독 기반 외부 백업 대체 서비스를 제공합니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 보안 이벤트에 효과적으로 대응하는 핵심 단계는 계획, 조사, 해결입니다.
- 비즈니스 연속성 계획(BCP)과 재해 복구 계획(DRP)을 통해 중단을 예방하고 최대한 빠르게 복구하는 방법을 식별하고 정의합니다.
- 백업의 주요 유형에는 증분형, 미분형, 전체 백업이 있습니다.
- Amazon S3와 같은 클라우드 서비스에서는 구독 기반 외부 백업 대체 서비스를 제공합니다.