

## IBM Cognos Controller on Cloud

다음은 주문자용 서비스 명세입니다.

### 1. 클라우드 서비스

클라우드 서비스 오퍼링은 아래 설명되어 있으며 선택되어 권한이 부여된 오퍼링은 주문서에 지정되어 있습니다. 주문서는 제공된 견적서와 클라우드 서비스의 시작일과 기간을 명시한 라이선스 증서로 구성됩니다. 청구서 작성은 클라우드 서비스를 프로비저닝한 후에 시작합니다.

#### 1.1 IBM Cognos Controller User on Cloud

IBM Cognos Controller 는 마감, 통합 및 보고 프로세스를 지원하는 금융 통합 소프트웨어입니다. 이 오퍼링을 통해 사용자는 재무 결과를 제공하고 재무 및 관리 보고서를 작성하고 주요 재무 비율과 척도에 대한 전사적 보기를 제공합니다.

IBM Cognos Controller User on Cloud 는 시스템을 통합하고 관리하며 시스템에 대해 보고할 수 있습니다.

#### 1.2 IBM Cognos Controller Jump Start on Cloud

IBM Cognos Controller Jump Start on Cloud 원격 서비스에는, 초기 IBM Cognos Controller on Cloud(CCoC) 유스 케이스의 간편한 식별, IBM CCoC 구현의 프로젝트 계획 및 시작을 위한 코칭, IBM CCoC 보고서 작성에 대한 검증된 사례의 코칭을 포함하여 최대 80 시간의 코칭과 지원이 포함되며, 유지보수 코칭과 IBM CCoC 서비스의 관리는 인게이지먼트별로 구매되며 모든 시간을 사용했는지 여부에 관계 없이 구입한 후 90 일에 만료됩니다.

#### 1.3 IBM Cognos Controller Additional Non-Production Instance

본 오퍼링은 IBM Cognos Controller 의 추가적인 비프로덕션 인스턴스를 추가합니다. 본 오퍼링은 테스트, 성능 조정, 결함 진단, 벤치마킹, 스테이징(Staging), 품질 보증 활동 및/또는 공개된 API(Application Programming Interfaces)를 통해 내부적으로 사용되는 오퍼링의 추가 기능 또는 확장 기능의 개발을 포함하여(단, 이에 한하지 않음) 클라이언트의 비프로덕션 활동의 일부로만 사용될 수 있습니다.

### 2. 보안 설명

#### 2.1 보안 정책

IBM 은 정보 보안 팀을 운영하며 IBM 직원에게 통지하는 개인 정보 보호 및 보안 정책도 유지 관리합니다. IBM 은 IBM 데이터 센터를 지원하는 직원에게 개인 정보 보호 및 보안 교육을 받도록 요구합니다. IBM 보안 정책 및 기준은 매년 검토되어 재평가됩니다. IBM 보안 문제는 종합적인 사고 대응 절차에 따라 처리됩니다.

#### 2.2 접근 권한 통제

고객 데이터에 대한 접근이 필요한 경우, 업무 분리 원칙에 따라 권한이 부여된 IBM 지원 담당자만 접근이 허용됩니다. IBM 직원(또는 그에 준하는)은 중간 "게이트웨이" 관리 호스트에 대한 이중(two-factor) 인증 방식을 사용합니다. 고객 데이터 접속 시 모든 연결은 암호화된 채널로 제공됩니다. 고객 데이터에 대한 접근과 호스팅 환경 내외부의 데이터 전송은 모두 기록됩니다. 이 클라우드 서비스를 지원하는 IBM 데이터 센터 내부에서는 WIFI 사용이 금지됩니다.

#### 2.3 서비스 무결성 및 가용성

운영 체제와 애플리케이션 소프트웨어를 수정하려면 IBM 변경 관리 프로세스를 준수해야 합니다. 방화벽 규칙의 변경도 변경 관리 프로세스에 따라 수행되며 변경사항을 구현하기 전에 IBM 보안 직원(또는 그에 준하는)의 검토를 별도로 받습니다. IBM 은 데이터 센터를 24x7 원칙으로 감시합니다. 허가된 관리자와 제 3 자 벤더는 내외부 취약성 스캐닝을 정기적으로 실시하여 잠재적인 시스템 보안 문제를 발견하고 해결할 수 있도록 지원합니다. 모든 IBM 데이터 센터에는 악성 소프트웨어 감지(안티바이러스, 침입 감지, 취약성 스캐닝 및 침입 방지) 시스템이 사용됩니다. IBM 데이터 센터 서비스는 공용 네트워크에서

데이터를 전송하기 위해 다양한 정보 전달 프로토콜을 지원합니다. 예를 들면, HTTPS/SFTP/FTPS/S/MIME, site-to-site VPN 이 있습니다. 오프 사이트 저장 목적의 백업 데이터는 전송되기 전에 암호화됩니다.

## 2.4 활동 로깅

IBM 은 활동 로깅 용도로 구성된 시스템, 애플리케이션, 데이터 저장소, 미들웨어 및 네트워크 인프라스트럭처 디바이스의 활동 로그를 유지 관리합니다. 로그의 조작을 방지하고 중앙 집중적 분석, 경보 및 보고 기능을 수행할 수 있도록 활동 로깅은 중앙 로그 저장소에서 실시간으로 처리됩니다. 조작 방지를 위해 데이터는 서명됩니다. 이상 동작을 찾기 위해 정기 분석 보고서를 통해 로그를 실시간으로 분석합니다. 운영 직원(또는 그에 준하는)에게 이상 동작을 통지하고 필요한 경우 24x7 on-call 보안 전문가에게 문의합니다.

## 2.5 물리적 보안

IBM 은 IBM 데이터 센터에 대한 불법적인 물리적 접근을 제한하기 위해 마련된 물리적 보안 기준을 유지 관리합니다. 데이터 센터에 대해서는 이중 인증 방식과 감시 카메라를 통한 통제와 모니터링이 적용되는 제한적인 접근 지점만 제공됩니다. 데이터 센터에 대한 접근은 접근 권한이 승인된 직원(또는 그에 준하는)만 가능합니다. 운영 직원(또는 그에 준하는)은 승인 여부를 검증한 후 접근 권한을 부여하는 액세스 배지를 발행합니다. 해당 액세스 배지를 획득한 직원은 기타 상이한 액세스 배지는 포기해야 하며 활동 기간에만 데이터 센터 액세스 배지를 소유할 수 있습니다. 액세스 배지의 사용은 기록됩니다. 비 IBM 방문자는 근무지 사이트에 입장 시 등록을 해야 하고 근무지 사이트에 있는 동안 안내자가 동행합니다. 권한이 없는 개인이 현장을 방문할 수 있는 서비스 제공 지역, 물류장 및 기타 지점은 관리 하에 격리됩니다.

## 2.6 준수

IBM 은 IBM 개인정보 보호정책이 미국 상무부의 Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement 와 일치하는지 매년 증명합니다. IBM 은 프로덕션 데이터 센터에서 매년 업계 표준 SSAE 16 감사(또는 그와 동등한 감사)를 실시합니다. IBM 은 IBM 비즈니스 요건을 준수하기 위해 보안 및 개인 정보 보호 관련 활동을 검토합니다. IBM 팀은 IBM 의 정보 보안 정책을 준수하는지 여부를 확인하기 위해 정기적인 평가와 감사를 합니다. IBM 직원과 공급업체 직원은 매년 보안 인식 교육을 받습니다. 업무 윤리 강령, 기밀 보호 및 IBM 보안 의무를 준수할 의무와 업무 목표를 매년 직원에게 숙지시킵니다.

## 3. 서비스 레벨 협약

IBM 은 클라우드 서비스의 가용성에 관한 "서비스 레벨 계약"(이하 SLA)을 제공합니다. 귀하는 SLA 가 귀하에게 보증을 제공하는 것이 아님을 이해합니다.

### 3.1 용어 정의

- a. "허가된 담당자"는 본 SLA 에 따라 클레임을 제출할 수 있는 권한이 부여된 IBM 에게 명시한 개인(들)을 의미합니다.
- b. "가용성 크레딧"은 유효한 클레임에 대해 IBM 이 제공하는 배상을 의미합니다. 가용성 크레딧은 클라우드 서비스 등록료를 청구하는 추후 청구서에 대한 크레딧 또는 할인의 형식으로 적용됩니다.
- c. "클레임"은 계약 월 동안 서비스 레벨에 부합하지 못하였다고 귀하가 SLA 에 따라 IBM 에 제출하는 클레임을 의미합니다.
- d. "고객"은 IBM 에게 직접 서비스를 신청하는 실체(entity)로서, IBM 과의 서비스 계약에 따른 지불 의무를 포함하여 어떠한 중대한 의무도 불이행 상태가 아닌 실체를 의미합니다.
- e. "계약 월"은 해당 월 1 일의 12:00 AM(미 동부시)부터 해당 월 말일의 11:59 PM(미 동부시)까지, 해당 기간 동안의 매월을 의미합니다.
- f. "중지 시간"은 클라우드 서비스에 대한 프로덕션 시스템 처리가 중지되고 권한을 가진 사용자가 클라우드 서비스의 모든 부분을 이용할 수 없는 기간을 의미합니다. 중지 시간에는 다음으로 인해 클라우드 서비스를 사용할 수 없는 기간은 포함되지 않습니다.

- (1) 스케줄되거나 통지된 유지보수 목적의 가동 중단

- (2) IBM의 통제권을 벗어난 이벤트 또는 원인(예: 자연 재해, 인터넷 중단, 긴급 유지보수 등);
  - (3) 귀하의 애플리케이션, 설비, 데이터 또는 제 3자의 애플리케이션, 설비, 데이터와 관련한 문제;
  - (4) 필수 시스템 구성 및 클라우드 서비스 액세스를 위한 지원 플랫폼을 이용하지 않은 경우;
  - (5) 귀하가 IBM에게 제공하거나 귀하를 대신한 제 3자가 IBM에 제공한 설계, 명세 또는 지침을 IBM이 따른 경우.
- g. "이벤트"는 특정 상황 또는 여러 상황이 합쳐져서 결과적으로 SLA에 부합되지 못하게 한 경우, 그러한 특정 상황 또는 여러 상황을 의미합니다.
- h. "서비스 레벨"은 본 SLA에서 IBM이 제공하는 서비스의 레벨을 IBM이 측정하도록 아래와 같이 설정된 표준을 의미합니다.

### 3.2 가용성 크레딧

- a. 클레임을 제출하기 위해서는 이벤트가 귀하의 클라우드 서비스 사용에 영향을 준 것을 귀하가 처음으로 인식한 시간으로부터의 24시간 이내에 각 이벤트에 대해 각 이벤트의 심각도 1 지원 티켓(아래 기술 지원 조항에서 정의된 사항 참조)을 귀하가 IBM 기술 지원 헬프 데스크에 로그(log)해야 합니다. 귀하는 이벤트에 대한 필요한 정보를 모두 제공하고 이벤트의 진단과 해결을 위해 합리적인 범위 내에서 IBM에 협력해야 합니다.
- b. 귀하는 가용성 크레딧에 대한 클레임이 발생한 계약 월의 말일로부터 3영업일이 지나기 이전에 해당 클레임을 제출해야 합니다.
- c. 가용성 크레딧은 고객이 최초로 중지 시간에 의한 영향을 받았다고 고객이 보고한 시점부터 측정된 중지 시간의 기간을 기준으로 합니다. 유효한 각 클레임의 경우, IBM은 아래 표와 같이 각 계약 월 동안 달성한 서비스 레벨에 따라 적용 가능한 최대의 가용성 크레딧을 적용합니다. IBM은 동일한 계약 월에서 동일한 이벤트에 대해 복수의 가용성 크레딧을 제공하지 않습니다.
- d. 어떠한 경우에도 계약 월에 적용되는 가용성 크레딧의 총 금액은 귀하가 IBM에 클라우드 서비스 대가로 지불한 연간 대금의 12분의 1(1/12)의 10%를 초과하지 않습니다.

### 3.3 서비스 레벨

계약 당월 동안 클라우드 서비스 가용성

계약 당월 동안 가용성	가용성 크레딧 (클레임 대상이 되는 계약 월의 월 등록(Subscription) 사용료의 %)
99% - 99.75%	2%
95% - 98.99%	5%
95.0% 미만	10%

백분율로 표시된 가용성은 (a) 계약 월의 총 시간(분)에서 (b) 계약 월의 총 중지 시간(분)을 뺀 후 이를 (c) 계약 월의 총 시간(분)으로 나누어 산출합니다.

예제: 계약 월의 총 중지 시간 476 분

계약 월 30 일 동안 총 43,200 분 - 중지 시간 476 분 = 42,724 분	= 계약 월 동안 가용성 98.9%에 대한 가용성 크레딧 5%
<hr/> 계약 월 30 일 동안 총 43,200 분	

### 3.4 SLA 에 대한 기타 정보

본 SLA 는 IBM 의 고객에게만 제공되며 클라우드 서비스에 대한 귀하의 사용자, 게스트, 참여자 및 허용된 초청객이 청구한 클레임 또는 IBM 이 제공한 베타 서비스나 시험 서비스에는 적용되지 않습니다. SLA 는 프로덕션 용도의 클라우드 서비스에만 적용됩니다. 테스트, 재해 복구, 품질 보증 또는 개발을 포함한(단, 이에 한하지 않음) 비프로덕션 환경에는 SLA 가 적용되지 않습니다.

## 4. 권한 부여 및 대금 청구 정보

### 4.1 과금 체계

클라우드 서비스는 주문서에 명시된 바와 같이 다음 중 하나의 과금 체계 하에서 제공됩니다.

- a. 인스턴스(Instance)는 클라우드 서비스 오퍼링 구입 시 사용되는 측정 단위입니다. 인스턴스는 클라우드 서비스의 특정 구성에 대한 액세스를 의미합니다. 주문서에 명시된 측정 기간 동안 액세스하여 사용하도록 제공된 클라우드 서비스의 각 인스턴스에 대해 충분한 권한을 취득해야 합니다.
- b. 허가된 사용자(Authorized User)는 클라우드 서비스 구입 시 사용되는 측정 단위입니다. 허가된 사용자는 클라우드 서비스에 대한 고유의 액세스 권한이 부여되는 고유한 개인입니다. 귀하는 주문서에 명시된 서비스 제공 기간 동안 다양한 수단을 통해(예: 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스 오퍼링에 액세스하는 각 허가된 사용자에 대한 별도의 전용 권한을 취득해야 합니다. 허가된 사용자를 위한 권한은 해당 허가된 사용자에게만 부여되며, 다른 사람과 공유할 수 없고, 허가된 사용자 권한을 다른 사람에게 영구 양도하는 경우를 제외하고는 재양도할 수 없습니다. 클라우드 서비스의 목적상, 귀하는 귀하 기업집단 외부의 사용자에게 액세스를 제공할 수 있습니다. 이러한 사용자는 허가된 사용자로 간주되며 적절한 권한이 부여됩니다.
- c. 인게이지먼트(Engagement)는 서비스 구입 시 사용되는 측정 단위입니다. 인게이지먼트는 클라우드 서비스와 관련된 전문 서비스 및/또는 교육 서비스로 구성됩니다. 각 인게이지먼트(Engagement)를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

### 4.2 대금 및 청구

클라우드 서비스에 대해 지불하는 대금은 주문서에 명시됩니다.

### 4.3 설치(Set-Up) 요금

설치 요금은 주문서에 명시됩니다.

### 4.4 월 분할(Partial Month) 요금

월 분할 요금은 비례 배분된 일일 요금입니다. 월 분할 요금은 클라우드 서비스 오퍼링에 대한 액세스가 허용된다고 귀하가 IBM 으로부터 통지받은 날부터 시작하는 해당 월의 나머지 일수를 기준으로 계산합니다.

### 4.5 On Demand 요금

주문서에 포함된 On-Demand 옵션의 경우 귀하가 On-Demand 파트의 활성화를 요청하지 않으면 청구되지 않습니다. 활성화하는 경우에는 주문서에 명시된 비율에 따라 청구됩니다.

## 5. 기간 및 갱신 옵션

### 5.1 기간

클라우드 서비스의 기간은 주문서에 명시된 바와 같이, 클라우드 서비스에 대한 액세스 권한을 귀하가 가진다고 IBM 이 귀하에게 통지한 날부터 시작됩니다. 해당 기간의 정확한 시작 날짜와 종료 날짜는 주문서의 라이선스 증서 부분에 명시됩니다. 귀하는 IBM 또는 귀하의 IBM 비즈니스 파트너와의 계약을 통해 해당 기간 동안 귀하의 클라우드 서비스의 사용 레벨을 상향 조정할 수 있습니다. IBM 은 상향 조정된 사용 레벨을 주문서를 통해 확정합니다.

## 5.2 클라우드 서비스 기간 갱신 옵션

귀하의 거래서류는 다음 중 하나로 기간을 지정하여, 기간 종료 시 클라우드 서비스가 갱신될지 여부를 명시합니다.

### 5.2.1 자동 갱신

주문서에서 자동 갱신으로 명시되어 있는 경우 귀하는 주문서에 지정된 기간 만료일보다 최소 90 일 이전에 서면 요청서를 통해 클라우드 서비스를 해지할 수 있습니다. IBM 또는 고객의 IBM 비즈니스 파트너가 만료일까지 그러한 해지 통지를 수신하지 못하면 만료 기간은 1 년 또는 라이선스 증서에 명시된 최초 기간과 동일한 기간만큼 자동으로 갱신됩니다.

### 5.2.2 연속적 청구

주문서에서 연속적 청구로 명시한 경우 귀하는 귀하의 기간이 종료된 후에도 계속해서 클라우드 서비스에 대한 액세스 권한을 가지며 연속적 기준에 따라 클라우드 서비스의 사용 대금이 청구됩니다. 클라우드 서비스의 사용을 중단하고 연속적 청구 절차를 중지하려면 귀하의 클라우드 서비스의 취소를 요청하는 서면 통지를 90 일 전에 IBM 이나 IBM 비즈니스 파트너에게 제공해야 합니다. 귀하의 액세스가 취소되면 취소가 발효된 해당 월의 미지불된 액세스 대금이 귀하에게 청구됩니다.

### 5.2.3 갱신

주문서에서 갱신 유형을 "종료"로 지정한 경우에는 기간이 만료되면 클라우드 서비스가 종료되며 클라우드 서비스에 대한 액세스 권한은 소멸됩니다. 종료 날짜 이후에도 클라우드 서비스를 계속 사용하려면 귀하는 IBM 영업 담당자나 IBM 비즈니스 파트너에게 새로운 등록 기간을 구매하는 주문서를 접수해야 합니다.

## 6. 기술 지원

등록 기간에는 클라우드 서비스에 대한 기술 지원이 제공됩니다.

**전화 및 이메일 지원의 정기 운영 시간은 다음과 같습니다.**

지원 티켓 또는 이메일: 언제든지. 지정된 심각도 레벨에 따라 티켓 처리. 심각도 2 - 4 레벨은 업무 시간에 처리됩니다.

전화: 월요일 - 금요일(IBM 회사 준수 휴일 제외), 현지 시간 오전 9 시 - 오후 5 시.

**업무 시간 외 지원:**

업무 시간 외 지원(상기의 정기 운영 시간 외)은 심각도 1 의 문제점에 한해 영업일, 주말 및 공휴일에 제공됩니다.

지원 핫라인: 1-877-465-5444.

이메일: [vsupport@ca.ibm.com](mailto:vsupport@ca.ibm.com)

이메일을 통한 티켓 로깅에서 고객은 임시 Varicent/IBM 주소를 사용해야 합니다.

지원 웹 포털: <http://support.varicent.com>

기술 지원 안내는 첨부된 링크를 참조하십시오. <http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html>.

심각도(Severity)	심각도 정의	대응 시간 목표	대응 시간 범위
1	<b>심각한 업무 영향/서비스 다운:</b> 중대한 업무 기능이 작동 불가능하거나 중대한 인터페이스에 장애가 발생했습니다. 일반적으로 프로덕션 환경에 적용되며 서비스에 대한 액세스 불능으로 인해 운영에 심각한 영향을 끼치는 경우를 의미합니다. 이 경우 즉각적인 해결책을 제공해야 합니다.	1 시간 이내	24x7

심각도(Severity)	심각도 정의	대응 시간 목표	대응 시간 범위
2	<b>상당한 업무 영향:</b> 서비스 업무 기능이 사용에 있어 상당히 제한되거나 귀하가 업무 기한을 준수하지 못하게 됩니다.	2 영업시간 이내	월요일 - 금요일 영업시간
3	<b>사소한 업무 영향:</b> 서비스 또는 기능을 이용할 수 있으며 운영에 대한 심각한 영향이 없는 것을 의미합니다.	4 영업시간 이내	월요일 - 금요일 영업시간
4	<b>최소 업무 영향:</b> 조사 또는 비기술적 요청	1 영업일 이내	월요일 - 금요일 영업시간

## 7. Safe Harbor 준수

본 클라우드 서비스에 대한 US-EU and US-Swiss Safe Harbor Frameworks 준수 여부에 대해서는 결정된 바 없습니다.

## 8. 추가 정보

### 8.1 파생 혜택 사업장

해당하는 경우, 세금은 귀하가 클라우드 서비스의 혜택을 제공받는 것으로 식별한 사업장을 기준으로 부과됩니다. 귀하가 추가 정보를 제공하지 않는 한, IBM은 클라우드 서비스 주문 시 1 차 혜택 사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 귀하는 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM에 제공해야 할 책임이 있습니다.

### 8.2 개인 건강 정보

클라우드 서비스는 HIPAA를 준수하도록 설계되지 않으며 개인 건강 정보를 전송하거나 저장할 목적으로는 사용될 수 없습니다.

### 8.3 쿠키

귀하는 IBM이 클라우드 서비스의 정상적인 운영과 지원 과정에서 추적 및 기타 기술을 사용하여 클라우드 서비스 사용과 관련된 개인 정보를 귀하(귀하의 직원과 계약직 직원)로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM은 사용자 경험을 개선하거나 소통을 맞추기 위한 목적으로 클라우드 서비스의 효율성에 대한 통계와 정보를 수집합니다. 귀하는 IBM, 기타 IBM 회사 및 하도급자 내부에서, 그리고 IBM 및 IBM 하도급자가 비즈니스를 수행하는 어디서나, 관련 법률을 준수하면서, 상기의 목적으로 수집된 개인 정보를 IBM이 처리하기 위해 필요한 동의를 이미 획득했거나 획득할 것임을 확인합니다. IBM은 수집된 개인 정보에 접근하거나 갱신하거나 정정하거나 삭제하고자 하는 고객 직원과 계약직 직원의 요청을 수용합니다.

### 8.4 재해 복구 및 콘텐츠 백업

본 클라우드 서비스에는 다음 재해 복구 및 콘텐츠 백업 서비스도 포함됩니다.

재난 상황(재난은 "불가항력"을 의미하며, 이는 천재지변, 테러, 노동 쟁의, 화재, 홍수, 지진, 폭동, 전쟁, 정부의 조치, 명령 또는 제한, 바이러스, DOS 공격 및 기타 악의적 행위, 유틸리티 및 네트워크 연결 장애, IBM의 합리적인 제어를 벗어난 클라우드 서비스 장애의 기타 원인을 의미함)이 발생한 경우 IBM은 다음과 같이 클라우드 서비스에 대한 귀하의 액세스를 복원하도록 작업합니다.

- 표준 옵션 - 고객이 14일 이내에 클라우드 서비스에 대한 액세스를 재개할 수 있도록 IBM의 데이터 센터 네트워크에 하드웨어, 소프트웨어 및 네트워크 인프라스트럭처를 제공합니다.
- 프리미엄 옵션 - 고객이 5일 이내에 클라우드 서비스에 대한 액세스를 재개할 수 있도록 IBM의 데이터 센터 네트워크에 하드웨어, 소프트웨어 및 네트워크 인프라스트럭처를 제공합니다.

복원된 콘텐츠 데이터 세트의 콘텐츠 손실로부터 24시간 내에 아래와 같이 최신 콘텐츠 백업을 통해 환경을 복원합니다.

백업은 매일 수행되며 1 차 위치의 불가항력 상황 시 오프사이트에 복사됩니다. IBM은 순환 주기(rolling basis)로 백업을 보관합니다. 전체 데이터베이스 백업을 7일마다 수행하고 해당 주 이내의 각 익일에

상대적 차등 백업을 수행합니다. IBM 은 최근 7 일 간의 매일 차등 백업과 이전 28 일 간의 전체 백업을 보관합니다. 새로운 전체 백업이 작성되면 가장 오래된 버전이 삭제됩니다. 백업은 디스크 기반 백업 시스템 저장 시(at rest)와 오프사이트로 전송 시에 암호화됩니다.