IBM Financial Crimes Insight

본 서비스 명세서는 본 클라우드 서비스에 대해 설명합니다. 관련 주문 서류에서는 고객의 주문에 대한 가격 책정과 추가적인 세부사항을 제공합니다.

1. 클라우드 서비스

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM Financial Crimes Insight Basic

이 클라우드 서비스는 Financial Crimes Insights 오퍼링을 구축하는 공통 인프라와 공통 서비스 세트를 제공합니다. IBM Financial Crimes Insight 는 고객이 통합된 금융 범죄 오퍼링 세트를 활용할 수 있도록 오퍼링 간에 필요한 통합을 제공합니다.

1.1.2 IBM Financial Crimes Insight Advanced

이 클라우드 서비스는 IBM Financial Crimes Insight Basic 과 동일한 기능 세트를 제공하며 IBM Financial Crimes Insight - Data Science 에 명시된 기능도 포함합니다.

IBM Financial Crimes Insight Basic 또는 IBM Financial Crimes Insight Advanced 는 클라우드 서비스의 인스턴스(Instance)를 제공하는 필수 구성요소입니다.

1.1.3 IBM Financial Crimes Insight Basic Non-Production

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Financial Crimes Insight Basic Non-Production 기능에 액세스할 수 있도록 해줍니다.

1.1.4 IBM Financial Crimes Insight Advanced Non-Production

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Financial Crimes Insight Advanced Non-Production 기능에 액세스할 수 있도록 해줍니다.

1.1.5 IBM Financial Crimes Insight Advanced BYOL

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Financial Crimes Insight Advanced 기능에 액세스할 수 있도록 해줍니다. 고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. IBM Financial Crimes Insight Advanced BYOL 오퍼링에 필요한 IBM 프로그램은 IBM Cloud Pak for Data Financial Crimes Insight 입니다.

1.1.6 IBM Financial Crimes Insight Advanced Non-Production BYOL

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Financial Crimes Insight Advanced Non-Production 기능에 액세스할 수 있도록 해줍니다. 고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. IBM Financial Crimes Insight Advanced Non-Production BYOL 오퍼링에 필요한 IBM 프로그램은 IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment 입니다.

1.1.7 IBM Financial Crimes Insight for Entity Research Negative News API

이 클라우드 서비스는 필터링하여 순위를 매긴 기사 목록을 출력하여 잠재적 금융 범죄 위험을 밝힐 목적으로 비정형 뉴스와 미디어를 검색하고 분석하고 우선 순위를 정하는 코그너티브 컴퓨팅 기술 및 고급 분석을 활용합니다. 이 오퍼링은 조직에서 워크플로우 및 프로세스에 호출하거나 내장할 수 있는 API 로 제공됩니다.

1.1.8 IBM Financial Crimes Insight for Entity Research Enrichment API

이 클라우드 서비스는 코그너티브 컴퓨팅 기술을 활용하여 조직의 엔티티 이해도를 높이고 엔티티 또는 고객의 레코드를 최신 상태로 유지하고 엔티티의 잠재적 금융 범죄 위험을 밝힐 수 있도록 돕는 데이터를 정형 소스들에서 수집합니다. 엔티티에는 고객, 거래 상대방 또는 공급자가 포함됩니다. 이 오퍼링은 조직에서 워크플로우 및 프로세스에 호출하거나 내장할 수 있는 API 로 제공됩니다.

1.2 선택적 서비스

고객은 IBM Financial Crimes Insight 또는 IBM Financial Crimes Insight Non-Production 의 사용등록에 추가하여, 다음 클라우드 서비스 중 하나에 대해서도 사용등록해야 합니다.

1.2.1 IBM Financial Crimes Insight Data Science

이 클라우드 서비스는 데이터를 준비하고 모델을 구축, 훈련 및 관리하는 기능뿐만 아니라 엔터프라이즈 데이터와 AI 모델 거버넌스, 품질 및 협업을 관리하기 위한 데이터 카탈로그도 제공합니다.

1.2.2 IBM Financial Crimes Insight for Anti-Money Laundering

IBM Financial Crimes Insight for Anti-Money Laundering(FCI for AML)은 고급 분석 계층들을 적용하여 금융 활동을 감시하며 고객이 엔티티의 자금 세탁 성향을 파악할 수 있도록 돕습니다. FCI for AML 은 인적, 활동 및 관계 데이터를 활용하여 알려진 위험에 대한 고객의 검토 프로세스를 지원하고 숨겨진 위험을 설명할 수 있는 통찰을 제공하여 위험 적용 범주를 확장할 수도 있습니다.

1.2.3 IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring

이 클라우드 서비스는 경보 선별 프로세스를 효율화하고 거짓 긍정(false positives)을 줄이고 경보 처분을 촉진하며 엔티티의 위험성에 대한 더 나은 이해를 바탕으로 의사 결정을 개선하는 것을 목표로 과거 사례의 데이터, 문맥적 증거의 데이터 집합 및 기계 학습 기능을 활용합니다. 이 서비스는 고객 기관의 기존 거래 감시와 사례 관리 시스템 간에 적합한 추가 구성요소입니다.

1.2.4 IBM Financial Crimes Insight for Alert Triage – Transaction List Screening

이 클라우드 서비스는 구성 및 확장 가능한 API 기반 파이프라인을 통해 경보가 발행된 거래를 분석하여 기존 제재 심사 시스템을 보강합니다. 거래 데이터는 정리, 구문 분석 및 랭글링 후 휴리스틱 및 코그너티브 컴퓨팅 기술을 사용하여 처리됩니다. 결과를 기초로 스코어링하고 거짓 긍정(false positives)을 식별하며 유익한 맞춤형 통찰을 제공합니다.

1.2.5 IBM Financial Crimes Insight for Entity Research

이 클라우드 서비스는 엔티티 및/또는 관련 위험성에 대한 이해를 개선하고 KYC(Know Your Customer) 활동을 완료하는 시간을 단축하는 것을 목표로 정형 및 비정형 데이터 소스의 관련 컨텐츠를 선별하고 추출하고 연관시키는 코그너티브 컴퓨팅 기술을 활용합니다. 이 솔루션은 다양한 데이터 소스를 통합하여 고객 정보 검색과 분석을 자동화하고 표준화하도록 돕습니다. 이 서비스의 목표는 리서치 및 실사 활동을 효율적으로 완료하여 고객 경험을 개선하는 것과 더불어 향상된 KYC 레코드 품질을 제공하는 것입니다.

고객은 다음 권한 옵션 중에서 선택할 수 있습니다.

- IBM Financial Crimes Insight for Entity Research – Enterprise – 각 이벤트(Event)로 6 개 이상의 관련 당사자에 대한 조사가 가능합니다.
- IBM Financial Crimes Insight for Entity Research – Advanced – 각 이벤트(Event)로 최대 5 개의 관련 당사자에 대한 조사가 가능합니다.
- IBM Financial Crimes Insight for Entity Research – Basic – 각 이벤트(Event)로 최대 2 개의 관련 당사자에 대한 조사가 가능합니다.

관련 당사자는 4.1 항에 정의된 상위 조사에 대한 검토 과정에서 조사가 필요한 엔티티(조직 또는 개인)를 의미합니다. 일반적으로, 이는 조직도 내에서 승인된 서명자, 임원, 궁극적 수혜자, 모회사 또는 자회사가 될 수 있습니다. 다시 말해서, 관련 당사자가 개별 또는 관련 구성원의 조사를 필요로 하는 엔티티인 경우 각 개별 또는 관련 구성원도 관련 당사자로 간주됩니다.

1.2.6 IBM Financial Crimes Insight for Entity Research with Material Change

이 클라우드 서비스는 엔티티 및/또는 관련 위험성에 대한 이해를 개선하고 KYC(Know Your Customer) 활동을 완료하는 시간을 단축하는 것을 목표로 정형 및 비정형 데이터 소스의 관련 컨텐츠를 선별하고 추출하고 연관시키는 코그너티브 컴퓨팅 기술을 활용합니다. 이 솔루션은 다양한 데이터 소스를 통합하여 고객 정보 검색과 분석을 자동화하고 표준화하도록 돕습니다. 이 서비스의 목표는 리서치 및 실사 활동을 효율적으로 완료하여 고객 경험을 개선하는 것과 더불어 향상된 KYC 레코드 품질을 제공하는 것입니다. 이에는 일정에 따라 엔티티를 감시하여 중요한 차이점을 확인하고 분석가에게 검토를 위한 경보를 제공할 수 있도록 하는 중요 변경 기능이 포함됩니다.

고객은 다음 권한 옵션 중에서 선택할 수 있습니다.

- IBM Financial Crimes Insight for Entity Research – Enterprise – 각 이벤트(Event)로 6 개 이상의 관련 당사자에 대한 조사가 가능합니다.
- IBM Financial Crimes Insight for Entity Research – Advanced – 각 이벤트(Event)로 최대 5 개의 관련 당사자에 대한 조사가 가능합니다.
- IBM Financial Crimes Insight for Entity Research – Basic – 각 이벤트(Event)로 최대 2 개의 관련 당사자에 대한 조사가 가능합니다.

관련 당사자는 4.1 항에 정의된 상위 조사에 대한 검토 과정에서 조사가 필요한 엔티티(조직 또는 개인)를 의미합니다. 일반적으로, 이는 조직도 내에서 승인된 서명자, 임원, 궁극적 수혜자, 모회사 또는 자회사가 될 수 있습니다. 다시 말해서, 관련 당사자가 개별 또는 관련 구성원의 조사를 필요로 하는 엔티티인 경우 각 개별 또는 관련 구성원도 관련 당사자로 간주됩니다.

1.2.7 IBM Financial Crimes Insight for Claims Fraud – Property and Casualty

이 클라우드 서비스는 전체 조사 라이프사이클을 관리하고 결과물에 대해 보고하기 위해 그리고 고객, 의료 제공자 또는 기타 주체가 제출한 사기 청구로 인해 발생한 위험성을 발견하기 위해 조직이 데이터를 분석하도록 도와주는 오퍼링입니다.

1.2.8 IBM Financial Crimes Insight for Claims Fraud – Investigation

이 클라우드 서비스는 조직이 의심스러운 활동 및 잠재적 사기에 대한 전체 조사 라이프사이클을 관리하도록 도와줍니다.

1.2.9 IBM Electronic Communication Surveillance Analytics on Cloud

이 클라우드 서비스는 의심스러운 의사 교환의 다양한 패턴을 발견하기 위해 금융 서비스 기관에서 다중 채널을 통한 직원의 상호작용 데이터를 효과적으로 분석하여 모니터링할 수 있도록 지원하는 도구입니다. 이 도구를 사용하여 시장 지위 남용 및 조작에 대한 다양한 부정 행위 패턴을 감지할 수 있습니다. 이 도구는 자연어 처리 기능을 활용하여 텍스트 정보를 이해하고 컨텍스트에 따라 모호한 용어를 구분합니다. 또한 의사 교환을 분석하는 데 활용될 수 있는 정서 및 감정 분석 기능을 사용합니다. 이들 기능은 개인의 성격 특성을 추론하지 않으며 이를 추론하는 데 사용하도록 의도되지 않습니다. 전반적 추론 엔진에 분석을 제공하여 다양한 통찰을 연관시키고 특별 감사 책임자에게 리스크 예측을 제공하도록 지원합니다.

1.2.10 IBM Voice Surveillance Analytics on Cloud

이 클라우드 서비스는 금융 서비스 기관이 다중 채널을 통한 직원의 음성 의사 교환을 분석하고 감시하여 의심스러운 활동을 발견하도록 돕는 도구입니다. 이 도구는 문법과 언어 구조를 감지하는 기계 학습을 활용하여 음성-문자 변환 기술을 통해 사람의 음성을 문자로 된 단어로 변환합니다. 음성-문자 변환 출력과 전화 통신 시스템에서 생성한 리치 메타 데이터를 연결하고 텍스트에 스피커 이원화를 적용하여 원하는 음성 대화를 빠르고 쉽게 검색하고 재생할 수 있도록 합니다. 메타 데이터와 함께 음성-문자 변환 출력을 알기 쉬운 형식으로 고객에게 제공합니다. 이 도구에서는 추가 옵션으로, 컨텐츠에서 시맨틱 메타 데이터를 추출하는 자연어 처리 기능과 주제, 어조, 정서 및 감정을 감지하는 언어적 분석 기능을 사용할 수 있습니다. 이들 기능은 개인의 성격 특성을 추론하지 않으며 이를 추론하는 데 사용하도록 의도되지 않습니다. 모든 음성-문자 변환은 중복 파일 및 음성 내용의 저장 공간을 줄이기 위해 "인메모리"에서 수행되며 처리 이후에는 음성 데이터가 클라우드에 저장되지 않습니다.

1.2.11 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics

이 클라우드 서비스는 조직이 불만사항, 부정 혐의 및 기타 활동을 식별하고 집계하며 분류할 수 있도록 합니다. 높아지는 규제 기대를 충족하기 위해 새로운 문제점에 대한 통찰을 제공합니다. 이 도구는 고급 분석을 활용하여 기존 시스템에서 놓칠 수 있는 불만사항을 식별하고 분석합니다. 이 도구는 고객 데이터, 이메일, 서비스 메모, 소셜 미디어 불만사항, 음성 기록 등의 정형 및 비정형 데이터를 수집합니다. 그런 다음, 코그너티브 기능을 사용하여 시스템의 리스크를 식별하도록 불만사항 데이터를 집계하고 보강합니다. 또한 동적 분석 방식과 시계열 프로파일링을 적용하여 변동사항과 경향을 모니터링하고 예측합니다.

IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics 를 사용하기 위해서는 고객은 IBM Electronic Communication Surveillance Analytics on Cloud 또는 IBM Voice Surveillance Analytics on Cloud 중 하나에도 반드시 등록해야 합니다.

1.2.12 IBM Electronic Communication Surveillance Analytics on Cloud BYOL

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Electronic Communication Surveillance Analytics on Cloud 기능에 액세스할 수 있도록 합니다. 고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. IBM Electronic Communication Surveillance Analytics on Cloud BYOL 오퍼링에 필요한 IBM 프로그램은 IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication 입니다.

1.2.13 IBM Voice Surveillance Analytics on Cloud BYOL

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Voice Surveillance Analytics on Cloud 기능에 액세스할 수 있도록 합니다. 고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. IBM Voice Surveillance Analytics on Cloud BYOL 오퍼링에 필요한 IBM 프로그램은 IBM Financial Crimes Insight for Conduct Surveillance Software – Voice 입니다.

1.2.14 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL

이 클라우드 서비스는 고객이 클라우드 오퍼링으로 IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics 기능에 액세스할 수 있도록 해줍니다. 고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL 오퍼링에 필요한 IBM 프로그램은 IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics 입니다.

1.3 Acceleration 서비스

1.3.1 IBM Financial Crimes Insight Set-up

고객은 해당 클라우드 서비스를 사용하기 위해서 다음 설치(set-up) 서비스가 필요합니다.

- IBM Financial Crimes Insight for Anti-Money Laundering Set-up
- IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up
- IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up
- IBM Financial Crimes Insight for Entity Research – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research – Basic Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up
- IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up
- IBM Financial Crimes Insight for Entity Research Negative News API Set-up

- IBM Financial Crimes Insight for Entity Research Enrichment API Set-up
- IBM Financial Crimes Insight for Claims Fraud - Property and Casualty Set-up
- IBM Financial Crimes Insight for Claims Fraud - Investigation Set-up
- IBM Surveillance Insight for Financial Services on Cloud Set-up

2. 데이터 처리 및 보호 데이터 시트

IBM 데이터 처리 부칙(Data Processing Addendum: DPA)(http://ibm.com/dpa 참조) 및 아래 링크의 데이터 처리 및 보호 데이터 시트(Data Processing and Protection Data Sheet(s))(데이터 시트(들) 또는 DPA 별표(들)로 참조됨)는 클라우드 서비스에 대한 추가적인 데이터 보호 정보와 처리할 수 있는 컨텐츠의 유형, 관련 처리 활동, 데이터 보호 기능 및 컨텐츠의 보관 및 반환 정보와 관련한 옵션을 제공합니다. DPA 는 컨텐츠에 포함된 개인 데이터에 i) European General Data Protection Regulation (EU/2016/679)(GDPR) 또는 ii) http://www.ibm.com/dpa/dpl 에 명시된 기타 데이터 보호법이 적용되는 경우 그 범위에 한 해 적용됩니다.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

3. 서비스 레벨(Service Levels) 및 기술 지원

3.1 SLA(Service Level Agreement)

IBM 은 다음 가용성 "서비스 레벨 계약"(이하 SLA)을 고객에게 제공합니다. IBM 은 아래 표와 같이 누적 클라우드 서비스 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 가용률은 약정 월의 총 시간(분)에서 약정 월의 총 Service Down(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다. Service Down 의 정의, 클레임 절차, 서비스 가용성 문제에 관한 IBM 문의 방법은 IBM Cloud 서비스 지원 핸드북(https://www.ibm.com/software/support/saas_support_overview.html)에서 확인할 수 있습니다.

가용성	크레디트 (월별 사용등록료*의 %)
99.9% 미만	2%
99.0% 미만	5%
95.0% 미만	10%

* 사용등록료는 클레임 대상이 되는 해당 월의 약정 요금입니다.

3.2 기술 지원

지원 문의 상세 정보, 심각도 레벨, 가용성 지원 시간, 응답 시간 및 기타 지원 정보와 절차를 포함하여, 클라우드 서비스에 대한 기술 지원은 IBM 지원 안내서(https://www.ibm.com/support/home/pages/support-guide/ 참조)에서 클라우드 서비스를 선택하면 확인할 수 있습니다.

4. 요금

4.1 청구 체계

클라우드 서비스에 대한 과금 체계는 거래서류에 명시됩니다.

이 클라우드 서비스에는 다음 청구 체계가 적용됩니다.

- 인게이지먼트(Engagement)는 클라우드 서비스들과 관련된 전문 서비스 또는 교육 서비스입니다.
- 인스턴스(Instance)는 클라우드 서비스의 특정 구성에 대한 각 액세스입니다.

- 이벤트(Event)는 클라우드 서비스에서 처리하거나 클라우드 서비스 사용과 관련된 특정 이벤트의 발생을 의미합니다.
  - IBM Financial Crimes Insight for Anti-Money Laundering 의 경우, 하나의 이벤트(Event)는 월(one calendar month) 천만 건의 금융 거래입니다.
  - IBM Financial Crimes Insight for Claims Fraud – Property and Casualty and IBM Financial Crimes Insight for Claims – Investigation 의 경우, 하나의 이벤트(Event)는 한 건의 배상 청구(Claim)의 발생입니다. 배상 청구는 보상 대상인 손실이나 이벤트의 보상이나 적용 범위에 관해 조직에 대한 공식 요청과 관련된 일련의 지침입니다.
  - IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring 의 경우, 하나의 이벤트(Event)는 한 달(one calendar month) 동안 발신 시스템에서 클라우드 서비스로 유입된 개별 경보/이벤트입니다. 일반적으로 발신 소스 시스템은 트랜잭션 모니터링 시스템이나 케이스 관리 시스템입니다.
  - IBM Financial Crimes Insight for Alert Triage – Transaction List Screening 의 경우, 하나의 이벤트(Event)는 한 달(one calendar month) 동안 발신 시스템에서 클라우드 서비스로 유입된 최대 1,000 개의 개별 경보입니다. 일반적으로 발신 소스 시스템은 트랜잭션 모니터링 시스템이나 케이스 관리 시스템입니다.
  - IBM Financial Crimes Insight for Entity Research 및 IBM Financial Crimes Insight for Entity Research with Material Change 의 경우, 하나의 이벤트(Event)는 클라우드 서비스에서 동일 반복 검색을 포함하여, 한 달(one calendar month)에 처리된 상위 검사입니다. 상위 검사는 다른 검사의 하위로 연결되지 않는 레코드입니다. 하위는 (1.2.5 항에서 설명한 바와 같이) 달리 상위 검사의 대상이 아닌 관련 당사자입니다.
- 적격 참여자(Eligible Participant)는 클라우드 서비스에서 관리하거나 추적하는 서비스 제공 프로그램에 참여할 수 있는 개인이나 법인을 의미합니다.
- 항목(Item)은 클라우드 서비스에서 관리하거나 처리하거나 클라우드 서비스 사용과 관련된 특정 항목의 발생을 의미합니다.
  - IBM Voice Surveillance Analytics on Cloud 의 경우, 하나의 항목은 클라우드 서비스에서 달력상 하루에 처리한 한 시간의 음성 스트림입니다. 음성 스트림(Voice Stream)은 실시간 또는 녹음 형식의 오디오 통신의 캡처입니다.
- API 호출은 프로그래밍 가능 인터페이스를 통한 클라우드 서비스의 호출입니다.
- 엔티티 ID(Entity ID)는 클라우드 서비스 내에 식별된 엔티티의 고유한 ID 입니다.
- 디지털 메시지는 클라우드 서비스에서 관리하거나 처리하는 전자 통신문입니다.

5. 추가 조항

2019 년 1 월 1 일 이전에 작성된 클라우드 서비스 계약들(또는 동등한 기본 클라우드 계약들)에는 https://www.ibm.com/acs 에서 제공한 조건들이 적용됩니다.

5.1 지원 프로그램(Supporting Program)

IBM Financial Crimes Insight 및 IBM Financial Crimes Insight Non-Production 에는 클라우드 환경에 배치된 특정 프로그램("지원 프로그램")에 대한 액세스 권한이 포함됩니다. 고객은 사기, 금융 범죄 및 부적절한 대금지급을 파악하거나 및/또는 방지하도록 대응하거나 의도된 조치를 취하기 위한 목적으로만 이들 지원 프로그램을 사용할 수 있습니다.

5.1.1 사용 제한사항 – 특정 지원 프로그램에 한정

다음 지원 프로그램은 아래 제한사항에 따라 사용 가능합니다.

- IBM Watson Studio – 권한: 5 명의 동시 사용자(Concurrent User)
- IBM Watson Machine Learning – 권한: 50 개의 모델(Model)
- IBM Openscale – 권한: 50 개의 모델(Model)

- IBM SPSS Modeler Premium – 권한: 4 명의 승인된 사용자(Authorized User)
- IBM SPSS Statistics Standard – 권한: 4 명의 승인된 사용자(Authorized User)
- Watson Explorer Advanced Edition – 권한: 아래에 정의된 바대로 X 기가바이트당.

  고객은 다음을 분석할 수 있습니다.

  - Non-Analytics Collections 와 함께 사용할 목적으로 클라우드 서비스의 저장소에 저장된 모든 컨텐츠.
  - Non-Analytics Collections 와 함께 사용할 목적으로 클라우드 서비스의 저장소에 저장되지 않은 최대 10 기가바이트의 컨텐츠.
  - Analytics Collections 와 함께 사용할 목적으로 클라우드 서비스의 저장소에 저장된 100 기가바이트의 컨텐츠.

    Analytics Collections 는 Watson Explorer 어노테이션 관리 콘솔 또는 Watson Explorer Content Analytics 관리 콘솔에서 작성되거나 API 을 통해 "Content Analytics" 또는 "Analytics"로 작성된 컬렉션을 의미합니다.

    Non-Analytics Collections 에는 본 프로그램 클라우드 서비스에서 분석한 기타 모든 컨텐츠가 포함됩니다.
- IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer 권한: 2 명의 승인된 사용자(Authorized User)
- IBM Operational Decision Manager – 권한: 백만 월별 규칙 의사결정(1 million Monthly Rules Decisions) 및 천 월별 관리 의사결정 아티팩트(1 thousand Monthly Managed Decision Artifacts)

권한 정의

a. 동시 사용자(Concurrent User)는 임의의 특정 시점에 지원 프로그램에 액세스하는 개인입니다. 지원 프로그램에 동시에 여러 번 액세스하는지 여부에 관계 없이 해당 개인을 한 명의 동시 사용자로 계산합니다.

b. 모델(Model)은 지원 프로그램에서 시뮬레이션, 설명 및 예측에 사용되는 기본 데이터 또는 데이터 생성 프로세스와 관련된 수학적 모델 또는 알고리즘입니다.

c. 승인된 사용자(Authorized User)는 어떠한 방법, 어떠한 형태로든(예, 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 지원 프로그램에 액세스하도록 권한이 부여된 고유한 사용자를 의미합니다.

d. 기가바이트(GB)는 지원 프로그램에서 처리, 분석, 사용, 저장 또는 구성된 2 의 30 승 바이트입니다.

e. 월별 규칙 의사결정(Monthly Rules Decisions)은 매월(calendar month) 지원 프로그램에서 실행하거나 처리하는 규칙 실행 서버에서 규칙 세트를 호출한 결과입니다.

f. 월별 관리 의사결정 아티팩트(Monthly Managed Decision Artifacts)는 매월(calendar month) 지원 프로그램에서 관리하는 오브젝트입니다.

5.2 IBM Financial Crimes Insight BYOL 에 적용되는 조항

고객은 BYOL(bring your own licenses) 오퍼링을 사용하기 위해서는 아래 표의 연관 IBM 프로그램에 대해 적절한 라이센스 권한을 보유하고 있어야 합니다. BYOL SaaS 에 대한 고객의 권한은 아래 지정된 비율에 따라, 연관 IBM 프로그램에 대한 고객의 권한을 초과할 수 없습니다.

BYOL 오퍼링에는 연관 IBM 프로그램에 대한 Subscription and Support(S&S)가 포함되어 있지 않습니다. 고객은 고객이 연관 IBM 프로그램에 적용되는 (1)라이센스 권한과 (2)S&S 를 이미 확보했음을 보증합니다. 고객은 BYOL 오퍼링의 사용등록(subscription) 기간 동안, BYOL 오퍼링 권한과 관련하여 사용하는 IBM 프로그램 권한에 대해 최신 S&S 를 유지해야 합니다. 연관 IBM 프로그램을 사용할 수 있는 고객의 라이센스 또는 연관 IBM 프로그램에 대한 고객의 S&S 가 종료되면 BYOL 오퍼링의 사용 권한은 종료됩니다.

고객은 BYOL 오퍼링의 사용에 적용되는 관련 IBM 프로그램에 대한 권한을 계속 사용하여 다음 기간("동시 사용 기간") 동안 고객의 BYOL 오퍼링 사용과 동시에 관련 IBM 프로그램을 배포할 수 있습니다. BYOL 오퍼링에 처음 사용등록한 후 90 일 이내에 사용등록 기간이 3 년 미만인 고객의 경우; 고객이 BYOL 오퍼링에 처음 사용등록한 후 1 년 이내에 사용등록 기간이 3 년 이상인 고객의 경우. 동시 사용 기간이 종료된 후 고객이 BYOL 오퍼링을 사용하는 동안 BYOL 오퍼링 사용에 적용되는 관련 IBM 프로그램에 대한 고객의 권한이 일시 중단되고 고객은 관련 IBM 프로그램을 배치하기 위해 이러한 권한을 더 이상 이용할 수 없게 됩니다(명시된 여하한의 예외 적용).

아래 표에서는 설명된 권한에 의거해서 BYOL 오퍼링을 사용하기 위해 필요한 연관 IBM 프로그램의 권한 비율에 대해 간략하게 설명합니다. 고객은 일단 BYOL 오퍼링을 취득하였으면 BYOL 오퍼링 사용 기간 동안 BYOL 오퍼링의 사용에 적용되는 연관 IBM 프로그램의 권한은 일시 중단되며, 고객은 (명시된 예외사항에 근거하여) 연관 IBM 프로그램을 배포하기 위한 해당 권한을 더 이상 사용할 수 없습니다.

연관 IBM 프로그램	BYOL 오퍼링	n/m 비율*
IBM Cloud Pak for Data Financial Crimes Insight	IBM Financial Crimes Insight BYOL	비율: 1 설치 / 1 인스턴스
IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment	IBM Financial Crimes Insight Non-Production BYOL	비율: 1 설치 / 1 인스턴스
IBM Financial Crimes Insight for Conduct Surveillance Software - Electronic Communication	IBM Electronic Communication Surveillance Analytics on Cloud BYOL	누적 비율: 등급 1(1-100 RVU): ● 1 RVU / 1 적격 참여자 등급 2(101-235 RVU): ● 0.9 RVU / 1 적격 참여자 등급 3(236-435 RVU): ● 0.8 RVU / 1 적격 참여자 등급 4(436-585 RVU): ● 0.6 RVU / 1 적격 참여자 등급 5(586-835 RVU): ● 0.5 RVU / 1 적격 참여자 등급 6(836-1,135 RVU): ● 0.4 RVU / 1 적격 참여자 등급 7(1,136+ RVU): ● 0.3 RVU / 1 적격 참여자
IBM Financial Crimes Insight for Conduct Surveillance Software - Voice	IBM Voice Surveillance Analytics on Cloud BYOL	누적 비율: 등급 1(1-100 RVU): ● 1 RVU / 1 항목 등급 2(101-235 RVU): ● 0.9 RVU / 1 항목 등급 3(236-435 RVU): ● 0.8 RVU / 1 항목 등급 4(436-585 RVU): ● 0.6 RVU / 1 항목 등급 5(586-835 RVU): ● 0.5 RVU / 1 항목 등급 6(836-1,135 RVU): ● 0.4 RVU / 1 항목 등급 7(1,136+ RVU): ● 0.3 RVU / 1 항목

연관 IBM 프로그램	BYOL 오퍼링	n/m 비율*
IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics	IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics BYOL	누적 비율: 등급 1(1-100 RVU): ● 5,000 RVU / 1 디지털 메시지 등급 2(101-235 RVU): ● 4,500 RVU / 1 디지털 메시지 등급 3(236-435 RVU): ● 4,000 RVU / 1 디지털 메시지 등급 4(436-585 RVU): ● 3,000 RVU / 1 디지털 메시지 등급 5(586-835 RVU): ● 2,500 RVU / 1 디지털 메시지 등급 6(836-1,135 RVU): ● 2,000 RVU / 1 디지털 메시지 등급 7(1,136+ RVU): ● 1,500 RVU / 1 디지털 메시지

* "n/m 비율"이란 표시된 연관 IBM 프로그램 체계의 매 ('n')개 권한을 표시된 BYOL 오퍼링 체계의 지정된 ('m')개 권한에 적용할 수 있음을 의미합니다. 연관 IBM 프로그램에서 BYOL 오퍼링으로 변환한 결과가 정수가 아닌 경우, 가장 근접한 정수로 반올림하십시오.

예제 1:

710 RVU 대 적격 참여자(EPS)

(IBM Trade Surveillance Analytics 및 IBM Electronic Communication Surveillance Analytics 에 적용 가능)

등급 1: 710>100 이면 100/1 = 100 EPS

등급 2: 710>235 이면 (235-100)/.9 = +150 EPS

등급 3: 710>435 이면 (435-235)/.8 = +250 EPS

등급 4: 710>585 이면 (585-435)/.6 = +250 EPS

등급 5: 710>835 이 아니면 (710-585)/.5 = +250 EPS

총 EPS: 100 + 150 + 250 + 250 + 250 = 1000 EPS

예제 2:

500,000 RVU 대 디지털 메시지(5,000 팩)

(IBM Financial Crimes Insight for Conduct Surveillance – Complaint Analytics 에 적용 가능)

등급 1: 500,000>100 이면 100/5,000 = .02 디지털 메시지

등급 2: 500,000>235 이면 (235-100)/4,500 = + .03 디지털 메시지

등급 3: 500,000>435 이면→ (435-235)/4,000 = + .05 디지털 메시지

등급 4: 500,000>585 이면→ (585-435)/3,000 = + .05 디지털 메시지

등급 5: 500,000>835 이면→ (835-585)/2,500 = + .1 디지털 메시지

등급 6: 500,000>1,135 이면→ (1,135-835)/2,000 = + .15 디지털 메시지

등급 7, 500,000>1,135 이면→ (500,000-1135)/1,500 = + 99.6 디지털 메시지

총 디지털 메시지: .02 + .03 + .05 + .1 + .15 + 99.6 = 100 디지털 메시지

5.3 검색 결과

고객은 본 명세서에 기술된 클라우드 서비스의 일부로 생성된 보고서를 통해 확보되고 참조된 검색 결과에는 제 3 자가 소유한 데이터나 컨텐츠가 포함될 수 있으며 IBM 은 그러한 검색 결과나 컨텐츠에

대한 여하한 라이센스 또는 기타 권리를 판매하거나 제공하지 않는다는 점을 인정합니다. 검색 결과는 이러한 클라우드 서비스에 대한 컨텐츠로 간주됩니다.

5.4 클라우드 서비스 만기

클라우드 서비스가 만료되거나 종료되기 전에 고객은 제공된 클라우드 서비스의 보고 또는 반출 기능을 사용하여 데이터를 추출할 수 있습니다. 사용자 정의 데이터 추출 서비스는 별도의 계약에 의거하여 제공될 수 있습니다.

클라우드 서비스 만료일 또는 종료일 이후 30 일 이내에 고객의 지원 요청을 수신한 경우 IBM 은 기본 애플리케이션 형식의 고객 컨텐츠의 전자적 사본을 고객에게 반환합니다.