IBM Cloud Identity

Diese Servicebeschreibung beschreibt den Cloud-Service. Die anwendbaren Auftragsdokumente enthalten Preisangaben und weitere Einzelheiten zur Bestellung des Kunden.

1. Cloud-Service

IBM Cloud Identity bietet Single Sign-On (SSO), Mehrfaktorauthentifizierung und Steuerungsmöglichkeiten für den Identitätslebenszyklus sowohl für interne Benutzertypen (Mitarbeiter) als auch externe Benutzertypen.

1.1 Angebote

Der Kunde kann aus den folgenden Angeboten wählen, die alle über eine Ereigniskapazität von 400 Ereignissen pro Sekunde verfügen.

1.1.1 IBM Cloud Identity Connect

Dieser Cloud-Service bietet Single Sign-On (SSO) und Open ID Connect (OIDC), Authentication-as-a-Service für cloudbasierte API-Autorisierung, ein Application Launchpad, Berichterstellung durch den Administrator und ein Analysedashboard. Er verbindet Benutzer mit Anwendungen über moderne, auf Standards basierenden Authentifizierungs- und Federation-Protokolle und verfügt über Hunderte von Konnektoren für den Zugriff auf allgemeine Anwendungen. Dieser Cloud-Service lässt sich nahtlos mit dem On-Premises-Softwareprogramm IBM Security Access Management (ISAM) integrieren, das als Aktivierungssoftware zum Lieferumfang gehört, um den Kunden eine Lösung bereitzustellen, die die Forderungen ihrer Geschäftsbereiche nach einem Zugriffsmanagement unterstützt, das sowohl ihre On-Premises- als auch ihre Cloudanwendungen einbezieht.

1.1.2 IBM Cloud Identity Connect for ISAM

Dieser Cloud-Service lässt sich nahtlos mit dem On-Premises-Softwareprogramm IBM Security Access Management (ISAM) integrieren, um den Kunden eine Lösung bereitzustellen, die die Forderungen ihrer Geschäftsbereiche nach einem Zugriffsmanagement unterstützt, das sowohl ihre On-Premises- als auch ihre Cloudanwendungen einbezieht. Für diesen Cloud-Service muss der Kunde über eine aktive Berechtigung für Software-Subscription und -Support (S&S) für das Programm IBM Security Access Management (ISAM) verfügen und S&S muss für die Dauer seiner Cloud-Service-Subscription aufrechterhalten. Die Berechtigung des Kunden für diesen Cloud-Service muss der ISAM-Lizenzberechtigung des Kunden für seine On-Premises-Anwendungen entsprechen. Die Kündigung von S&S durch den Kunden hat auch die Einstellung dieses Cloud-Service zur Folge. Der in Abschnitt 5.2 beschriebene Zugriff auf die Aktivierungssoftware ist bei diesem Cloud-Service nicht eingeschlossen.

1.1.3 IBM Cloud Identity Essentials

Dieser Cloud-Service stellt den Kunden Single-Sign-on-Funktionen (SSO) für die verschiedenen von ihnen genutzten IBM und öffentlichen Cloudanwendungen zur Verfügung. In Verbindung mit IBM MaaS360 bietet dieser Cloud-Service zusätzliche Sicherheitsstufen, indem der Zugriff beispielsweise an Bedingungen geknüpft wird.

1.1.4 IBM Cloud Identity Verify

Dieser Cloud-Service bietet Mehrfaktorauthentifizierung für Anwendungen, die von Cloud Identity Connect oder über direkten API-Aufruf geschützt werden, und für weitere Durchsetzungspunkte, einschließlich RADIUS-Clients, Unix/Linux PAM-Server und Windows-Server, um deren Identitäten beim Zugriff auf einen digitalen Service zu überprüfen. Dazu gehören Verfahren wie E-Mail, SMS und zeitbasierte (Software-Token) Einmalkennwörter sowie Push-basierte mobile biometrische Authentifizierung, die von IBM Verify unterstützt werden. Dieser Cloud-Service lässt sich mit dem On-Premises-Softwareprogramm IBM Security Access Management (ISAM) integrieren, um den Kunden eine Lösung bereitzustellen, die die Forderungen ihrer Geschäftsbereiche nach einem Zugriffsmanagement unterstützt, das sowohl ihre On-Premises- als auch ihre Cloudanwendungen einbezieht. Er ist als Standalone-Version oder als Ergänzung zu Cloud Identity Connect, Cloud Identity Connect for ISAM und Cloud Identity Essentials verfügbar.

1.1.5 IBM Cloud Identity Govern

Dieser Cloud-Service lässt sich nahtlos mit dem On-Premises-Softwareprogramm IBM Governance and Intelligence (IGI) integrieren, das als Aktivierungssoftware zum Lieferumfang gehört, um den Kunden eine Lösung bereitzustellen, die die Forderungen ihrer Geschäftsbereiche nach einem Zugriffsmanagement unterstützt, das sowohl ihre On-Premises- als auch ihre Cloudanwendungen einbezieht. Dieser Cloud-Service bietet Unternehmen umfassende Funktionen für Identitätslebenszyklusmanagement in der Cloud und schließt einen Zugriffsanforderungsworkflow für Anwendungen ein.

1.1.6 IBM Cloud Identity Connect and Verify

Dieser Cloud-Service bietet dem Kunden die Funktionalität von IBM Cloud Identity Connect und IBM Cloud Identity Verify in einem einzigen Angebot.

1.1.7 IBM Cloud Identity Analyze

Dieser Cloud-Service erweitert vorhandene IBM Lösungen, wie z. B. IBM Security Identity Governance and Intelligence (IGI) und IBM Security Identity Manager (ISIM), indem ein ganzheitliches Risikoprofil für verwaltete Benutzer bereitgestellt wird. Bestandteil dieses Cloud-Service ist eine vielseitig einsetzbare On-Premises-Analyseengine, die Aktivitäts- und Berechtigungsdaten aus einer Reihe von Quellen verarbeitet, die eine 360-Grad-Ansicht der Zugriffsrisiken mit der Möglichkeit zur Ergreifung von Maßnahmen auf der Basis dieser Risikoerkenntnisse bereitstellen.

1.1.8 IBM Cloud Identity Adaptive Access

Dieser Cloud-Service verwendet von künstlicher Intelligenz (KI) getriebene kontextbezogene Erkenntnisse über Benutzer, deren Geräte und Verhaltensmuster, um Unternehmen bei der Durchsetzung korrekter Authentifizierungsrichtlinien zu helfen.

1.1.9 IBM Cloud Identity Connect Verify and Govern

Dieser Cloud-Service bietet dem Kunden die Funktionalität von IBM Cloud Identity Connect, IBM Cloud Identity Verify und IBM Cloud Identity Govern in einem einzigen Angebot.

1.2 Optionale Services

1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud ist eine separate Instanz der IBM Cloud Identity-Plattform, die vom Kunden nur für interne nicht produktionsbezogene Aktivitäten eingesetzt werden darf, wie beispielsweise Tests, Leistungsoptimierung, Fehlerdiagnose, internes Benchmarking, Staging, Qualitätssicherung und/oder Entwicklung intern verwendbarer Zusätze oder Erweiterungen für den Cloud-Service über veröffentlichte Anwendungsprogrammierschnittstellen. Bei diesem Cloud-Service besteht die Möglichkeit, ein Verfügbarkeits-Service-Level-Agreement (SLA) einzuschließen, das den Bedingungen in Abschnitt 3 „Service-Levels und technische Unterstützung“ unterliegt. Dieser Cloud-Service hat eine Kapazität von 100 Ereignissen pro Sekunde.

1.2.2 IBM Cloud Identity Vanity Domain

Eine Vanity Domain (eine einzelne Domäne) ermöglicht dem Kunden die Nutzung einer Domäne, die seinem Unternehmen gehört und für sein Unternehmen wichtiger ist als die Standardtenantdomäne, die von der Plattform „out of the box“ bereitgestellt wird. Für diese Domäne wird von IBM ein SSL-Zertifikat aufrechterhalten und jährlich verlängert.

1.2.3 IBM Cloud Identity Application Gateway Hosted

Das Application Gateway bietet eine von IBM verwaltete und gehostete einfache Appliance für Kunden, die auf der Suche nach einem Service sind, der vom Standard abweichende oder ältere Authentifizierungsverfahren unterstützt. Zu diesen Verfahren gehören LTPA- und HTTP-Header-basierte Authentifizierung. Die fortlaufende Überwachung und Wartung wird von IBM durchgeführt.

1.3 Acceleration Services

1.3.1 IBM Cloud Identity Connect Solution Planning

Dieser Service bietet Professional Services im Umfang von einer (1) Woche, in der IBM einige oder alle der folgenden Maßnahmen durchführen wird:

- Einrichten von Single Sign-on (einmalige Anmeldung) für cloudbasierte SaaS-Anwendungen

- Konfigurieren eines Launchpads für die einfache Suche nach Anwendungen
- Verbindung zu Anwendungen mit vordefinierten Konnektoren
- Lösungsplanung, Architektur und Anleitung
- Von IBM empfohlene Vorgehensweise und Verfahren

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Dieser Service bietet einen dreitägigen Professional-Services-Workshop, der sich auf die Herausforderungen der Mehrfaktorauthentifizierung und den Schutz von Kundenanwendungen mit IBM Cloud Identity Verify konzentriert. Im Workshop werden einige oder alle der folgenden Themen abgedeckt:

- Einbetten der gewohnten Authentifizierung in alle digitalen und persönlichen Interaktionen, bei denen eine Authentifizierung erforderlich ist
- Erzwingen einer strikten Authentifizierung in einer Anwendung über eine entwicklerfreundliche REST-API
- Bereitstellen branchenüblicher Best-Practices-Empfehlungen für Identitätssicherheit
- Optimiertes Benutzererlebnis bei allen Gerätetypen wie Telefonen, Tablets und Laptops

1.3.3 IBM Cloud Security Strategy and Planning

Dieser Service bietet einen dreiwöchigen Professional-Services-Workshop zur Anwendung von Best Practices für Cloudsicherheit, wobei der Schwerpunkt auf der Infrastruktur- und Anwendungssicherheit liegt. Im Workshop werden einige oder alle der folgenden Themen abgedeckt:

- Einrichten von Single Sign-on (einmalige Anmeldung) für cloudbasierte SaaS-Anwendungen
- Konfigurieren eines Launchpads für die einfache Suche nach Anwendungen
- Verbindung zu Anwendungen mit vordefinierten Konnektoren
- Lösungsplanung, Architektur und Anleitung
- Erkenntnisse über neue Trends bei der Cybersicherheit
- Von IBM empfohlene Vorgehensweise und Verfahren

1.3.4 IBM Cloud Identity Expert On Demand

Dieser Service bietet Professional Services im Umfang von zwanzig (20) Stunden, die nach Servicebeginn in zweistündigen Sitzungen über einen Zeitraum von dreißig (30) Tagen erbracht werden. Im Rahmen der Services wird ein Cloud-Identity-Architekt Fragen beantworten sowie Anleitungen und Empfehlungen unter anderem zu folgenden Themen geben:

- Erforderliche fachliche Qualifikationen für die Erweiterung der Cloud Identity-Lösungsimplementierung des Kunden
- Beantwortung von Fragen zur Architektur und Implementierung der Cloud Identity-Lösung des Kunden
- Empfehlungen zur Cloud Identity-Lösung und/oder -Strategie des Kunden

2. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung von IBM unter http://ibm.com/dpa (EB-AV) und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheets, nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Datenschutzinformationen für die Cloud-Services und deren Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungstätigkeiten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Die EB-AV finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) oder ii) eines der unter http://ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

3. Service-Levels und technische Unterstützung

3.1 Service-Level-Agreement

IBM stellt dem Kunden das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) bereit. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service anwenden (siehe die nachstehende Tabelle). Der Prozentsatz der Verfügbarkeit wird berechnet als Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Serviceausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die Definition von Serviceausfall, der Prozess zur Bearbeitung von Ansprüchen und die Kontaktaufnahme mit IBM bei Problemen mit der Serviceverfügbarkeit sind in der Übersicht zu IBM SaaS-Support unter https://www.ibm.com/software/support/saas_support_overview.html enthalten.

Verfügbarkeit	Gutschrift (in Prozent (%) der monatlichen Subscription-Gebühr*)
Unter 99,9 %	10 %

* Die Subscription-Gebühr ist der vertraglich vereinbarte Preis für den Monat, der Gegenstand des Anspruchs ist.

3.1.1 Weitere Informationen zu diesem SLA

Während der ersten sechzig (60) Tage der Laufzeit („Burn-in-Periode“) hat der Kunde keinen Anspruch auf eine Gutschrift, wenn die IBM Cloud Identity-Umgebung die Verfügbarkeitszeit von mindestens 99,9 % unter dieser Vereinbarung nicht erreicht. Sollte IBM vor oder während der Burn-in-Periode feststellen, dass vorhandene Konfigurationen, Richtlinien, Daten oder Code des Kunden (nachfolgend „Bereits vorhandene Komponenten“ genannt), die auf den IBM Cloud Identity Service migriert werden sollen, verhindern würden, dass der in dieser Vereinbarung festgelegte Prozentsatz für die Verfügbarkeitszeit erfolgreich erreicht wird, behält IBM sich das Recht vor, den Kunden davon in Kenntnis zu setzen und die betroffenen bereits vorhandenen Komponenten nach alleinigem Ermessen von den Bestimmungen des SLA auszuschließen. Falls IBM dem Kunden den Ausschluss bereits vorhandener Komponenten ankündigt, ist IBM dafür verantwortlich, dem Kunden einen Maßnahmenplan zu unterbreiten (sofern möglich), der aufzeigt, wie die ausgeschlossenen Komponenten den in dieser Vereinbarung festgelegten Prozentsatz für die Verfügbarkeitszeit erreichen können. Der Kunde trägt allein die Kosten dieser Maßnahmen, außer wenn beide Vertragsparteien eine abweichende Vereinbarung getroffen haben.

3.2 Technische Unterstützung

Eine Beschreibung der technischen Unterstützung für den Cloud-Service, einschließlich Support-Kontaktinformationen, Fehlerklassen, Unterstützungszeiten, Reaktionszeiten und sonstiger Unterstützungsinformationen und -prozesse, finden Sie durch Auswahl des Cloud-Service im IBM Support Guide, der unter https://www.ibm.com/support/home/pages/support-guide/ verfügbar ist.

4. Gebühren

4.1 Gebührenmetriken

Die Gebührenmetriken für den Cloud-Service sind im Auftragsdokument angegeben.

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Berechtigter Benutzer“ ist ein bestimmter Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, ein Gerät oder einen Anwendungsserver) Zugriff auf die Cloud-Services erteilt wird.
- „Mitarbeiter“ ist eine bestimmte Person, die im Unternehmen des Kunden angestellt ist oder anderweitig vom Unternehmen des Kunden bezahlt wird oder in dessen Auftrag handelt, unabhängig davon, ob dieser Person Zugriff auf den Cloud-Service erteilt wird.
- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „Instanz“ ist jeder Zugriff auf eine bestimmte Konfiguration der Cloud-Services.
- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit den Cloud-Services.

- „Ereignis“ ist das Auftreten eines bestimmten Vorkommnisses, das von den Cloud-Services verarbeitet wird oder mit der Nutzung der Cloud-Services in Zusammenhang steht.
  - Bei Cloud Identity Connect ist ein Ereignis eine HTTP-Anforderung an den Cloud-Service.
  - Bei Cloud Identity Verify ist ein Ereignis eine Mehrfaktormethode, die über den Cloud-Service aufgerufen wird.

5. Zusätzliche Bedingungen

Für Vereinbarungen für Cloud-Services (oder vergleichbare Cloud-Basisvereinbarungen), die vor dem 1. Januar 2019 unterzeichnet wurden, finden die Bedingungen unter https://www.ibm.com/acs Anwendung.

5.1 Kundenreferenz

Der Kunde erklärt sich damit einverstanden, dass IBM in Werbe- oder Marketingmaterial öffentlich auf den Kunden als Subskribenten der Cloud-Services verweisen darf.

5.2 Aktivierungssoftware

Der Cloud-Service enthält die folgende Aktivierungssoftware:

Die folgende Aktivierungssoftware darf nur in Verbindung mit den Cloud-Services IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify und IBM Cloud Identity Connect Verify and Govern verwendet werden:

- IBM Security Access Manager Virtual Enterprise Edition

Die folgende Aktivierungssoftware darf nur in Verbindung mit den Cloud-Services IBM Cloud Identity Govern und IBM Cloud Identity Connect Verify and Govern verwendet werden:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

Die folgende Aktivierungssoftware darf nur in Verbindung mit dem IBM Cloud Identity Analyze Service verwendet werden:

- IBM Cloud Identity Analyze On-Premises-Analyseengine

5.3 Prüfung

Der Kunde wird i) Aufzeichnungen und Ausgaben von Systemtools aufbewahren und auf Anforderung bereitstellen, soweit dies für IBM und ihre beauftragten externen Prüfer erforderlich ist, um die Einhaltung der Vereinbarung durch den Kunden zu überprüfen, und ii) unverzüglich alle erforderlichen Berechtigungen bestellen und zu den zum jeweiligen Zeitpunkt gültigen Preisen von IBM bezahlen und andere Verbindlichkeiten, die sich aufgrund der Prüfung ergeben und in einer Rechnung von IBM angegeben sind, begleichen. Die Verpflichtungen im Rahmen dieses Abschnitts bleiben während der Laufzeit des Cloud-Service und eines Zeitraums von zwei Jahren danach in Kraft.