IBM Cloud Identity

Nella presente Descrizione dei Servizi viene descritto il Servizio Cloud. I documenti d'ordine applicabili riportano prezzi e dettagli aggiuntivi sull'ordine del cliente.

1. Servizio in Cloud

IBM Cloud Identity fornisce Single Sign-On (SSO), autenticazione a più fattori e identificazione dei controlli del ciclo di vita per i dipendenti interni e per gli utenti esterni.

1.1 Offerte

Il Cliente potrà scegliere tra le seguenti offerte disponibili, tutte con una capacità di 400 eventi al secondo.

1.1.1 IBM Cloud Identity Connect

Questo Servizio Cloud offre Single Sign-On (SSO) tramite ISAM e Open ID Connect (OIDC), Authentication as a Service per l'autorizzazione API basata su cloud, un launchpad dell'applicazione, report dell'amministratore e un dashboard di analisi. Questo Servizio Cloud collega gli utenti alle applicazioni utilizzando protocolli di autenticazione e federazione basati su standard moderni, tra cui centinaia di connettori ad applicazioni comuni. Questo Servizio Cloud si integra con il software IBM Security Access Management (ISAM) in sede incluso come prerequisito software, per fornire ai Clienti una soluzione che supporti le richieste delle relative linee di business per la gestione accessi, incluse sia le applicazioni in sede che su Cloud.

1.1.2 IBM Cloud Identity Connect for ISAM

Questo Servizio Cloud si integra con il software IBM Security Access Management (ISAM) in sede per fornire ai Clienti una soluzione che supporti le richieste delle relative linee di business per la gestione accessi, incluse sia le applicazioni in sede che su Cloud. Questo Servizio Cloud richiede che il Cliente disponga una titolarità attiva di Software Subscription and Support (S&S) del programma IBM Security Access Management (ISAM) e S&S deve restare attivo per la durata dell'abbonamento del Cliente al Servizio Cloud. La titolarità del Cliente a questo Servizio Cloud deve essere equivalente alla titolarità della licenza ISAM locale del Cliente. La cessazione di S&S del Cliente interromperà anche questo Servizio Cloud. L'accesso ai prerequisiti software definiti nell'Articolo 5.2 non è incluso in questo Servizio Cloud.

1.1.3 IBM Cloud Identity Essentials

Questo Servizio Cloud fornisce al Cliente le funzionalità di Single Sign-On (SSO) per le diverse applicazioni IBM e di cloud pubblico che il Cliente utilizza. Questo Servizio Cloud può essere abbinato a MaaS360 di IBM per fornire ulteriori livelli di controllo della sicurezza come, ad esempio, l'accesso condizionale.

1.1.4 IBM Cloud Identity Verify

Questo Servizio Cloud fornisce l'autenticazione a più fattori per le applicazioni protette da Cloud Identity Connect o tramite richiamo diretto dell'API e, per altri punti di applicazione, tra cui client RADIUS, dei server Unix/Linux PAM e Windows, per la verifica delle identità al momento dell'accesso ad un servizio digitale. Ciò include meccanismi quali e-mail, SMS e password monouso basate sul tempo (token software) e autenticazione biometrica mobile basata su push fornita tramite IBM Verify. Questo Servizio Cloud si integra con il software 8IBM Security Access Management (ISAM) in sede per fornire ai Clienti una soluzione che supporti le richieste delle relative linee di business per la gestione accessi, incluse sia le applicazioni in sede che su Cloud. È disponibile nella versione standalone, o in combinazione con Cloud Identity Connect, Cloud Identity Connect for ISAM e Cloud Identity Essentials.

1.1.5 IBM Cloud Identity Govern

Questo Servizio Cloud si integra con il software IBM Governance and Intelligence (IGI) in sede incluso come prerequisito software, per fornire ai Clienti una soluzione che supporti le richieste delle relative linee di business per la gestione accessi, incluse sia le applicazioni in sede che su Cloud. Questo Servizio Cloud fornisce alle organizzazioni funzionalità avanzate di gestione del ciclo di vita di identità all'interno del cloud ed include il flusso di lavoro della richiesta di accesso all'applicazione.

1.1.6 IBM Cloud Identity Connect e Verify

Questo Servizio Cloud fornisce al Cliente le funzionalità di IBM Cloud Identity Connect e IBM Cloud Identity Verify in un'unica offerta.

1.1.7 IBM Cloud Identity Connect Verify e Govern

Questo Servizio Cloud fornisce al Cliente le funzionalità di IBM Cloud Identity Connect, IBM Cloud Identity Verify e IBM Cloud Identity Govern in un'unica offerta.

1.2 Servizi Opzionali

1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud è un'istanza separata della piattaforma IBM Cloud Identity che il Cliente può utilizzare solo come parte delle attività di non produzione del Cliente, incluse, a titolo esemplificativo ma non esaustivo, attività di test, ottimizzazione delle prestazioni, diagnosi dell'errore, verifica delle prestazioni interne, stage sulle attività di 'quality assurance' e/o sviluppo interno di implementazioni addizionali o estensioni del Servizio Cloud, utilizzando le API pubblicate. Questo Servizio Cloud ha la possibilità di includere un contratto un Service Level Agreement ("SLA"), soggetto ai termini indicati nell'Articolo 3 Livelli di Servizio e Supporto Tecnico. Per questo Servizio Cloud ha una capacità di 100 Eventi al secondo.

1.2.2 IBM Cloud Identity Vanity Domain

Un vanity domain (un dominio) consente al Cliente di utilizzare un dominio di proprietà e più pertinente per la propria organizzazione, anziché utilizzare il dominio tenant predefinito fornito dalla piattaforma. Per questo dominio IBM gestirà un certificato SSL che verrà rinnovato su base annuale.

1.3 Servizi di accelerazione

1.3.1 IBM Cloud Identity Connect Solution Planning

Questo Servizio fornisce 1(una) settimana di servizi professionali durante le quali IBM eseguirà alcune o tutte le seguenti attività:

- Impostare il single sign-on per le applicazioni SaaS basate su cloud
- Configurare un launch pad per semplificare l'individuazione delle applicazioni
- Connettere le applicazioni con i connettori "ready-made"
- Pianificazione, architettura e guida per la soluzione
- Approccio e pratiche consigliate da IBM

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Questo servizio offre un workshop di tre (3) giorni di servizi professionali, incentrato su sfide di autenticazione multi-fattore e sulla protezione delle applicazioni del Cliente utilizzando IBM Cloud Identify Verify. Il workshop riguarderà alcuni o tutti i seguenti aspetti:

- Incorporazione dell'autenticazione familiare in tutte le interazioni digitali e tra persone in cui è richiesta l'autenticazione
- Abilitare un'applicazione per applicare un'autenticazione solida utilizzando l'API REST comune per gli sviluppatori
- Fornire suggerimenti sulle migliori pratiche del settore sulla sicurezza delle identità
- Semplificazione dell'esperienza utente e adozione di tutti i fattori dei formati: telefoni, tablet e laptop

1.3.3 IBM Cloud Security Strategy and Planning

Questo servizio fornisce tre (3) settimane di workshop sui servizi professionali incentrati sull'applicazione delle best practice sulla sicurezza del Cloud, con particolare attenzione all'infrastruttura ed alla sicurezza delle applicazioni. Il workshop riguarderà alcuni o tutti i seguenti aspetti:

- Impostare il single sign-on per le applicazioni SaaS basate su cloud
- Configurare un launch pad per semplificare l'individuazione delle applicazioni
- Connettere le applicazioni con i connettori "ready-made"
- Pianificazione, architettura e guida per la soluzione
- Analisi approfondite delle tendenze emergenti nella cyber security
- Approccio e pratiche consigliate da IBM

1.3.4 IBM Cloud Identity Expert On Demand

Questo servizio offre venti (20) ore di servizi professionali, erogati in due (2) sessioni di un'ora entro trenta (30) giorni dall'inizio. I servizi forniranno un architetto Cloud Identity che possa rispondere alle domande e fornire indicazioni e suggerimenti su, ma non limitatamente a:

- Competenze tecniche per favorire l'implementazione della soluzione Cloud Identity del Cliente
- Domande sull'architettura e sull'implementazione sulla soluzione Cloud Identity di un Cliente
- Guida sulla soluzione Cloud Identity e/o la strategia di un Cliente

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web http://ibm.com/dpa e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applichino i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina http://www.ibm.com/dpa/dpl.

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

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità, viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nella panoramica sul supporto SaaS di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.1.1 Ulteriori informazioni su questo SLA

Durante i primi sessanta (60) giorni della durata contrattuale del Cliente ("Periodo Burn-In"), il Cliente non avrà diritto ad alcun credito per il mancato raggiungimento da parte dell'ambiente IBM Cloud Identity della Percentuale di Attività minima del 99,9% in base al presente Accordo. Se prima di o durante il Periodo Burn-In, IBM identifica le configurazioni, le policy, i dati o il codice esistenti del Cliente ("Componenti Pre-Esistenti") destinati ad essere migrati nel Servizio IBM Cloud Identity, che impedirebbe al Servizio IBM Cloud Identity di raggiungere correttamente la Percentuale di Attività all'interno dell'Accordo, IBM si riserva il diritto di comunicare al Cliente di tali Componenti Pre-Esistenti e li esonera, ad esclusiva discrezione di IBM, dalle disposizioni dello SLA. Se IBM comunica al Cliente di eventuali Componenti Preesistenti esonerati, IBM sarà responsabile di presentare al Cliente un piano di rimedio, per quanto possibile, che consenta a tali componenti esonerati di soddisfare la Percentuale di Attività di tale Accordo. Il Cliente sarà l'unico responsabile per il costo di tale rimedio salvo diversamente concordato da entrambe le parti.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina https://www.ibm.com/support/home/pages/support-guide/.

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Un Utente Autorizzato è una persona specifica cui è stato fornito l'accesso ai Servizi Cloud in qualsiasi modo, direttamente o indirettamente (ad esempio, tramite un programma multiplexing, dispositivo o server applicativo) con qualsiasi mezzo.
- Un Dipendente è una singola persona impiegata o altrimenti retribuita o che agisce per conto dell'azienda del Cliente, con o senza l'accesso ai Servizi Cloud.
- Si definisce Partecipante Eleggibile, qualsiasi persona fisica o giuridica idonea a partecipare a qualsiasi programma di erogazione del servizio, gestito o tracciato mediante i Servizi Cloud.
- Per Istanza si intende ogni accesso ad una configurazione specifica dei Servizi Cloud.
- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.
- Un Evento rappresenta il verificarsi di un evento specifico che viene elaborato o relativo all'utilizzo dei Servizi Cloud.
    - Per Cloud Identity Connect, un Evento è una richiesta http al Servizio Cloud.
    - Per Cloud Identity Verify, un Evento è un qualsiasi metodo multi-fattore richiamato tramite il Servizio Cloud.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web https://www.ibm.com/acs.

5.1 Referenza Cliente

Il Cliente accetta che IBM possa fare pubblicamente riferimento al Cliente come abbonato dei Servizi Cloud in una pubblicità o comunicato commerciale.

5.2 Prerequisiti Software (Software di Abilitazione)

Il Servizio Cloud contiene il seguente Software di Abilitazione:

Il seguente software di abilitazione può essere utilizzato solo con i Servizi Cloud IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify e IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

Il seguente software di abilitazione può essere utilizzato solo con i Servizi Cloud IBM Cloud Identity Govern e IBM Cloud Identity Connect Verify and Govern:

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

5.3 MaxMind

Questo Servizio Cloud include dati GeoLite2 creati da MaxMind, disponibili in http://www.maxmind.com. GeoLite2 fornisce la geolocalizzazione degli IP per consentire di localizzare la posizione geografica di un computer attraverso l'identificazione dell'indirizzo IP.

5.4 Verifica

Il Cliente provvederà a i) mantenere e fornire su richiesta le registrazioni e l'output degli strumenti di sistema, come ragionevolmente richiesto da IBM e dai suoi revisori esterni, per verificare la conformità

del Cliente alle condizioni del presente Accordo, e ii) richiedere tempestivamente a IBM, tramite un nuovo ordine, gli eventuali ulteriori diritti di utilizzo, pagare i corrispettivi aggiuntivi in base alle tariffe applicate da IBM al momento, assumendosi tutte le responsabilità determinate in seguito a tali controlli, come specificato da IBM nella fattura. Questi obblighi di verifica della conformità restano validi per la durata del Servizio Cloud e per i due anni successivi.

Accettato da:

_____

Firma e timbro del Cliente

Data: .....

Ai sensi degli artt. 1341 e 1342 del Codice Civile Italiano, il Cliente accetta espressamente i seguenti articoli del presente documento: "Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement (SLA)", "Ulteriori informazioni su questo SLA".

Accettato da:

_____

Firma e timbro del Cliente

Data: .....