

„IBM Cloud Identity“

Šiame paslaugos apraše aprašoma „Cloud Service“. Taikomuose užsakymo dokumentuose pateikiama kainų ir papildoma informacija apie Kliento užsakymą.

1. „Cloud Service“

„IBM Cloud Identity“ teikia vienkartinį registravimąsi (SSO), kelių veiksmų autentifikaciją ir vidinių bei išorinių vartotojų tipų tapatybės gyvavimo ciklo valdiklius.

1.1 Pasiūlymai

Klientas gali rinktis iš šių pasiūlymų, kiekvieno iš kurių įvykių dažnis yra 400 įvykių per sekundę.

1.1.1 „IBM Cloud Identity Connect“

Ši „Cloud Service“ teikia debesimi pagrįsto API įgaliojimo, taikomosios programos „paleidimo aikštelės“, administratoriaus ataskaitų teikimo ir analizės stebėjimo skydo vienkartinį registravimąsi (SSO) ir „Open ID Connect“ (OIDC) autentifikaciją kaip paslaugą. Ši „Cloud Service“ sujungia vartotojus su taikomosiomis programomis, naudodama modernius standartus, pagrįstus autentifikacija ir federaciniais protokolais, įskaitant šimtus jungčių su bendromis taikomosiomis programomis. Ši „Cloud Service“ glaudžiai integruoja su vietine „IBM Security Access Management“ (ISAM) programine įranga, kuri įtraukta kaip įgalinimo programinė įranga, ir suteikia Klientams sprendimą, skirtą prieigos, apimančios taikomąsias programas vietoje ir debesyje, valdymui palaikyti, atsižvelgiant į verslo krypties poreikius.

1.1.2 „IBM Cloud Identity Connect for ISAM“

Ši „Cloud Service“ glaudžiai integruoja su vietine „IBM Security Access Management“ (ISAM) programine įranga ir suteikia Klientams sprendimą, skirtą prieigos, apimančios taikomąsias programas vietoje ir debesyje, valdymui palaikyti, atsižvelgiant į verslo krypties poreikius. Šiai „Cloud Service“ Klientas privalo turėti aktyvias „IBM Security Access Management“ (ISAM) programos Programinės įrangos prenumeratos ir palaikymo (S&S) teises ir S&S privalo išlikti aktyvi visą Kliento „Cloud Service“ prenumeratos laikotarpį. Kliento teisių į šią „Cloud Service“ turi būti tiek pat, kiek ir Kliento vietinės ISAM licencijos teisių. Nutraukus Kliento S&S, nutraukiama ir ši „Cloud Service“. Prieiga prie įgalinimo programinės įrangos apibrėžta 5.2 skyriuje ir neįtraukta į šią „Cloud Service“.

1.1.3 „IBM Cloud Identity Essentials“

Ši „Cloud Service“ suteikia Klientams Vienkartinio prisijungimo (SSO) funkciją įvairiose jų naudojamose IBM ir viešosiose debesies taikomosiuose programose. Šią „Cloud Service“ galima sujungti su IBM „MaaS360“ ir suteikti papildomus saugos valdiklių lygius, pvz., sąlyginę prieigą.

1.1.4 „IBM Cloud Identity Verify“

Ši „Cloud Service“ suteikia kelių veiksmų autentifikaciją, skirtą taikomosioms programoms, kurias saugo „Cloud Identity Connect“ arba per tiesioginę API iškvietą, ir kitiems vykdymo taškams, įskaitant RADIUS klientus, „Unix“ / „Linux“ PAM serverius ir „Windows“ serverius, kad būtų patikrintos jų tapatybės, prisijungiant prie skaitmeninės paslaugos. Tai apima tokius mechanizmus, kaip el. paštas, SMS ir laiku pagrįsti (programinės įrangos atpažinimo ženklas) vienkartiniai slaptažodžiai ir „Push“ pranešimai, pagrįsti mobiliųjų įrenginių biometrine autentifikacija, kurią teikia „IBM Verify“. Ši „Cloud Service“ integruoja su vietine „IBM Security Access Management“ (ISAM) programine įranga ir suteikia Klientams sprendimą, skirtą prieigos, apimančios taikomąsias programas vietoje ir debesyje, valdymui palaikyti, atsižvelgiant į verslo krypties poreikius. Ji pasiekama viena arba kartu su „Cloud Identity Connect“, „Cloud Identity Connect“, skirta ISAM ir „Cloud Identity Essentials“.

1.1.5 „IBM Cloud Identity Govern“

Ši „Cloud Service“ glaudžiai integruoja su vietine „IBM Governance and Intelligence“ (IGI) programine įranga, kuri įtraukta kaip įgalinimo programinė įranga, ir suteikia Klientams sprendimą, skirtą prieigos, apimančios taikomąsias programas vietoje ir debesyje, valdymui palaikyti, atsižvelgiant į verslo krypties poreikius. Ši „Cloud Service“ suteikia organizacijoms debesyje naudojamas išplėstines tapatybės gyvavimo ciklo valdymo galimybes ir apima taikomosios programos prieigos užklausų darbo srautą.

1.1.6 „IBM Cloud Identity Connect and Verify“

Ši „Cloud Service“ teikia Klientui „IBM Cloud Identity Connect“ ir „IBM Cloud Identity Verify“ funkcijas kaip atskirą pasiūlymą.

1.1.7 „IBM Cloud Identity Analyze“

Ši „Cloud Service“ papildo esamus IBM sprendimus, pavyzdžiui, „IBM Security Identity Governance and Intelligence“ (IGI) ir „IBM Security Identity Manager“ (ISIM) ir pateikia holistinį valdomų vartotojų rizikos profilį. Ši „Cloud Service“ apima vietinį, universalų analizės modulį, kurį naudojant apdorojami iš įvairių šaltinių gauti veiklų ir teisių duomenis ir pateikiamas 360 laipsnių prieigos rizikų vaizdas ir suteikiama galimybė imtis veiksmų pagal tas rizikos įžvalgas.

1.1.8 „IBM Cloud Identity Adaptive Access“

Ši „Cloud Service“ naudoja pasitelkus Dirbtinį intelektą (DI) gautas kontekstines įžvalgas apie vartotojus, jų įrenginius ir elgesį siekiant organizacijoms padėti vykdyti tinkamą autentifikavimo politiką.

1.1.9 „IBM Cloud Identity Connect Verify and Govern“

Ši „Cloud Service“ teikia Klientui „IBM Cloud Identity Connect“, „IBM Cloud Identity Verify“ ir „IBM Cloud Identity Govern“ funkcijas kaip atskirą pasiūlymą.

1.2 Pasirinktinės paslaugos

1.2.1 „IBM Cloud Identity Non-Production“

„IBM Cloud Identity Non-Production Environment on Cloud“ yra atskiras „IBM Cloud Identity“ platformos egzempliorius, kurį Klientas gali naudoti tik ne gamybos vidiniams veiksams atlikti, įskaitant, bet neapsiribojant, tikrinimą, veikimo reguliavimą, trikčių diagnozavimą, vidinį kontrolinį testą, parengimo kokybės užtikrinimo veiksmus ir (arba) viduje naudojamų „Cloud Service“ priedų ar plėtinių kūrimą, naudojant paskelbtas taikomųjų programų programavimo sąsajas. Šioje „Cloud Service“ yra galimybė įtraukti pasiekiamumo paslaugos lygio sutartį (PLS), atsižvelgiant į 3 skyriaus „Paslaugos lygiai ir techninis palaikymas“ sąlygas. „Cloud Service“ dažnis yra 100 įvykių per sekundę.

1.2.2 „IBM Cloud Identity Vanity Domain“

„Vanity Domain“ (vienas domenas) leidžia Klientui naudoti domeną, priklausantį jo organizacijai ir labiau su ja susijusį, o ne numatytąjį kliento domeną, kurį teikia iš anksto parengta platforma. Šio domeno SSL sertifikatą tvarkys IBM ir kasmet jį atnaujins.

1.2.3 „IBM Cloud Identity Application Gateway Hosted“

Taikomosios programos šliuzu Klientams, ieškantiems nestandartinių arba sentelėjusių pagrįstų autentifikavimo mechanizmų palaikymo, suteikiamas IBM valdomas ir nuomojamas paprastas prietaisas. Šie mechanizmai apima LTPA ir HTTP antraštėmis grindžiamą autentifikavimą. Už vykdomą priežiūrą ir patikrą atsakinga yra IBM.

1.3 Akceleravimo paslaugos

1.3.1 „IBM Cloud Identity Connect Solution Planning“

Ši paslauga teikia vieną (1) savaitę profesionalių paslaugų, kurių metu IBM atliks kelis arba visus iš šių veiksmų:

- debesimi pagrįstų „SaaS“ taikomųjų programų vienkartinio registravimosi kūrimas;
- „paleidimo aikštelės“, kad būtų galima lengvai nustatyti taikomiosios programos vietą, konfigūravimas;
- taikomųjų programų su parengtomis jungtimis sujungimas;
- sprendimų planavimas, architektūra ir instrukcijos;
- IBM pateiks metodo rekomendacijas ir praktikas.

1.3.2 „IBM Cloud Identity Verify Workshop for Multi-Factor Authentication“

Ši paslauga pateikia trijų (3) dienų profesionalius paslaugos seminarus, orientuotus į kelių veiksnių autentifikavimo sunkumus ir Kliento taikomųjų programų apsaugą, naudojant „IBM Cloud Identity Verify“. Seminaras apims kelias arba visas toliau nurodytas temas:

- pažįstamo autentifikavimo įdėjimas į visas skaitmenines ir asmenines sąveikas, reikalaujančias autentifikavimo;
- taikomosios programos, skirtos stipriam autentifikavimui vykdyti, naudojant kūrėjui patogią REST API, įgalinimas;
- geriausios pramonėje praktikos rekomendacijų apie tapatybės apsaugą teikimas;
- supaprastinta vartotojo patirtis ir visų formų veiksmų – telefonų, planšetinių ir nešiojamųjų kompiuterių – perėmimas;

1.3.3 „IBM Cloud Security Strategy and Planning“

Ši paslauga teikia trijų (3) savaitių profesionalių paslaugų seminarą apie tai, kaip taikyti debesies apsaugos geriausias praktikas, orientuotas į infrastruktūrą ir taikomųjų programų apsaugą. Seminaras apims kelias arba visas toliau nurodytas temas:

- debesimi pagrįstų „SaaS“ taikomųjų programų vienkartinio registravimosi kūrimas;
- „paleidimo aikštelės“, kad būtų galima lengvai nustatyti taikomosios programos vietą, konfigūravimas;
- taikomųjų programų su parengtomis jungtimis sujungimas;
- sprendimų planavimas, architektūra ir instrukcijos;
- kibernetinio saugumo tendencijų išvalgos;
- IBM pateiks metodo rekomendacijas ir praktikas.

1.3.4 „IBM Cloud Identity Expert On Demand“

Ši paslauga suteikia dvidešimt (20) valandų profesionalių paslaugų, teikiamų po dviejų (2) valandų sesijas per trisdešimt (30) dienų nuo pradžios. Paslauga pateiks „Cloud Identity“ architektą, kuris atsakys į klausimus ir pateiks instrukcijas bei rekomendacijas dėl (tačiau tuo neapsiribojant):

- techninių įgūdžių, reikalingų Kliento „Cloud Identity“ sprendimo diegimui papildyti;
- architektūros ir diegimo klausimų apie Kliento debesies tapatybės sprendimą;
- Kliento „Cloud Identity“ sprendimo ir (arba) strategijos instrukcijų.

2. Duomenų tvarkymo ir apsaugos duomenų lapai

Svetainėje <http://ibm.com/dpa> pateikiamame IBM Duomenų tvarkymo priede (DTP) ir toliau esančiose nuorodose pateikiamame (-uose) Duomenų tvarkymo bei apsaugos duomenų lape (-uose) (vadinamame (-uose) duomenų lapu (-ais) arba DTP įrodymu (-ais) pateikiama papildoma „Cloud Service“ duomenų apsaugos informacija ir jos apsaugos galimybės, susijusios su Turinio, kuris gali būti tvarkomas, tipais, atliekamais tvarkymo veiksmais, duomenų apsaugos funkcijomis ir Turinio saugojimo bei grąžinimo specifiką. DTP taikomas asmeniniams duomenims, esantiems turinyje, jei (ir tik tokia apimtimi) taikomas i) Europos bendrasis duomenų apsaugos reglamentas (ES/2016/679) (BDAR) arba ii) kiti duomenų apsaugos teisės aktai, nurodyti <http://ibm.com/dpa/dpl>.

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

3. Paslaugos lygiai ir techninis palaikymas

3.1 Paslaugos lygio sutartis

IBM teikia Klientui toliau nurodytus pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus. IBM taikys aukščiausią galimą kompensaciją, pagrįstą „Cloud Service“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Pasiekiamumo procentas apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą Paslaugos neveikimo minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį. Neveikiančios paslaugos apibrėžimas, pretenzijos pateikimo procesas ir informacija, kaip susisiekti su IBM dėl paslaugos pasiekiamumo problemų, pateikiama IBM „SaaS“ palaikymo apžvalgoje, kurią galima rasti adresu https://www.ibm.com/software/support/saas_support_overview.html.

Prieinamumas	Kreditas (% mėnesio prenumeratos mokesčio*)
Mažiau nei 99,9 %	10 %

* Prenumeratos mokestis yra teiginyje minimo mėnesio sutartinė kaina.

3.1.1 Kita informacija apie šią PLS

Per pirmąsias šešiasdešimt (60) Kliento termino dienų („Išbandymo laikotarpis“) Klientui nebus suteiktas joks kreditas, jei „IBM Cloud Identity“ aplinka nepasieks minimalaus 99,9 % Veiksnumo procento pagal šią Sutartį. Jei iki Išbandymo laikotarpio arba per jį IBM nustatys esamas Kliento konfigūracijas, strategijas, duomenis ar kodą („Esami komponentai“), numatytus perkelti į „IBM Cloud Identity Service“, kurie neleistų „IBM Cloud Identity Service“ sėkmingai pasiekti Veiksnumo procento, nurodyto šioje Sutartyje, IBM pasilieka teisę pranešti Klientui apie tokius Esamus komponentus ir savo nuožiūra jiems netaikyti PLS nuostatų. Jei IBM praneš Klientui apie bet kokius netaikomus Esamus komponentus, IBM privalės Klientui pateikti ištaisymo planą, kiek tai įmanoma, pagal kurį šie netaikomi komponentai atitiks šios Sutarties Veiksnumo laiko procentą. Tik Klientas bus atsakingas už bet kokio ištaisymo kaštus, jei abi šalys nėra sutarusios kitaip.

3.2 Techninė pagalba

„Cloud Service“ techninį palaikymą, įskaitant palaikymo kontaktinę informaciją, sudėtingumo lygius, pasiekiamumo palaikymo valandas, atsakymo laiką ir kitą palaikymo informaciją ir procesus rasite pasirinkę „Cloud Service“ IBM palaikymo vadove svetainėje <https://www.ibm.com/support/home/pages/support-guide/>.

4. Mokesčiai

4.1 Mokesčio apskaičiavimas

„Cloud Service“ mokesčio apskaičiavimas nurodytas Operacijų dokumente.

Šiai „Cloud Service“ taikomas toks mokesčio apskaičiavimas:

- Įgaliotasis vartotojas – tai unikalus vartotojas, kuriam bet koku tiesioginiu arba netiesioginiu būdu (pavyzdžiui, naudojant tankinimo programą, įrenginį arba taikomųjų programų serverį) ir bet kokiomis priemonėmis suteikiama teisė naudotis prieiga prie „Cloud Services“.
- Darbuotojas – tai unikalus asmuo, dirbantis arba gaunantis atlyginimą ar veikiantis vardu Kliento organizacijos, kuriai suteikta (arba nesuteikta) prieiga prie „Cloud Services“.
- Priskirtas dalyvis – tai privatus ar juridinis asmuo, turintis teisę dalyvauti bet kurioje „Cloud Services“ valdomoje arba stebimoje paslaugos teikimo programoje.
- Egzempliorius yra kiekviena prieiga prie konkrečios „Cloud Services“ konfigūracijos.
- „Engagement“ yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.
- Įvykis yra konkretaus įvykio, kurį apdoroja „Cloud Service“ arba kuris susijęs su „Cloud Services“ naudojimu, atvejis.
 - „Cloud Identity Connect“ įvykis yra http užklausa iš „Cloud Service“.
 - „Cloud Identity Verify“ įvykis yra kelių veiksmų metodas, išskviečiamas per „Cloud Service“.

5. Papildomos sąlygos

„Cloud Service“ sutartims (arba atitinkamoms debesies technologijomis pagrįstoms sutartims), vykdytoms iki 2019 m. sausio 1 d., taikomos sąlygos, pateikiamos <https://www.ibm.com/acs>.

5.1 Kliento nuoroda

Klientas sutinka, kad spaudoje ar rinkodaros informacijoje IBM gali Klientą viešai vadinti „Cloud Service“ prenumeratoriumi.

5.2 Įgalinimo programinė įranga

„Cloud Service“ yra ši įgalinimo programinė įranga:

Toliau nurodytą įgalinimo programinę įrangą galima naudoti tik su „IBM Cloud Identity Connect“, „IBM Cloud Identity Connect and Verify“ ir „IBM Cloud Identity Connect Verify and Govern Cloud Services“:

- „IBM Security Access Manager Virtual Enterprise Edition“

Toliau nurodytą įgalinimo programinę įrangą galima naudoti tik su „IBM Cloud Identity Govern“ ir „IBM Cloud Identity Connect Verify and Govern Cloud Services“:

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

Toliau nurodytą įgalinimo programinę įrangą galima naudoti tik su „IBM Cloud Identity Analyze Service“.

- Vietinis „IBM Cloud Identity Analyze“ analizės modulis

5.3 Patikrinimas

Klientas i) palaikys ir gavęs prašymą teiks įrašus ir sistemos įrankių išvestį, kai tai pagrįstai bus reikalinga IBM ir jos nepriklausomam auditoriui, kad patikrintų, kaip Klientas laikosi šios Sutarties sąlygų, ir ii) nedelsdamas užsakys bei apmokės visas reikiamas teises pagal tuo metu IBM galiojančius tarifus ir kitus tokio patikrinimo metu nustatytus mokesčius bei prievoles, nurodytas IBM sąskaitoje faktūroje. Šie sąlygų laikymosi patikrinimo įsipareigojimai galioja „Cloud Service“ laikotarpi ir dvejus metus po jo.