„IBM Cloud Integrated Analytics Environment“

Šiame Paslaugos apraše apibūdinta „Cloud Service“, kurią IBM pateikia Klientui. Klientas reiškia susitariančiąją šalį, jos įgaliotuosius vartotojus ir „Cloud Service“ gavėjus. Atitinkamas Pasiūlymas ir Teisių suteikimo dokumentas (TSD) pateikiami kaip atskiri Sandorio dokumentai.

1. „Cloud Service“

„IBM Cloud Integrated Analytics Environment“ (IAE) – tai diegimo modelis, įgalinantis privatų vietinį ryšį tarp skirtingų įgalintų, atskirai įsigytų „Cloud Service“ pasiūlymų, taip pat saugaus kliento ryšio galimybių.

Klientas turi įsigyti šias teises:

- „IBM Cloud Integrated Analytics Environment“ arba „IBM Cloud Integrated Analytics Dedicated Environment“ ir
- „IBM Cloud Integrated Analytics VPN Connectivity“ arba „IBM Cloud Integrated Analytics Standard Security Appliance“, arba „IBM Cloud Integrated Analytics Enterprise Security Appliance“.

1.1 Bazinės paslaugos

1.1.1 „IBM Cloud Integrated Analytics Environment“

„IBM Cloud Integrated Analytics Environment“ diegiama „IBM SoftLayer“ duomenų centre, kurį sudaro dvi zonos:

- Valdomųjų paslaugų zona, kur diegiamos IAE vietinės valdomosios paslaugos (įskaitant IBM valdomus „vietos su vieta“ VPN) ir „IBM Analytics“ valdomieji „SaaS“ pasiūlymai. Šią zoną valdo IBM.
- Nuomojamų išteklių zona, kur diegiami „IBM Analytics“ nuomojamų išteklių „SaaS“ pasiūlymai. Šios sistemos gali būti:
  - Nuomojamų išteklių pasiūlymai, pvz., „DB2 on Cloud“
  - IAE serveriai, kaip apibrėžta toliau

Nuomojamų išteklių zona gali naudoti išorinę užkardą, kurią teikia atskirai įsigyjamas ir Kliento valdomas „IBM Cloud Integrated Analytics Standard Security Appliance“ arba „IBM Cloud Integrated Analytics Enterprise Security Appliance“.

1.1.2 „IBM Cloud Integrated Analytics Dedicated Environment“

Ši „Cloud Service“ Klientams suteikia visas anksčiau paminėtas funkcijas, įtrauktas į „IBM Cloud Integrated Analytics Environment“ ir sukonfigūruotas veikti su skirtomis užkardomis.

1.1.3 „IBM Cloud Integrated VPN Connectivity“

IBM valdoma „vietos su vieta“ VPN paslauga. IBM automatiškai nutrauks kiekvieną VPN ryšį pasibaigus „IBM Cloud Integrated Analytics Environment“ naudojimui. „IBM Cloud Integrated Analytics VPN Connectivity“ paslauga naudoja „vietos su vieta“ „IPsec“ VPN technologiją.

1.1.4 „IBM Cloud Integrated Analytics Standard Security Appliance“

Nuomojamų išteklių zonoje diegiamas ir Kliento valdomas saugos įrenginys. Kliento naudojamas įgalinti Kliento valdomą „vietos su vieta“ VPN arba Kliento valdomą „kliento su vieta“ VPN, taip pat nuomojamų išteklių zonos užkardai nuo viešojo interneto.

1.1.5 „IBM Cloud Integrated Analytics Enterprise Security Appliance“

Perteklinė Nuomojamų išteklių zonoje įdiegtų ir Kliento valdomų saugos įrenginių pora, ji gali būti naudojama įgalinti Kliento valdomą „vietos su vieta“ VPN arba Kliento valdomą „kliento su vieta“ VPN, taip pat nuomojamų išteklių zonos užkardai nuo viešojo interneto.

1.2 Pasirinktinės paslaugos

1.2.1 IAE serveriai

„IBM Cloud Integrated Analytics Environment“ serveriai, diegiami nuomojamų išteklių zonoje, naudojami su Klientui priklausančiomis programomis, kurioms reikalingas spartus ir mažos gaišties ryšys su kitomis programomis Valdomųjų paslaugų ir Nuomojamų išteklių zonose.

- **„IBM Cloud Integrated Analytics Extra Small Server“**

  Kliento valdomas „SoftLayer“ serveris su minimaliomis 1 viešojo virtualiojo branduolio, 4 GB RAM, 25 GB SAN disko specifikacijomis.

- **„IBM Cloud Integrated Analytics Small Server“**

  Kliento valdomas „SoftLayer“ serveris su minimaliomis 4 viešųjų virtualiųjų branduolių, 16 GB RAM, 100 GB SAN disko specifikacijomis.

- **„IBM Cloud Integrated Analytics Medium Server“**

  Kliento valdomas „SoftLayer“ serveris su minimaliomis 8 viešųjų virtualiųjų branduolių, 32 GB RAM, disk1 100 GB SAN disko, disk2 100 GB SAN disko specifikacijomis.

- **„IBM Cloud Integrated Analytics Large Server“**

  Kliento valdomas „IBM SoftLayer“ serveris su minimaliomis 16 privačiųjų virtualiųjų branduolių, 64 GB RAM, disk1 100 GB SAN disko, disk2 100 GB SAN disko specifikacijomis.

- **„IBM Cloud Integrated Analytics Storage“**

  SAN saugykla gali būti pridėta prie IAE serverių 100, 250 arba 500 GB dalimis.

2. Saugos aprašas

Šiai „Cloud Service“ netaikomi „Cloud Service“ duomenų saugos ir privatumo principai. „Cloud Service“ kontroliuoja Klientas, ir turi būti palaikomi Kliento saugos standartai.Klientas pripažįsta, kad ši „Cloud Service“ nesiūlo funkcijų, skirtų apsaugoti turiniui, kuriame yra asmens duomenų, konfidencialių asmens duomenų ar duomenų, kuriems taikomi papildomi teisiniai reikalavimai. Jei Klientas įtraukia šiuos duomenis į savo turinį, IBM nurodoma, kad tokius duomenis reikia tvarkyti pagal šią Sutartį, nustačius, kad techninės ir organizacinės saugos priemonės yra tinkamos pagal riziką, kuri kyla tvarkant, ir saugotinų duomenų pobūdį. Klientas pripažįsta, kad IBM nežino, kokių tipų duomenys yra įtraukti į turinį, ir negali įvertinti jų tinkamumo „Cloud Service“ ar vietoje taikomoms saugos priemonėms.

2.1 Saugos funkcijos ir įsipareigojimai

„Cloud Service“ įgyvendina šias saugos funkcijas:

„Cloud Service“ šifruoja turinį, perduodant duomenis už IBM tinklo ribų. „Cloud Service“ nešifruoja turinio, kai yra neaktyvi laukdama duomenų perdavimo.Klientas yra atsakingas už turinio šifravimą prieš įtraukiant jį į „Cloud Service“.

IBM Klientui praneš apie saugos incidentus, tačiau pats Klientas yra atsakingas už tokių incidentų ištyrimą ir išsprendimą. IBM pasilieka teisę izoliuoti ir sulaikyti „Cloud Service“, jei dėl neišspręsto incidento iškiltų pavojus jos saugai.

3. Techninis palaikymas

„Cloud Service“ techninis palaikymas teikiamas per internetinius forumus ir internetinę pranešimo apie problemas sistemą. IBM pateiks „IBM Software as a Service Support Handbook“ (IBM Programinės įrangos kaip paslaugos palaikymo vadovą), kuriame nurodyta techninio palaikymo centro kontaktinė informacija, kita informacija ir procesai. Techninis palaikymas įtrauktas į „Cloud Service“ ir kaip atskiras pasiūlymas neteikiamas.

4. Teisių suteikimo ir sąskaitų išrašymo informacija

4.1 Mokesčio apskaičiavimas

„Cloud Service“ pateikiama pagal mokesčių apskaitos metriką, nurodomą Operacijų dokumente:

Egzempliorius yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Egzempliorius yra prieiga prie konkrečios „Cloud Service“ konfigūracijos. Reikia įsigyti pakankamas teises, skirtas kiekvienam „Cloud Service“ Egzemplioriui pasiekti ir naudoti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

Gigabaitas yra matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Gigabaitas yra 2 pakelta trisdešimtuoju laipsniu baitų duomenų (1 073 741 824 baitai). Reikia įsigyti teises, pakankamas gigabaitų, apdorojamų „Cloud Service“, bendram skaičiui padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

5. Terminas ir pratęsimo galimybės

„Cloud Service“ naudojimo terminas prasideda nuo dienos, kai IBM praneša Klientui, kad jis turi prieigą prie „Cloud Service“, kaip aprašyta TSD. TSD bus nurodyta, ar „Cloud Service“ bus atnaujinama automatiškai, naudojama nepertraukiamo naudojimo pagrindu ar nutraukiama laikotarpio pabaigoje.

Atnaujinant automatiškai, jei Klientas nepateikia prašymo neatnaujinti raštu mažiausiai prieš 90 dienų iki termino galiojimo pabaigos datos, „Cloud Service“ automatiškai atnaujinama TSD nurodytam laikotarpiui.

Naudojant nuolat, „Cloud Service“ pasiekiamumas pratęsiamas kiekvieną mėnesį, kol Klientas prieš 90 dienų iki nutraukimo raštu pateiks prašymą nutraukti. Praėjus 90 dienų laikotarpiui, „Cloud Service“ bus pasiekiama iki kalendorinio mėnesio pabaigos.

6. Papildomos sąlygos

6.1 Bendrosios nuostatos

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

6.2 Kliento įsipareigojimai

Užpildyti virtualaus privačiojo tinklo (VPN) klausimyną ir jį pateikti IBM peržiūrėti prieš VPN konfigūravimo pradžios datą.

Skirti atskirą kontaktinį asmenį, išmanantį kliento organizacijos tinklą, VPN ir saugos reikalavimus.

Užtikrinti, kad saugos ir tinklo administratorius (-iai) būtų pasiekiamas (-i) VPN konfigūravimo ir tikrinimo etape, kad jie galėtų dirbti su IBM atliekant VPN sąranką.

Visas VPN reikalingos aparatūros bei programinės įrangos administravimas, priežiūra, modifikavimas, konfigūravimas ir testavimas kliento vietoje.

Priimtinumo vartotojams testavimas norint patikrinti VPN konfigūraciją įgyvendinimo etape.

Naudojant internetinę pranešimo apie problemas sistemą pranešti apie bet kokius VPN konfigūracijai reikalingus pakeitimus.