Techninė dokumentacija

„Qlik® Sense“ saugumo apžvalga

2015 m. rugsėjis

Platforma

„Qlik® Sense“ – tai analitikos platforma, kurioje naudojamas asociatyvinis analitikos variklis operatyvinėje atmintyje. Remiantis naudotojo pasirinktimis, skaičiavimai atliekami apdorojimo laiku pagal atmintyje saugomus duomenis. Rezultatai pateikiami naudotojams per nediegiamą interneto sąsają staliniuose ar nešiojamuosiuose kompiuteriuose bei mobiliuosiuose įrenginiuose, taip per integruotąją analitiką. „Qlik Sense“ siūlo labai interaktyvią ir asociatyvią patirtį, o naudotojai gali nevaržomai naršyti duomenyse be jokių ar beveik be jokių analizės apribojimų.

Apžvalga

„Qlik® Sense“ suteikia galimybę savarankiškai kurti vizualizaciją, kuri yra pritaikoma, saugi ir valdoma. Siekiant užtikrinti platformos saugumą, „Qlik® Sense“ derindama vidinius ir išorinius išteklius valdo prieigą, tapatybės patvirtinimą, autorizaciją ir duomenų valdymą keturiais lygmenimis.

- **Tinklo apsauga**: visi ryšiai tarp „Qlik® Sense“ tarnybų ir žiniatinklio klientų naudoja interneto protokolus su siuntimo lygmens apsauga (TLS). Naudodama skaitmeninius sertifikatus TLS šifruoja informaciją, siunčiamą tarp tarnybų, serverių ir klientų. Šifruota informacija keliauja tuneliais, kuriuose ryšiui apsaugoti reikalaujama dviejų sertifikatų: serverio sertifikato, leidžiančio identifikuoti reikiamą serverį, ir kliento sertifikato, kuris leidžia klientui užmegzti ryšį su nurodytu serveriu.

- **Serverio apsauga**: operacinės sistemos apsaugos sistema kontroliuoja sertifikatų, saugyklos, atminties ir centrinio procesoriaus išteklių pasiekimą. Naudodama šias kontrolės priemones „Qlik® Sense“ apsaugo platformą leisdama pasiekti atitinkamus išteklius tik įgaliotiems naudotojams ir procesams.[1]

- **Procesų apsauga**: kūrimo metu atliekami griežti „Qlik® Sense“ tikrinimo procesai, padedantys mažinti rizikas ir išvengti nenumatytų įvykių. Papildomais bandymais patikrinama, ar „Qlik® Sense“ gali atlaikyti žinomas saugumo grėsmes programinei įrangai.

- **Aplikacijų apsauga**: atributais grindžiama prieigos kontrolė suteikia visapusišką bendrąją sistemą, leidžiančią valdyti naudotojų galimybes platformoje. Eilučių ir stulpelių lygmens duomenų ribojimas naudojant sekcijų prieigos funkciją dinamiškai kontroliuoja, kokius duomenis naudotojai gali peržiūrėti ir pasirinkti programose.

[1] Daugiau informacijos apie „Qlik Sense“ architektūrą žr. „Qlik Sense“ architektūros apžvalgoje.

Tapatybės patvirtinimas

„Qlik® Sense“ tarpinis serveris

Bet kokį tapatybės patvirtinimą „Qlik® Sense“ įdiegtyje valdo tarpinių serverių tarnyba „Qlik® Sense Proxy Service“ (QPC), įskaitant ir klientus, kurie jungiasi prie centro arba valdymo konsolės „Qlik® Management Console“ (QMC). „Qlik® Sense“ reikalauja, kad išorinis tapatybės teikėjas patikrintų konkretaus naudotojo tapatybę. Atlikus patikrinimą, „Qlik® Sense“ perduoda naudotoją centrui arba QMC naudodama TLS ir sertifikato tapatybės patvirtinimą šiais metodais:

- **Bilieto API** perduoda naudotoją ir naudotojo atributus naudodama vienkartinį bilietą. Pavyzdžiui, „Windows“ tapatybės patvirtinimo funkcija su „Qlik® Sense“ iškviečia bilieto API po patikrinimo domene.
- **Seanso API**, kai išorinis modulis perduoda internetinį seansą, kuriuo naudotojas identifikuojamas „Qlik® Sense“ programinėje įrangoje.
- **HTTP antraštės** – sprendimuose su patikimomis sistemomis, kurios perduoda naudotojų informaciją šiuo metodu.
- **SAML** integracija su „Qlik® Sense“ veikia kaip paslaugos teikėjas (SP), integruojamas su tapatybės teikėju (IdP).
- Galima konfigūruoti ir **anoniminių** naudotojų prieigą prie „Qlik® Sense“.

„Qlik Sense“ – tapatybės patvirtinimas trimis etapais

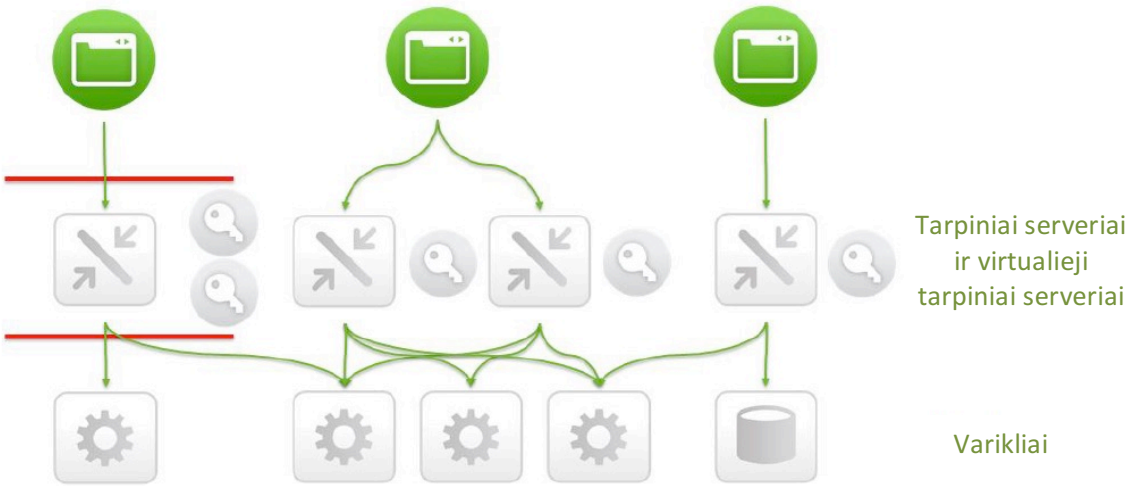
1. Tapatybės patvirtinimo modulis gauna naudotojo tapatybę ir kredencialus.

2. Tapatybės patvirtinimo modulis prašo išorinės sistemos patikrinti naudotojo tapatybę naudojantis kredencialais.

3. Naudotojas perduodamas „Qlik® Sense“ naudojant bilieto API, seanso API, HTTP antraštes arba SAML.

Virtualieji tarpiniai serveriai

Kiekviena QPC „Qlik® Sense“ įdiegtyje naudoja virtualiuosius tarpinius serverius, padedančius atlikti tapatybės patvirtinimą. Virtualieji tarpiniai serveriai leidžia vienam tarpiniam serveriui palaikyti kelias tapatybės patvirtinimo sistemas, atlikti seanso valdymą ir balansuoti apkrovas daugiamazgėse įdiegtyse. Virtualieji tarpiniai serveriai gali užmegzti ryšį su vienu ar keliais QPS mazgais, kad nukreiptų srautus, balansuotų variklių apkrovą arba suteiktų specialią prieigą prie įdiegties administracinių lygmenų. Toliau pateiktoje iliustracijoje kairysis virtualusis tarpinis serveris yra DMZ zonoje ir jungiasi prie dviejų variklių. Kiti tarpiniai serveriai su virtualiaisiais tarpiniais serveriais jungiasi prie kelių variklių priklausomai nuo virtualiojo tarpinio serverio konfigūracijos ir apkrovos balansavimo.



Autorizacija

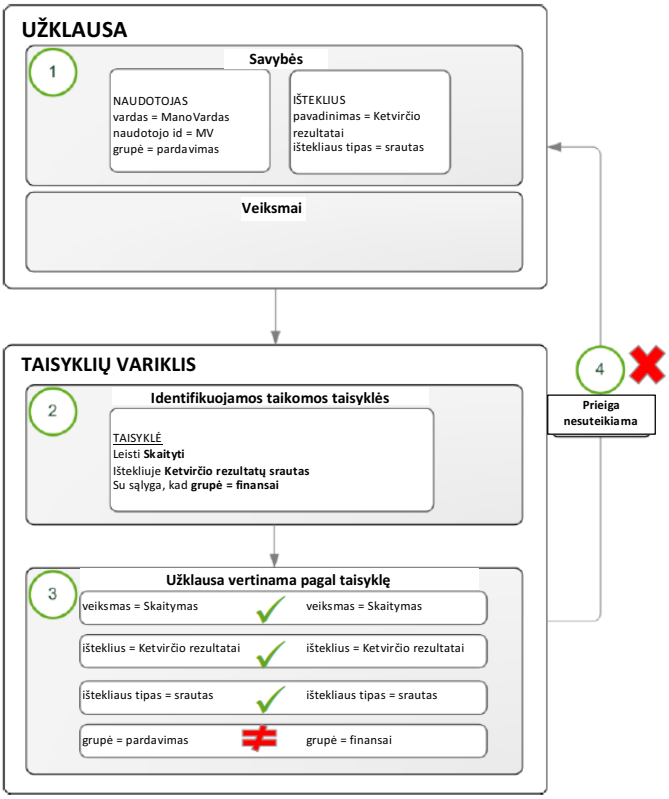
Kai patvirtinama naudotojo tapatybė ir jam suteikiama prieiga prie „Qlik® Sense“, autorizacija naudojant atributais grindžiamos prieigos kontrolės (ABAC)[2] modelį užtikrina aplikacijos matomumą ir savarankiško darbo galimybes aplikacijose.

Atributais grindžiama prieigos kontrolė (ABAC)

Programoje „Qlik® Sense“ ABAC apibrėžiama kaip prieigos kontrolės metodas, kai **naudotojo** teisės atlikti **veiksmus ištekliuose** suteikiamos remiantis priskirtais **naudotojo** atributais, priskirtais **ištekliaus** atributais, **aplinkos** sąlygomis ir rinkiniu **apsaugos taisyklių**, kurios nurodytos tokių atributų ir sąlygų nuostatose. Atributai iš „Active Directory“, LDAP (supaprastintos prieigos prie katalogų protokolo) ir duomenų bazių įkeliami į „Qlik Sense“. Be to, atributus galima apibrėžti bei administruoti ir tiesiogiai programoje „Qlik Sense“.

Apsaugos taisyklės

„Qlik® Sense“ apsaugos taisyklės nustato naudotojo galimybes „Qlik® Sense“ ištekliuose pagal tam tikrą sąlygą.
Prieiga suteikiama, jei bent vienos taisyklės rezultatas yra „teisinga“ pagal tokius atributus kaip naudotojo ir išteklių vaidmenys ar grupės.



Apsaugos taisyklės kontroliuoja prieigą prie aplikacijos srautų centre, galimybes aplikacijose (lapų, istorijos, skirtukų kūrimas) ir administracines galimybes QMC (aplikacijų skelbimas, srauto prieigos nustatymas, užduočių kūrimas ir vykdymas).

Apsaugos taisyklių sistema pateikiama su keliomis iš anksto nustatytomis taisyklėmis, leidžiančiomis administratoriams pritaikyti apsaugą skirtingiems naudotojams derinant esamus vaidmenis ir grupes įmonėje.

Vaidmenimis grindžiamoje įmonėje verslo analitikos autoriai yra atsakingi už aplikacijų kūrimą ir gali pasiekti duomenis. Turinio administratoriai nekuria, bet skelbia aplikacijas srautuose, skirtuose vartotojų grupėms. Vartotojai gali išplėsti nuosavą analizę naudodamiesi lapais ir interpretacijomis aplikacijoje bei dalytis naujai rastomis įžvalgomis su kolegomis nekenkdami pagrindinės aplikacijos vientisumui. Visos šios galimybės ir atitinkamos taisyklės yra įgyvendintos „Qlik® Sense“ kaip standartinės funkcijos.

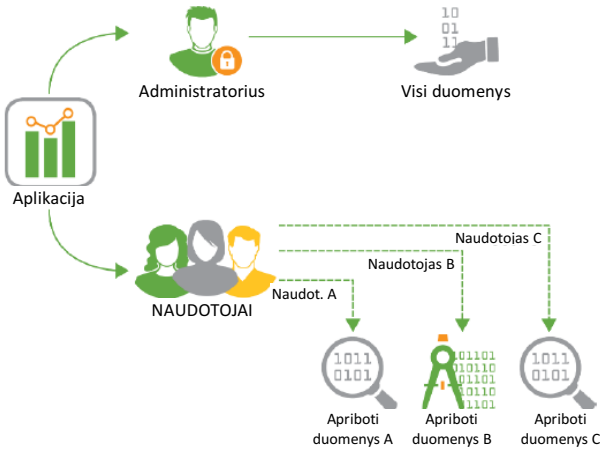
[2] ABAC yra specialus Nacionalinio standartų ir technologijų instituto (NIST) leidinys, kataloguojamas kaip NIST specialusis leidinys 800-162.

Duomenų ribojimas

Duomenų ribojimas programoje „Qlik® Sense“ lemia, kokius duomenis naudotojams ir grupėms leidžiama matyti atidarius „Qlik® Sense“ aplikaciją. „Qlik® Sense“ aplikacijoje duomenų ribojimas vadinamas sekcijų prieiga.

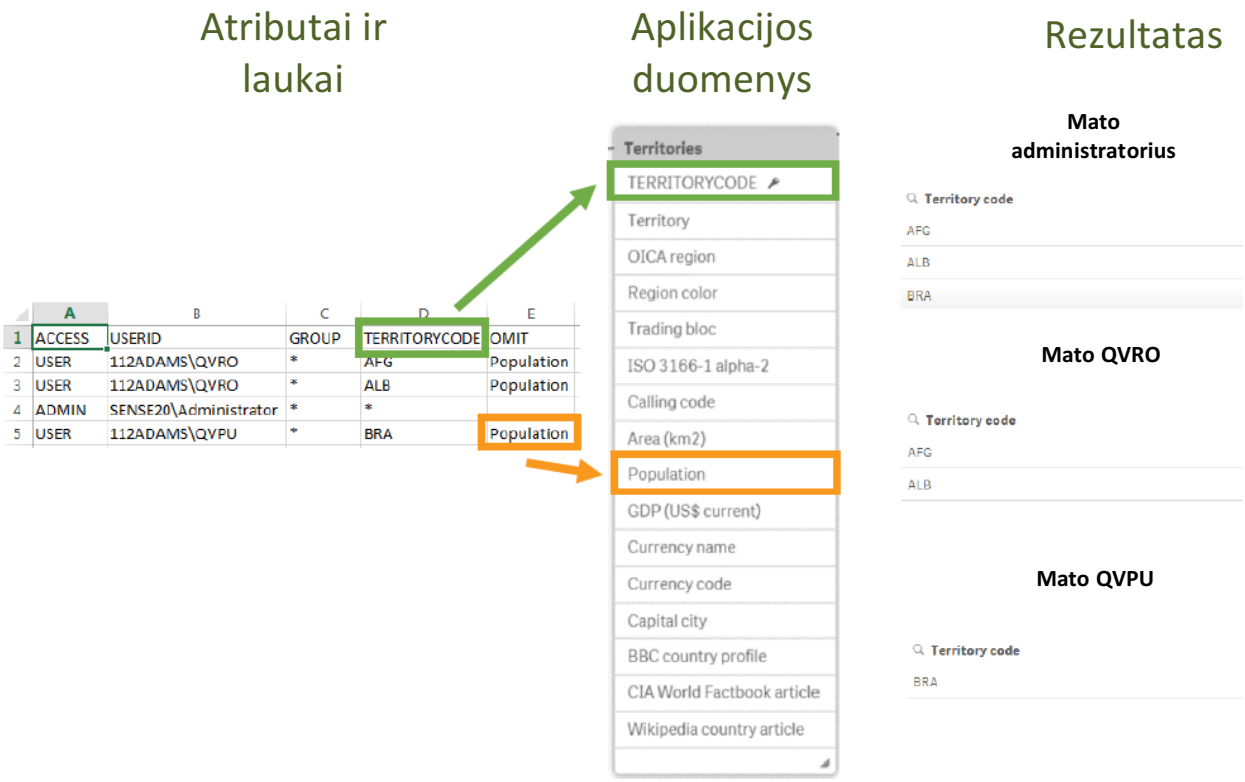
Sekcijų prieiga

Sekcijų prieigos funkcija užtikrina eilučių ir stulpelių lygmens apsaugą aplikacijoje „Qlik® Sense“. Naudojant sekcijų prieigą, vienoje „Qlik® Sense“ aplikacijoje gali būti saugomi kelių naudotojų ar grupių duomenys. Atliekant tapatybės patvirtinimo ir autorizacijos procesą naudotojo informacija siunčiama į aplikaciją siekiant dinamiškai apriboti duomenis, kad naudotojai pasiektų tik duomenis, kuriuos peržiūrėti jiems leidžiama. Kontroliuojant naudotojo galimybes matyti duomenis, sekcijų prieigos funkcija gali naudoti atributus ir laukus iš išorinių duomenų bazių, katalogų, peržvalgos lentelių arba sukurtų lentelių.



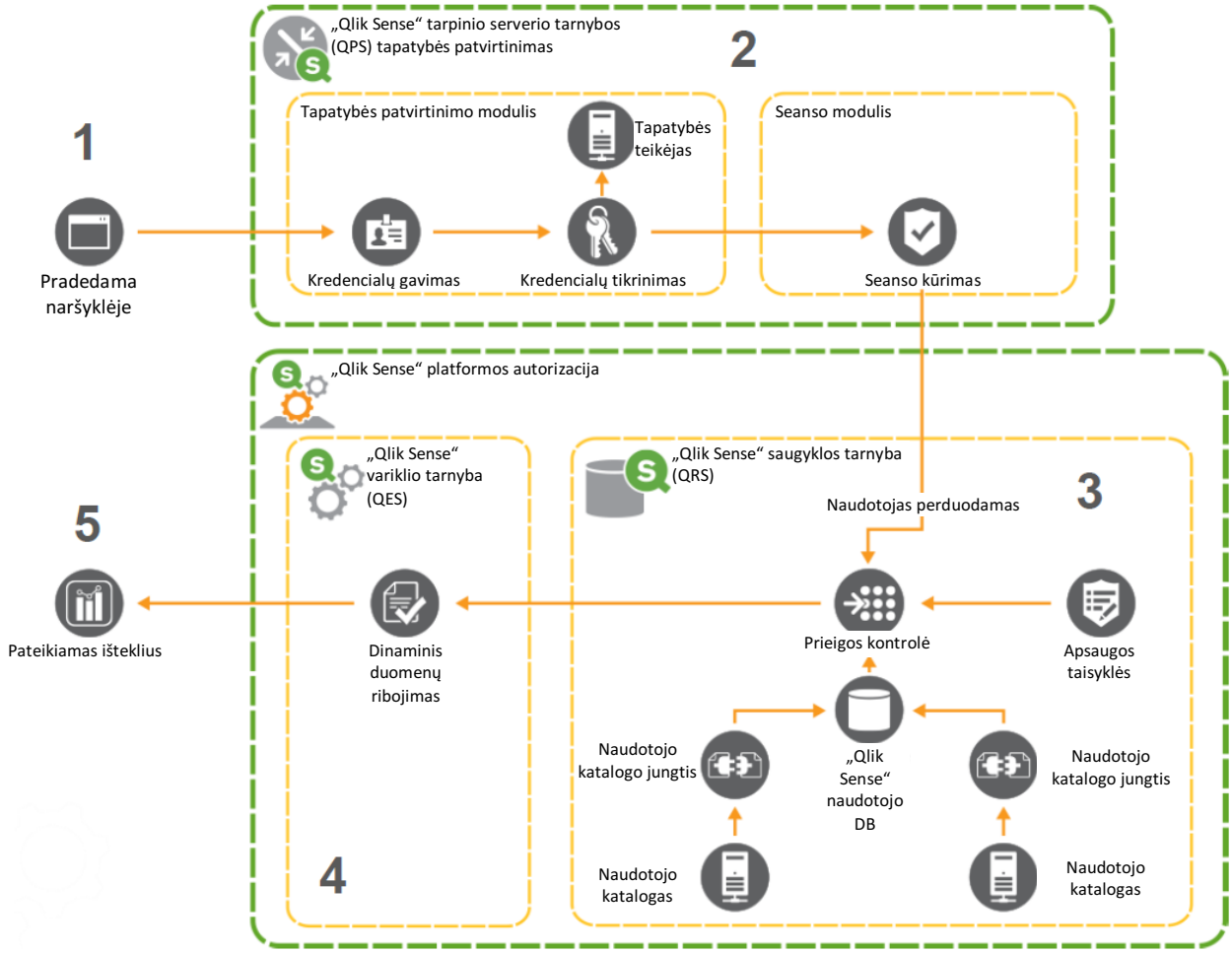
Dinaminis duomenų ribojimas

Sekcijų prieigos funkcija dinamiškai riboja duomenis aplikacijoje susiedama sekcijų prieigos duomenis su į aplikaciją įkeltais verslo duomenimis vieninteliu apibrėžtu santykiu. Naudojant bendrus laukų pavadinimus, duomenų eilutės paslepiamos nuo naudotojo jam atliekant veiksmus aplikacijoje. Be to, galima neleisti matyti duomenų stulpelius nurodant laukų pavadinimus, kurie turi būti praleidžiami kiekvienam naudotojui.



„Qlik Sense“ apsaugos naudotojo prieigos darbo eiga

Tapatybės patvirtinimo, autorizacijos ir duomenų ribojimo derinimas užtikrina sklandžią patirtį „Qlik® Sense“ pasiekiančiam naudotojui.

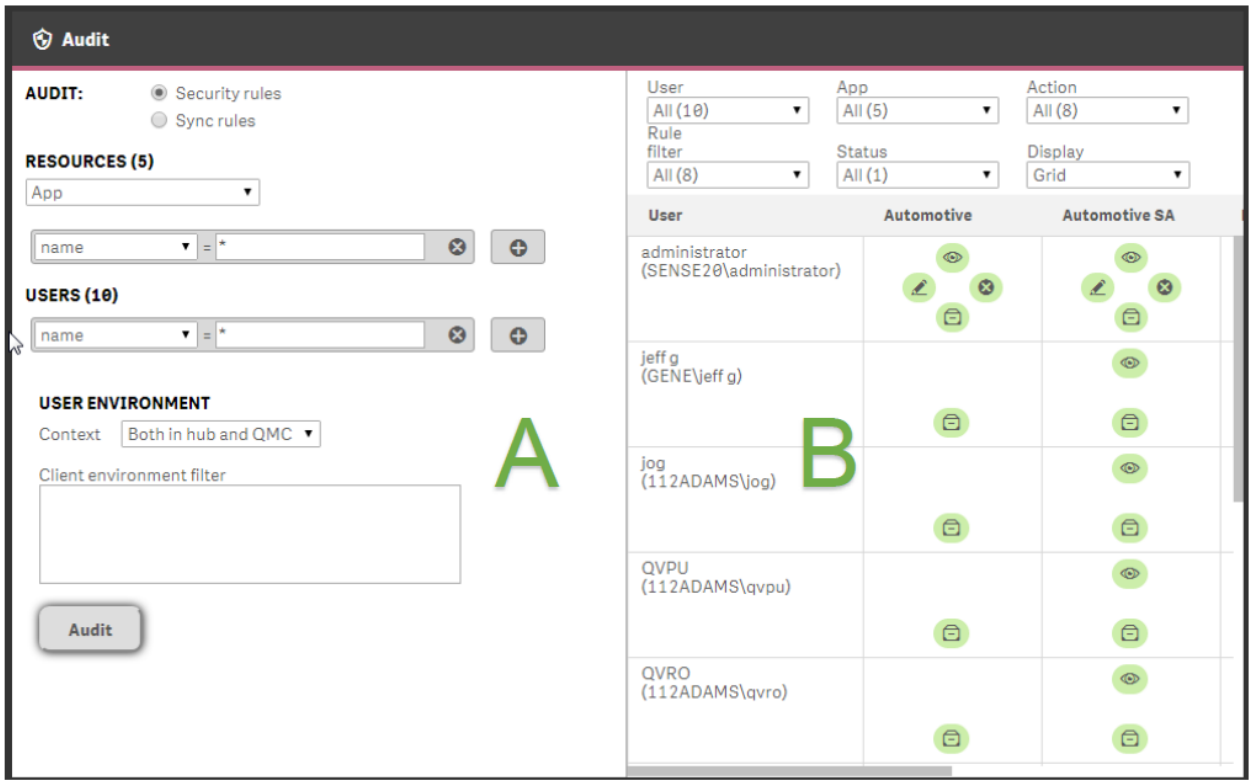


1. Naudotojas pateikia „Qlik® Sense“ turinio užklausą.
2. „Qlik® Sense“ tarpinio serverio tarnyba patvirtina naudotojo tapatybę ir sukuria seanso slapuką naršyklėje.
3. Seanso slapukas identifikuoja naudotoją aplikacijoje „Qlik® Sense“ ir sinchronizuojasi su naudotojo katalogu, kad galėtų importuoti atributus. Tuo pačiu metu taisyklių variklis autorizuoja naudotoją pasiekti „Qlik® Sense“ turinį naudodamas atributais grindžiamą kontrolės modelį.
4. Variklyje sukuriama naudotojo seanso būsena. Variklis atlieka dinaminį duomenų apribojimą naudodamas sekcijų prieigą.
5. Variklis siunčia turinį per interneto lizdo jungtį su klientu pateikdamas „Qlik® Sense“ turinį.

Auditas

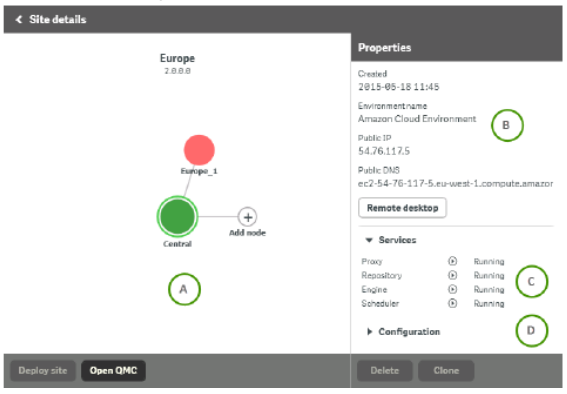
Įmonių verslo analitikoje labai svarbus yra valdymas. „Qlik® Sense“ vykdo auditą, stebėjimą ir registravimą naudodama QMC, aplikacijų ir registravimo failus administratoriams informuoti ir įdiegtyse kylančioms rizikoms mažinti.

- Atlikite apsaugos taisyklių **auditą** naudodamiesi audito skirtuku, integruotu „Qlik®“ valdymo konsolėje (QMC).

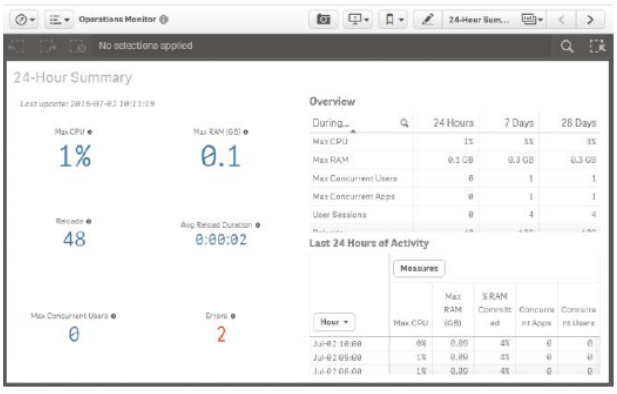


Užklausų rodinyje (A) ir rezultatų rodinyje (B) administratoriai gali vertinti, kaip kontroliuojama naudotojų prieiga prie aplikacijų. Administratoriai gali naudoti tiesioginio audito funkcijas kurdami srautų, turinio bibliotekų ir duomenų ryšių apsaugos taisyklės bei peržiūrėti prieigos kontrolę pagal jų rašomas taisykles.

- **Stebėkite** „Qlik® Sense“ naudodamiesi aplikacijomis „Operations Monitor“ ir „License Monitor“. Šios aplikacijos suteikia informacijos apie darbinės būsenos trukmę, seansus, išteklių naudojimą, registravimo keitimus ir licencijų atitiktų bei administravimą. „Qlik® Deployment Console“ suteikia administratoriams galimybę stebėti daugiamazges įdiegtis ir vizualiai įvertinti infrastruktūros vientisumą.



„Qlik Deployment Console“



„Qlik Operations Monitor“

- Registravimas tekstiniuose failuose atliekamas aplikacijos „Qlik® Sense“ foniniu režimu. Visos tarnybos apima audito, sistemos ir sekimo žurnalus, leidžiančius stebėti ir administruoti įdiegtį.

Santrauka

„Qlik® Sense“ apsaugos funkcijos užtikrina visapusišką apsaugą daugeliu lygmenų, todėl tik įgalioti naudotojai gali pasiekti leidžiamus naudoti duomenis naudodamiesi saugiu ryšiu.

- **Tapatybės patvirtinimas**, kurį tarpinio serverio tarnyba „Qlik® Sense Proxy Service“ (QPS) vykdo naudodama sertifikatus tapatybei patvirtinti ir siuntimo lygmens apsaugą (TLS) tinklo srautui šifruoti.
- **Autorizacija** tarp „QLik® Sense“ mazgų atliekama naudojant TLS ir sertifikatus, atributais grindžiamos prieigos kontrolės (ABAC) sistemą naudotojų prieigai ir turiniui valdyti bei pateikiant konkrečius duomenis naudotojams naudojant sekcijų prieigos funkciją.
- „Qlik® Sense“ platformos **auditas** sekant keitimus saugyklos duomenų bazėje, atliekant išsamų audito ir apsaugos registravimą, stebint aplikacijas ir naudojant įrankius, skirtus prieigos auditui ir daugiamazgių įdiegčių administravimui.
- **Konfidencialumą** užtikrina tinklo ryšių šifravimas naudojant TLS ir tapatybės patvirtinimas sertifikatais, operacinės sistemos failų sistemos ir serverio prieigos valdiklių derinimas saugant „Qlik® Sense“ mazguose esantį turinį, atminties apsauga naudojant operacinės sistemos valdiklius, prieigos prie aplikacijos apsauga išteklių lygmeniu, neskelbtinos informacijos (pvz., slaptažodžių ir duomenų jungčių eilučių) šifravimas bei aplikacijos duomenų apsauga naudojant duomenų ribojimo funkciją.
- **Vientisumas** užtikrinamas tokiais operacinės sistemos valdikliais kaip failų sistema siekiant apsaugoti neaktyvius duomenis, šifruoti neskelbtiną informaciją ir užkirsti kelią atgaliniam duomenų perrašymui į šaltinio sistemą.

Jei norite sužinoti daugiau, apsilankykite Qlik®.com.