IBM SolutionsConnect 2013

Dan pametnijih rješenja

Pametnim podacima do pametnih odluka

BKS Bank d.d.

Nadzor baza podataka: IBM Guardium

Siniša Babić – CISO BKS Bank d.d.
Marko Gustović – Voditelj IT BKS Bank d.d.
Tomislav Mihelić – CISO ETNA d.o.o.

1. Nadzor baza podataka.
- zahtjevi

IBM

1.Nadzor baza podataka.

Zahtjevi:

•Banke imaju višestruke razloge za nadzor baza podaka:

- Zakonska obaveza praćenja (praćenje transakcija, informacijska sigurnost, čuvanje operativnih i sistemskih zapisa)
- Industrijski standardi i dobra praksa.
- Ugovorne obaveze (npr. PCI-DSS i slično).
- Nadzor DBA.
- Nadzor neovlaštenog pristupa i pokušaja neovlaštenog pristupa.
- Forenzička analiza kod analize incidenata i potencijalnih incidenata u svrhu prikupljanja dokaza.
- Izvješćivanje (automatizacija i unifikacija)

1. Nadzor baza podataka. Problemi kod nadzora ugrađenim alatima

IBM

1.Nadzor baza podataka.

Problemi kod nadzora ugrađenim alatima:

•Banke imaju višestruke probleme kod uspostave sustava za nadzor baza podaka korištenjem ugrađenih sustava nadzora (DB auditing):

- Velik broj baza podataka različitih proizvođača i platformi.
- Ugrađeni sustavi nadzora ovisni o pojedinom proizvođaču, vrsti i tipu baze, svaka ima svoj način i logiku rada
- Ugrađeni sustavi nadzora pod kontrolom su DBA te se ne mogu koristiti za nazor samih administratora

•Izvješćivanje (automatizacija i unifikacija) je problematično jer svaka baza ima svoj način rada i alate.

- Većina auditing alata ujteče na performanse sustava, ponekad i značajno ako se nadzire velika količina podataka.

IBM SolutionsConnect 2013
Dan pametnijih rješenja

1. Nadzor baza podataka. Problemi kod nadzora dodatnim alatima proizvođača baza

IBM

1.Nadzor baza podataka.

Problemi kod nadzora dodatnim alatima proizvođača baza:

•Većina proizvođača baza podataka imaju dodatne proizvode za unaprijeđenje ugrađenih sustava nadzora (DB auditing):

- Velik broj baza podataka različitih proizvođača i platformi.
- Ugrađeni sustavi nadzora ovisni o pojedinom proizvođaču, vrsti i tipu baze, svaka ima svoj način i logiku rada
- Ugrađeni sustavi nadzora pod kontrolom su DBA te se ne mogu koristiti za nazor samih administratora

•Izvješćivanje (automatizacija i unifikacija) je problematično jer svaka baza ima svoj način rada i alate.

- Većina tih alata oslanja se na ugrđene mehanizme baze te olakšava samo izvješćivanje i pretraživanje. Utjecaj na performanse je jednako kritičan.

1. Nadzor baza podataka. Problemi , zaključci:

IBM

1.Nadzor baza podataka.

Problemi , zaključci:

• Klasični sustavi nadzora nedovoljno sigurni i nezavisni (pod kontrolom DBA, zapisuju u datoteke na samom serveru i slično).
• Potrebno je kupiti zasebne proizvode za svaki tip baze, što je neekonomično, zahtjeva zasebnu obuku za svaki tip baze koji se nadzire.
• Svaki sustav radi na svoj način i nije unificiran niti mogućnostima, niti načinom rada, niti izvješćima koje daje, tj, ne možemo pratiti svaku bazu na isti način i očekivati iste podatke.
• Sve to otežava praćenje toka podataka kada podaci prelaze iz sustava u sustav, te smanjuje mogućnosti nadzora.

1. Nadzor baza podataka. Problemi , zaključci, razmišljanja:

Kako bi trebao izgledati sustav praćenja koji bi zadovoljio potrebe banke:

1.Nadzor baza podataka.

Problemi , zaključci, razmišljanja:

•Kako bi trebao izgledati sustav praćenja koji bi zadovoljio potrebe banke:

- Sustav mora biti jedan, sa podrškom za razne tehnologije i proizvođače baza.(isplativost, unifikacija, pojednostavljena obuka)
- Sustav mora funkcionirati nezavisno od baza te biti pod kontrolom adminstratora sustava a ne DBA. (sigurnost, podjela odgovornosti, nadzor)
- Sustav mora podatke skupljati na način da vrši minimalni utjecaj na performanse sustava, po načelu nevidlivog nadzora koji neće ugroziti postojeći sustav i zahtjevati nova ulaganja i redizajn postojećeg sustava (zaštita postojećih ulaganja.
- Sustav mora omogućiti automatizaciju i unifikaciju izvješćivanja i kontrole preko cijelog skupa servera, bez obzira na vrstu i verziju (bolja kontrola, smanjena mogućnost greške, bolje kontrole.
- Ako je moguće, sustav treba biti reaktivan da može upozoriti Banku da se na bazi događaju aktivnosti koje bi trebalo istražiti. (reaktivna i proaktivna sigurnost, ovisno o pravilima.)

2.Rješenje:
IBM Guardium

IBM

2. Rješenje:

IBM Guardium

- Podržava sve vrste baza podataka i platforme u Banci.
- Koristi vanjski agent koji nezavisno nadzire bazu.
- Izvješćivanje ugrađeno u alat.

2. Rješenje:

IBM Guardium : Podržava sve vrste baza podataka u Banci.

- IBM Guardium podržava Oracle, MS SQL, IBM DB2, MySQL, itd
- Podrška za Windows, Linux, Solaris, AIX, HP UX, z/OS, itd

2. Rješenje:

IBM Guardium: Koristi vanjski agent koji nezavisno nadzire bazu.

- Detaljniji nadzor u odnosu na ugrađeni sustav nadzora u bazama
- Ekvivalent mrežnog “Sniffera” za baze
- Nadzire sav lokalni SQL promet, i detektira sve baze na serveru
- Alati za nadzor i nadzor unificiran za sve baze
- Ne degradira performanse sustava
- Ne traži promjene na bazama
- Separacija odgovornosti za nadzor i održavanje baze

2. Rješenje:

IBM Guardium: Izvješćivanje ugrađeno u alat.

- Olakšava postizanje usklađenosti sa zakonodavstvom, pravilnicima i pravilima struke
- Predefinirani izvještaji
- Automatizacija izrade izvješća i automatsko slanje
- Unifikacija izvještaja i izvještajnog procesa
- Forenzički alati za pretraživanje događaja
- Slanje upozorenja u realnom vremenu baziranih na složenim logičkim uvjetima

3.Implementacija:

3. Implementacija:

- Guardium server je virtualni uređaj – jednostavna implementacija.
- Instalacija osnovnog agenta na krajnje servere baza podataka
- Instalacija i daljnje održavanje ostalih komponenti nadzora sa centralne administrativne konzole

3. Implementacija:
Važne napomene:

- Kvaliteta nadzora izravno ovisi o kvaliteti postavljenih politika i filtara: potrebno je biti pažljiv da se postigne dobar balans između količine i kvalitete podataka.
- Dobra vijest: nije teško, već dolazi prirodno sa korištenjem sustava.
- Vrlo brzo prihvaćanje rada sa sustavom

3. Implementacija:

• BKS Bank d.d. je početnu implementaciju sustava povjerio tvrtci Etna d.o.o., koja je instalirala Guardium server, izvršila početnu instalaciju agenata na servere i početno podešavanje sustava skupljanja podataka.
• Tjekom tog procesa djelatnici Etne izvršili su početnu obuku djelatnika BKS Bank d.d. tako da mogu samostalno nastaviti sa održavanjem i korištenjem sustava.
• Na taj način postignute su značajne uštede u vremenu u odnosu na pokušaj samostalne implementacije svih faza sustava.
• Od instalacije do početka korištenja u 10 dana.

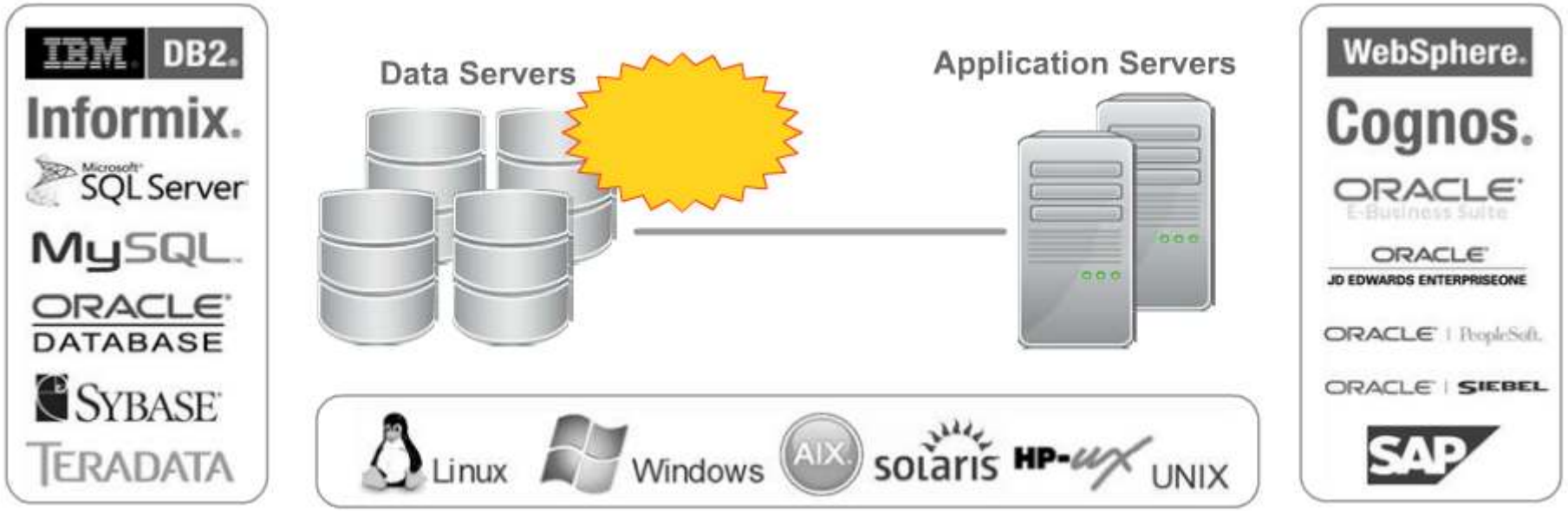
IBM SolutionsConnect 2013
Dan pametnijih rješenja

Guardium:

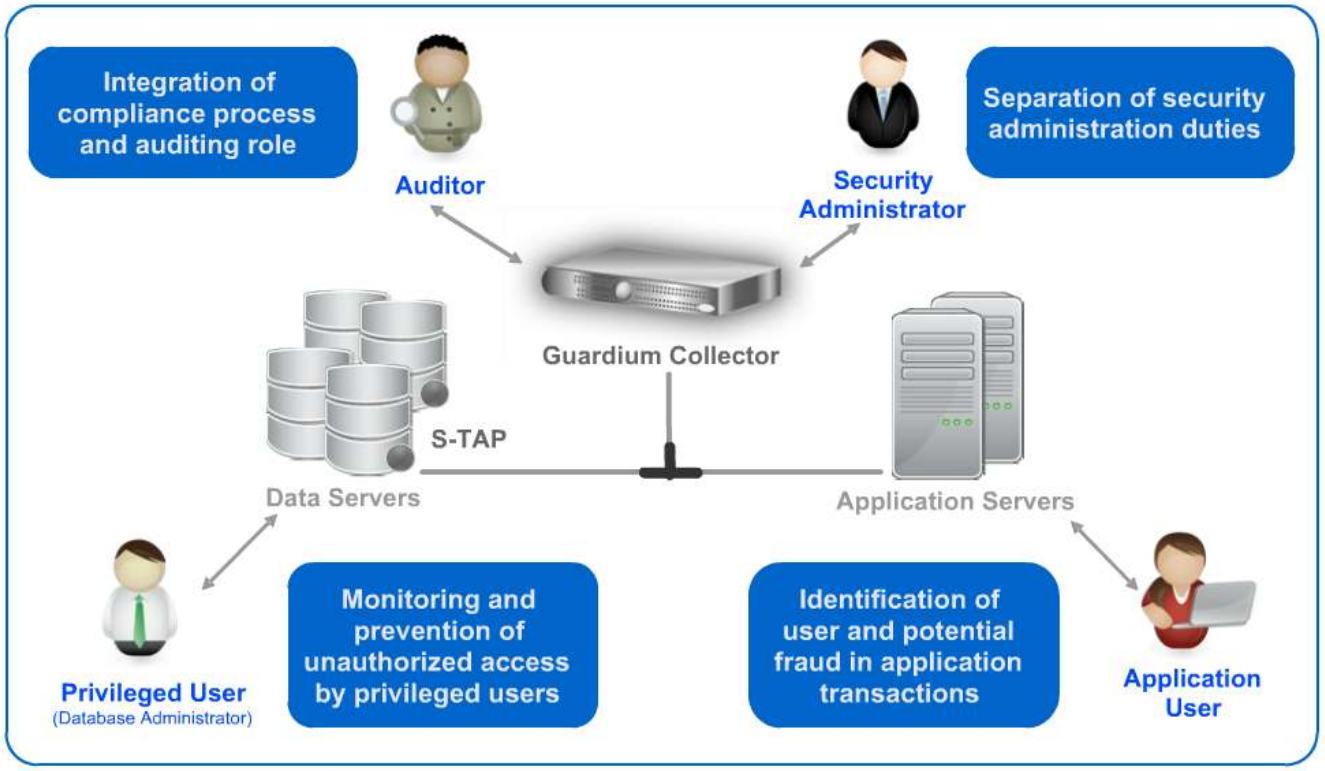
Kratki tehnički sažetak.

IBM

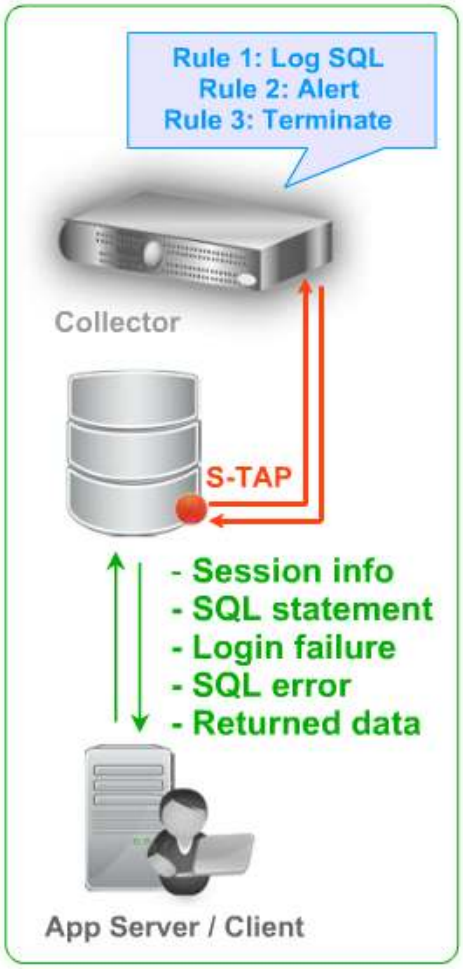
Kompleksno okruženje



Korisnici i prijetnje



Inspection engine and Logging



Informacije koje S-TAP može slati Guardium kolektoru:

- *session information*
- SQL *statement*
- Login *failures*
- SQL greške
- *Returned data*

Primjer:

TOMA QUERY v1 (SQL)

Start Date: **2013-05-27 08:46:49** End Date: **2013-05-27 11:46:49**
Aliases: OFF

Timestamp	Database Name	Client IP	Server IP/Server Port	DB User Name	Source Program	OS User	Sql
2013-05-27 11:48:35.0	[redacted]	192.168.1.57	192.168.1.2+50000	[redacted]	DB2BP.EXE	TOMA	SET CLIENT APPLNAME ?
2013-05-27 11:48:35.0	[redacted]	192.168.1.57	192.168.1.2+50000	[redacted]	DB2BP.EXE	TOMA	SET CLIENT ACCTNG ?,X?
2013-05-27 11:48:35.0	[redacted]	192.168.1.57	192.168.1.2+50000	[redacted]	DB2BP.EXE	TOMA	select * from db2admin.banka

S-GATE

- dodatan sloj protekcije baze podataka
- služi za terminiranje konekcije
- S-GATE može raditi u dva načina rada
  - Open Mode
  - Closed Mode (S-TAP Firewall Mode)
- potrebna dodatna licenca

HVALA !

Siniša Babić – CISO BKS Bank d.d.
sinisa.babic@bks.hr
Marko Gustović – Voditelj IT BKS Bank d.d.
marko.gustovic@bks.hr
Tomislav Mihelić – CISO ETNA d.o.o.
tomislav.mihelic@etna.hr

IBM

Thank You