

IBM WebSphere DataPower

Učinkovit način procesiranja sporočil in izkoriščanja potencialov arhitekture SOA

Osnovni namen tehnologije IT v podjetju je podpora poslovnim procesom. Elektronsko poslovanje služi poenostavitvi in pospeševanju izvedbe delovnih nalog ter olajšuje komuniciranje tako znotraj podjetja kot s poslovnimi partnerji in kupci. Pri razvoju infrastrukture IT v podjetju pa stvari postajajo vse bolj kompleksne. Prihaja do težav zaradi uporabe različnih tehnologij in komunikacije med njimi.

Tehnologije, ki temeljijo na odprtih standardih, že danes omogočajo povezovanje različnih okolij, vendar se pri povezovanju vedno postavi vprašanje, katero tehnologijo uporabiti, da bomo dosegli zastavljene cilje. Pomembna je enostavnost rešitve in primernost za vse vpletene partnerje, kar je težko zagotoviti, če upoštevamo dejstvo, da se partnerji običajno zavzemajo za uporabo tehnologije, ki jo že poznajo. V zasledovanju tega cilja se mnogokrat pozablja na varnost in zanesljivost ter uporabo odprtih standardov.

Kompleksnost obdelave dokumentov XML

Konec devetdesetih let je bila razvita tehnologija XML, ki omogoča prenosljivost podatkov ne glede na izbrano okolje. Uporaba te tehnologije se širi predvsem na področju elektronske izmenjave podatkov in elektronskega trgovanja, povezovanja poslovnih sistemov, objavljanja in shranjevanja informacij ter razvoja programske opreme. S širitvijo tehnologije XML raste potreba po shranjevanju dokumentov XML. Pri pretvorbi teh dokumentov v ustrezno obliko za shranjevanje v podatkovnih bazah običajno prihaja do težav. Ker obstajajo različne oblike dokumentov XML, je potrebno pri ravnanju z njimi uporabljati različne pristope. Obdelave dokumentov XML se izvajajo na aplikativnih strežnikih, kar povzroča dodatne stroške administracije, povezane s strojno opremo, predvsem pa nastajajo stroški na področju programiranja, vezanega na obdelavo dokumentov XML. Programerji se soočajo s problemi zagotavljanja varnosti

podatkov (nepooblaščenim vpogledi v vsebino dokumentov) ter s problemi zaščite pred vdori (poskusi ohromitve omrežja s pošiljanjem velikih količin sporočil, vrivanje programske kode v dokumente XML ...).

Vse naštetu botruje iskanju novih pristopov k reševanju kompleksnosti uporabe rešitev, ki so bile v osnovi razvite za reševanje kompleksnosti povezav med različnimi tehnologijami.

Kaj je DataPower?

DataPower je ime za skupino naprav, ki primarno služijo pospeševanju procesiranja dokumentov XML in sodijo v družino produktov IBM Websphere. Te naprave varujejo, pospešujejo in usmerjajo XML z namenom, da bi organizacije na stroškovno učinkovit način polno izkoristile potencial sporočilnih sistemov in arhitekture SOA.

V osnovi so naprave DataPower služile zgolj obdelavi dokumentov XML. Za razliko od programskih paketov, ki se običajno uporabljajo pri obdelavi dokumentov XML, imajo te naprave vgrajene strojne elemente za obdelavo. Zaradi specializiranega hardvera so naprave DataPower hitrejšje od podobnih programskih rešitev, delujejo namreč z omrežno hitrostjo.

S časom so se v naprave vgradile tudi možnosti obdelave drugih tipov podatkov, kot so binarni podatki, tekstovne datoteke, COBOL Copybook, ISO8583, ASN.1. Naprave lahko komunicirajo z zunanjimi sistemi, kot so baze

podatkov, MQ ali CICS. Podprti so enkripcija podatkov in digitalni podpis ter različni protokoli in mehanizmi za kontrolo dostopa (SAML, XACML, WS-Security, LDAP, SSO), kar omogoča pogoje za nemoteno poslovanje v smislu varnosti in verifikacije podatkov.

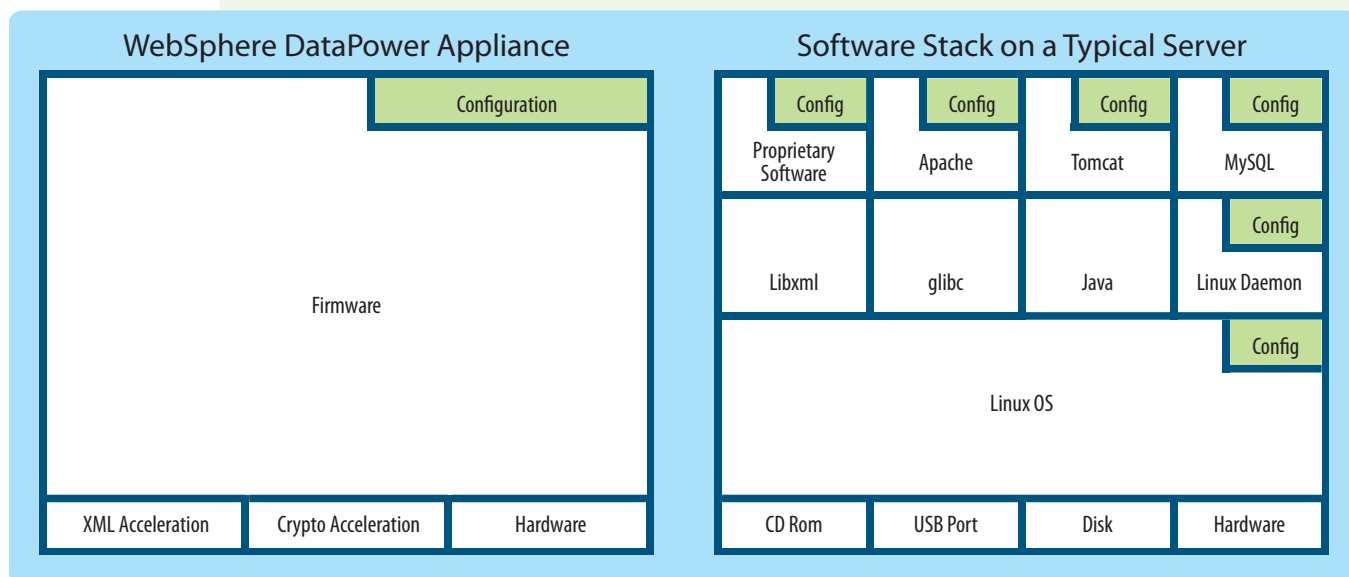
Sama naprava predstavlja tipično appliance - black box rešitev, ki se priklopi na lokalno omrežje. Konfiguracija je enostavna in vzame malo časa, upravljanje pa je mogoče centralizirati in na ta način olajšati administracijo. Omogočenih je več načinov upravljanja (Web GUI, CLI, scriptable Web services).

Naprava obdeluje sporočila glede na vnaprej definiran skupek pravil, ki so razdeljena v kategorije zahtev in odgovorov. Vsako pravilo je sestavljeno iz niza akcij, ki se opravljajo pri izvajanju pravil. Obstaja preddefiniran niz akcij, kot so validacija dokumentov XML, izvajanje transformacij XSLT, pošiljanje sporočil v MQ, logiranje, kriptiranje podatkov, pošiljanje sporočil na strežnik FTP in podobno.

Po podatkih IBM-a je izmerjen prenos sporočil XML nekje med 200 in 700 Mbit/s s povprečjem 300 Mbit/s ob uporabi enega pravila za izvedbo transformacij. Bolj kompleksno kot je pravilo, počasnejši je prenos. Procesiranje sporočil traja nekje med eno in desetimi milisekundami. Kapaciteta ene naprave je do 1000 transakcij na sekundo in lahko podpira do 25.000 sočasnih povezav TCP.

Slika 1: WS Security Gateway XS40.





Slika 2: Primerjava strukture naprave DataPower s programsko rešitvijo.

Ogromna količina podatkov, ki jo je naprava sposobna obdelati v kratkem času, pomeni tudi večjo grožnjo z vidika varnosti. Organizacije za zagotavljanje varnosti lokalnega omrežja običajno postavljajo požarne zidove, ki pa v primeru dokumentov XML niso najbolj zanesljivi. DataPower zato ponuja rešitev v obliki naprave (WS Security Gateway XS40), ki med drugim izvaja funkcijo požarnega zidu XML.

Požarni zid XML

Varnost je eden od najpomembnejših faktorjev pri planiranju arhitekture SOA. Že eno samo sporočilo XML se lahko izogne tradicionalnim varnostnim mehanizmom in ogrozi delovanje kritičnih poslovnih aplikacij.

WS Security Gateway XS40 je XML proxy, ki pregleduje vhodne zahteve in zavrača tiste, ki so neustrezni ali celo škodljivi. Na ta način ščiti strežnike back-end pred različnimi napadi XML. Povečevanje števila aplikacij v spletnih storitvah in arhitekturi SOA pomeni večjo izpostavljenost specifičnim grožnjam XML. Požarni zid XML pomaga pri zaščiti proti XPath injection, SQL injection in drugim tipom XML ranljivosti sistema. Pri tem izvaja varnostne preglede:

- preverjanje ustreznosti formata dokumenta XML,
- validacija dokumentov XML,
- zaščita pred ohromitvijo omrežja,
- filtriranje sporočil XML
 - na nivoju metod WSDL,
 - preko XPatha,

virtualizacija spletnih storitev,

- monitoriranje sporočil (SLA),
- limitiranje števila transakcij na časovno obdobje.

Vse varnostne funkcije XML, kot na primer validacija dokumentov XML, filtering XML in transformacije dokumentov XML zahtevajo intenzivno procesiranje XML, ki porabi veliko resursov, zato se morajo podjetja pogosto odločiti med zmogljivostjo in zaščito. Polna zaščita prometa XML namreč zahteva procesno moč, ki v tradicionalnih rešitvah ni na voljo. Patentirana DataPower tehnologija XG3 omogoča procesiranje dokumentov XML z omrežno hitrostjo. To pomeni, da je mogoče vključiti več potrebnih varnostnih funkcij za zagotavljanje višje ravni varnosti.

DataPower naprave se glede na osnovno namembnost delijo v nekaj kategorij:

- pospeševanje obdelave dokumentov XML – **XML Accelerator XA35**
- zagotavljanje varnosti dokumentov XML in spletnih storitev – **WS Security Gateway XS40**
- pospešitev obstoječih integracijskih vozlišč – **Integration Appliance XI50**
- B2B gateway (podpora standardov za prenos v formatu EID-INT) – **B2B Appliance XB60**
- prenos velikih količin sporočil brez zamud – **LLM (low latency messaging) Appliance XM70**

Pri prvih treh napravah vsaka naslednja vsebuje vse funkcionalnosti predhodne.

Prednosti naprav DataPower pred tradicionalnimi programskimi rešitvami

Ker gre pri DataPower za strojno rešitev, zagotavlja višjo raven zanesljivosti, varnosti in zmogljivosti. Naprava je optimizirana tako v smislu strojne kot programske opreme in firmvera. Prednaložen operacijski sistem je enostaven, specializiran in ne vsebuje nobenih nepotrebnih funkcij. S tem se zmanjšuje ranljivost samega sistema z vidika varnosti in s tem povezanih stroškov nadgradenj. Sistem je popolnoma varen (nobenih odprtokodnih rešitev, trojanskih konjev, Java/C++ knjižnic).

Naprava vsebuje manj gibljivih delov (nima vgrajenega trdega diska), kar povečuje zanesljivost delovanja. Nima USB portov in optične enote, kar izniči možnost zagona škodljive programske opreme, ki bi lahko ogrozila celoten sistem.

Uporaba naprav DataPower

DataPower se uporablja praktično v vseh IT okoljih, kjer je prisotna uporaba standarda XML. Po svetu je bilo uspešno izvedenih več projektov na področju telekomunikacij, bančništva, zavarovalništva, zdravstva in gospodarstva. Rešitev je dejansko primerna za vsa podjetja in organizacije, ki so že ali želijo standardizirati povezave v okolju IT.

Primer rešitve pri stranki: večje telekomunikacijsko podjetje

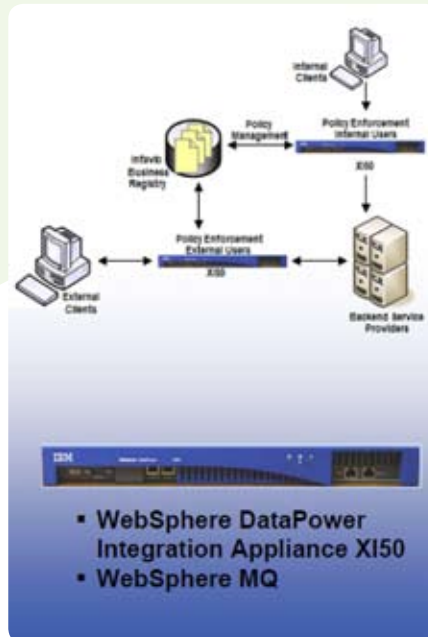
Osnova za projekt je povezava različnih tehnologij v interni infrastrukturi IT in izvrševanje pravil koncepta SOA.

Zahteve

Stranka želi postaviti ESB (enterprise service bus), ki bo zagotavljal varnost sporočil in funkcije prenosa na zanesljiv način, z možnostjo nadgradnje, medtem ko so stroški postavitve, razvoja in upravljanja minimalni.

Rešitev

Postavitev dveh naprav DataPower XI50 (v DMZ in notranje omrežje):



Slika 3: ESB in izvrševanje pravil SOA.

- XI50 sprejema promet HTTP/SOAP in zagotavlja upoštevanje pravil pri zunanjih uporabnikih,
- izvaja filtriranje in validacijo vhodnega prometa XML ter avtentikacijo in avtorizacijo uporabnikov,
- skrbi za usmerjanje sporočil na ustrezne naslove glede na vnaprej definirana pravila,
- omogoča pretvorbo XML-a v binarno obliko,
- omogoča prenos med HTTP, SOAP in MQ.

Koristi

Stranka dobi ESB, ki je nadgradljiv ter enostaven za postavitev, konfiguracijo in upravljanje.

Hitrejši čas izdelave storitev omogoča stranki, da dosega zastavljene roke.

Večanje potreb po napravah DataPower je tesno povezano s širitvijo tehnologije XML, za katero lahko rečemo, da je eden od najbolj razširjenih standardov na področju sporočilnih sistemov. Poleg tega trg potrebuje enostavne, varne in učinkovite rešitve, ki bodo odločilno pripomogle k optimizaciji okolja IT v podjetju in s tem posledično k optimizaciji poslovnih procesov.

Marko Velečič

DataPower in SRC

Podjetje SRC je uradni prodajalec naprav IBM WebSphere DataPower. Imamo certificirane strokovnjake za svetovanje, prodajo in tehnično izvedbo implementacije in vzdrževanja. Trenutno izvajamo testiranja naprave DataPower Integration Appliance XI50. Za natančnejšo predstavitev nas lahko kontaktirate in dogovorili se bomo za obisk.



Pametne rešitve za boljši jutri.
Bright Solutions for a Brighter Future.

