Appliances and SOA Security; DataPower and Z Integration

Rich Salz
IBM

August 5, 2010
Session 7661
Agenda

- DataPower SOA Appliances
  - Products
  - Uses
- DataPower and Z
  - Subsystems
  - Load Distribution and High Availability
  - Security
  - Management
  - Tooling
- Summary
DataPower SOA Appliances
Why an Appliance for SOA?

- Integrated
  - Many functions integrated into a single device
  - Addresses the divergent needs of different groups (architects, operators, developers)
  - Integrates well with other IBM SWG and standards-based products

- Hardware reliability
  - Dual power supplies, no spinning media, self-healing capability, failover support

- Security
  - Higher levels of security assurance certifications require hardware (HSM, government criteria)
  - Inline application-aware security filtering and intrusion protection

- Higher performance with hardware acceleration
  - Wire-speed application-aware parsing and processing
  - Ability to perform costly XML security operations without slow downs

- Consumability
  - Simplified deployment and management: up in minutes, not hours
  - Reduces need for in-house SOA skills & accelerates time to SOA benefits
DataPower Architecture

Specialized compiler technology creates optimized executable object code from transformations (e.g., XSLT) that execute natively on hardware.

Everything is viewed as a transformation that is extensible via DataPower custom extension functions.

High-performing throughput-optimized engine yields wire-speed capabilities.

Purpose-built hardware to execute SOA workloads and transformations.
DataPower SOA Appliances Product Family

Low Latency Appliance XM70
- High volume, low latency messaging
- Enhanced QoS and performance
- Simplified, configuration-driven approach to LLM
- Publish/subscribe messaging
- High Availability

Integration Appliance XI50
- Hardware ESB
- “Any-to-Any” Conversion at wire-speed with WTX
- Bridges multiple protocols
- Integrated message-level security

B2B Appliance XB60
- B2B Messaging (AS2/AS3)
- Trading Partner Profile Management
- B2B Transaction Viewer
- Unparalleled performance
- Simplified management and configuration

XML Security Gateway XS40
- Enhanced Security Capabilities
- Centralized Policy Enforcement
- Fine-grained authorization
- Rich authentication

Aug 4, 2010 17:53
Advantages of a DataPower Blade

- First-class support of new features: IPv6, 10GigE, XG4NG
- Increased load distribution and high availability options for optimized application support
- Configuration transparency: 1U and blade
- Opportunities for additional future integration
Use Cases

Monitoring and control
Example: centralized ingress management for all Web Services using ITCAM SOA

Deep-content routing and data aggregation
Example: XPath (content) routing on Web Service parameters

Functional acceleration
Example: XSLT, WS Security

Application-layer security and threat protection
Example: XML Denial-of-Service protection, WS Security

Protocol and message bridging
Example: Convert between WS and legacy Cobol/MQ
Deployment Scenarios

1. Helps protect against incoming attacks;
   Incoming access control

2. Outgoing access control, SAML injection, role mappings

3. Internal security

4. Web services management

5. Legacy transformation

- **federated extranet**: legacy enterprise application, SOA platform, XI50
- **Internet**: Internet user, Packet Filter, XS40
- **intranet**: internal user, Packet Filter, XS40

- **SOAP enabled enterprise application**
- **SOA platform**
DataPower and Z: Subsystem Integration
Integration Goals

• Enable Web Services interfaces to z Subsystems
• Enhance communication mechanisms and intelligence
  – Load distribution and high availability choices and optimizations
• Allow integrated and centralized security
  – Promote System z as the enterprise-wide security focal point
• Integrated system administration and monitoring
• Holistic approach focusing on all aspects of the SOA Lifecycle
• Unified map tooling
  – Used to build binary transformations, e.g. Cobol Copybook
IMS Integration (1)

Web Services Security and Management for IMS Web services

- Content-based Message Routing
- Protocol Bridging (HTTP, MQ, JMS, FTP, etc.)
- XML/SOAP Firewall
- Data Validation
- Field Level Security
- XML Web Services Access Control/AAA
- Web Services Management
IMS Integration (2)

- DataPower provides WS-enablement to IMS applications
- Customer codes schema-dependent FFD or WTX data map to perform request/response mapping
- This is the preferred way to WS-enable IMS applications
- Requires MQ
  - MQ bridge to access IMS
  - MQ client is embedded in DataPower
  - Some push back against MQ requirement due to cost and complexity issues
IMS Integration (3): WS-Enablement

- Remove MQ requirement
  - MQ still best alternative for scenarios requiring transactional support
  - IMS has few alternatives (IMS SOAP Gateway is an entry-level solution)
- “IMS Connect Client” (back-side handler) natively connects to IMS Connect using its custom request/response protocol
- 3.8.0 adds: Automatic chunking and de-chunking
- 3.8.1 adds: Commit mode 1, Sync level commit support
IMS Integration (4): IMS Proxy

- Bring DataPower value add to standard IMS connect usage patterns
- Provide an “IMS Connect Client” on DataPower that natively connects to IMS Connect
- Provide an “IMS Connect Server” on DataPower that accepts IMS Connect client connections and provides an intermediation framework that leverages DataPower
  - Enables authentication checks, authorization, logging, SLM, transformation, route, DB look-up, SSL offload, etc.
**DB2 Integration (1)**

- Supports DB2, Oracle, Sybase, Microsoft
  - Parameter marking
  - Array-based operations
  - Perf enhancements
  - Stored procedures
  - Native XML processing

- Web service requests are augmented with information from the database (message enrichment)

- Supports writing to DB also
  - Logging and auditing

---

**Diagram:**

- Service Originator → SOAP/HTTP → DataPower → DB2 → SOAP/HTTP → Service Provider

- Service request

- Augmented service request
DB2 Integration (2)

- A standard WS façade to DB/2
  - Common tool (IBM Data Studio 1.2) generates WSDL and data mapping in both Data Web Services runtime and DataPower
  - SOAP call is mapped to an ODBC (DRDA) invocation
- Exposes database content (information) as a service
CICS Integration (1)

Web Services Security and Management for CICS Web services

- Content-based Message Routing
- Protocol Bridging (HTTP, MQ, JMS, FTP, etc.)
- XML/SOAP Firewall
- Data Validation
- Field Level Security
- XML Web Services Access Control/AAA
- Web Services Management
- 3.8.0 adds: ID propagation
CICS Integration (2)

- DataPower provides WS-enablement to CICS
- Customer codes schema-dependent XSL/FFD/WTX to perform request/response mapping
- Requires MQ
  - MQ bridge to access CICS
  - MQ client capability is embedded in DataPower
CICS Integration (3)

- DataPower provides WS Security, XDoS to CICS WS back-end
- User creates schema-dependent transform to perform request/response mapping
- Payload transformation is pushed to DataPower
- SOAP Header information required at CICS WS back-end for correct operations, e.g. WS-AtomicTransactions
DataPower and Z
Load Distribution and HA
Application Optimization (AO): Self-Balancing and high availability HA of Appliances

Front-end IP load balancers not needed for AO workloads

Self balancing (IP spraying)

Active/Passive failover of distributor using standby control

Failure of target appliances are masked by appropriate weighted distribution

Clients

Service Provider
AO Intelligent Load Distribution (ILD)

- Request distribution, *not* connection distribution
  - This provides better distribution under persistent connections
- Today: WAS ND and VE are supported

Tier 2 Distribution using intelligent dynamic back-side load distribution

Dynamic back-side information from target environment (here, WAS via On-Demand Configuration-ODC)
Distribution and HA Options Today

Tier 1 distribution options:
- DataPower Self Balancing
- Fronting IP Sprayer

Tier 2 distribution options:
- Sysplex Distributor
- DataPower load distribution
- DataPower ILD (ODC)

Red = Connection distribution; Black = Request distribution
Emerging Distribution and HA Strategies

New in 3.8.0

Tier 1 distribution options

DataPower Self Balancing

Tier 2 distribution options

DataPower load distribution

Sysplex Distributor

Red = Connection distribution;
Black = Request distribution

Clients

Tier 1

DataPower Tier

Tier 2

DataPower ILD

Sysplex Distributor

ODC

ODC

SASP

z/OS

z/Linux

Any service provider on p or x

ASB

WebSphere on p or x

zBX

WebSphere on z/OS or z/Linux
DataPower and Z: Security Integration
NSS provides remote interface to RACF for I&A, and access control requests. Can request RACF certificate name filtering. z/OS R10.

Request NSS on z/OS to identify and access administrative users and to perform access control operations when access to DataPower resources is requested. GA 3.7.2.

Remote SAF Security Integration

NSS client

Target application or middleware

Client platform

TSOM

Audit records

RACF

RACF Users and resources

z/OS

NSS

I & A, AC req resp

SHARE in Boston
Request NSS on z/OS to perform operations that require access to RACF keyring. This includes signing, validating signatures during security initialization, key unwrapping, and key downloading.

NSS performs requested key operation using certificates and keys stored in RACF.
DataPower and Z: Management Integration
Management Integration

• Monitoring - many different “levels” of monitoring, all are important
  – System-level monitoring (CPU, memory, SNMP)
  – Service-level monitoring (WS, SOAP, WSDM)
  – Business-level monitoring (Key performance indicators, BPEL)

• Operational management
  – Configuration lifecycle management: Need to manage disparate configuration assets in the deployment lifecycle (development through production)
  – Control firmware upgrades

• Runtime management
  – How can we dynamically configure and affect DataPower in collaboration with other runtimes in our enterprise?
  – Peer-to-peer approach vs policy-driven approach: both are important
Monitoring Overview

Integrated Console
- Allow for seamless views across different layers of abstraction.

Integrated Reporting
- Generate enterprise-wide service level reporting
Thoughts on Operational Management

- Configuration management is an integral part of the Appliance Development Lifecycle
- Appliance Management Protocol (AMP) provides an appliance-generic SOAP interface for configuration deployment and firmware governance
  - Built on the notion of a configuration (domain) package (export)
  - Example: Full-device backup and restore primitive
- DataPower Management Interface (DeMI) is a java based component that provides consistent higher level functions for broader multi-appliance management support
  - DeMI is embedded in WAS and ITCAMSE
DataPower and WMB

- Exploit DataPower for WS Security
  - Single tool and security policy description
  - Security best practices
    - WS-Security at appropriate point in topology
    - Built-in XML threat protection; Hardened device
  - Built-in service level management
    - Manage traffic using policy; WSDM and WS-Man
  - Scale as volumes increase
    - Enhanced performance with SOA appliance
    - Add capacity when necessary
- Administration User Experience
  - Operational reconfiguration only
  - Applications and Message Flows unchanged
  - Right click on flow and select “Use DataPower”
    - DataPower performs WS-Security processing
    - Forwards processed request to MB
AO Dynamic WebSphere Configuration

- Session Affinity
- WebSphere Cell: AutoWCC
- Workload Management Group Name: xyzCluster
- Protocol: HTTP
- Damp Time: 120
- Do not Bypass Down State: on
- Try Every Server Before Failing: on
- Masquerade As Group Name: on
Web Services Registry and Repository

- Use of a central repository can facilitate Discovery and Reuse of Web services:
  - WSRR and UDDI supported today
- Artifacts can be stored, updated via repository
- Push/Retrieve configuration of new services to DataPower for enforcement
- Policy and Security enforcement for SOA Governance on DataPower
- Direction: Increased types of Policy (e.g. QoS/SLA)
DataPower and Z: Tooling
1. Client develops transformations in DP mode
2. Client chooses compile/execute from WTX Design Studio
3. Map Designer transmits transformations to the XI50
4. DataGlue engine runs, returning any errors back to WTX Design Studio
5. DataGlue loads the transformations
6. Transformation executes
7. Logs and output are transferred back to WTX Design Studio for examination
Summary – IBM SOA Appliances and System z

• DataPower improves System z resources
• Integration increases collaborative synergy across DataPower and z platforms
• Broad integration with System z
  – Subsystem: Higher performance with hardware acceleration
  – Networking: Comprehensive load distribution and HA options
  – Security: Higher levels of security assurance certifications require hardware
  – Management: Simplified deployment and ongoing management
  – Tooling: Consistent tooling across IBM product family

http://www.ibm.com/software/integration/datapower/

SOA Appliances: Creating customer value through extreme SOA performance and security

- Simplifies SOA with specialized devices
- Accelerates SOA with faster XML throughput
- Helps secure SOA XML implementations