GSB OVERVIEW

IBM WebSphere Data Power SOA Appliances are purpose-built, easy-to-deploy network devices that simplify, secure, and accelerate your XML and Web services deployments while extending your SOA infrastructure. Data Power provides configuration-based approach to meet MOICT's edge ESB requirements. The DataPower Appliance provides many core functions to applications, such as service-level management, routing, data and policy transformations, policy enforcement, access control, and hardened security—all in a single "drop-in" device.

For MOICT, Data Power provides the following key benefits.

- Platform for Vertical e-Services integration: Web services from different government entities (service providers) can be securely exposed using Data Power.
- Cross Organizational e-Services Platform: Data Power provides role-based access control to ensure the right level of secure access for cross-organizational e-Services.
- Composite e-Services integration platform: Data Power is the service composition layer that exposes composite services to service consumers.
- Shared e-Services integration platform: Data Power supports modular service integration architecture.

When deploying this IBM appliance in your network, you secure your enterprise at the Application Layer vs. at the Network Layer. DataPower is a next-generation appliance that operates on MESSAGES instead of PACKETS. This enables offloading security checks and structural checks from the service providers, there by simplifying integration while minimizing performance degradation.

SOLUTION BENEFITS

Using IBM DataPower as the ESB appliance, this provides the following benefits:

- Ease of implementing security and web services in a purpose-built appliance resulting in reduced Development Lifecycle and implementation costs.
- Configuration, rather than coding: This approach offers faster time to market compared to traditional coding approaches for service integration.
- Offloading tedious security tasks from Sevice Providers (Government entities), preventing potential performance degradation

- Appliance approach provides greater security compared to software based solutions (removes periodic operating system patches, OS vulnerabilities, virtualization layer vulnerabilities, regular software patches, etc.)
- Purpose built firmware, offering wire-speed processing.
- Prepare your environment for the future: DataPower is ready for mobile and web 2.0
- Extensible architecture: add-on modules can be turned on as required.
- Highly fault tolerant device (multiple power supplies, multiple network ports) with in-built load balancing & clustering options.

The DataPower Appliance is purpose-built, easy to consume and easy to use. DataPower delivers security, common message transformation, integration, and routing functions in a network device. IBM approach helps you to leverage and scale your existing infrastructure investments.

SOLUTION COMPONENTS AND FEATURES

The below sections lists the used components and the utilized features within the Data Power appliance during the implementation of the Edge ESG to help meet MoICT requirements:

- **Logging**

  IBM Data Power appliance offers a bunch of different options when it comes to logging. MOICT's main concerns when it came to logging were:

  - <u>The ability to troubleshoot a problem when one arises:</u> As for this point in the solution IBM Data Power offers a feature called 'debug probe', this feature can be enabled to log the messages temporarily and then view them at each stage within the policy execution, this also offers information like the requested and source URL/IP which should be sufficient when a problem arises at the message level.

- Being able to view and track events as they occur (mostly errors): As for this DataPower's out of the box logging behavior should suffice, it offers the ability to filter the logs based on the component from which they originated and the ability to increase and decrease the level of logging details based on the current need.

- DataPower auditing: Out of the box, DataPower offers the ability to log any administrational actions, by which user where they performed and when (this also included some lower level relevant action logging).

- **Security using SSL certificates**

  When it comes to SSL, the solution includes two different implementations:

  - Standard SSL over HTTP (for G2G services)

    In this scenario DataPower is issued a certificate which the service consumers should trust and accordingly be able to authenticate DataPower boxes and perform transport layer encryption. As for between DataPower and the service providers, DataPower should receive a copy of the public certificate of the entities it will connect to in order to trust them.

  - SSL with mutual authentication (for G2B services)

    As for this scenario the communication with the backend services is still done in the same manner but the communication with the consumers is done differently. In this case the first part still stands true where DataPower is still issued a certificate which the service consumers should trust but the difference is that the service consumers themselves should also be issued certificates which the DataPower should receive (public certificates) in order to perform a mutually authenticated connection.

  Mutual authentication or **two-way authentication** (sometimes written as 2WAY authentication) refers to two parties authenticating each other at the same time. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

  As for the certificates issuing three different options were discussed:

  - Purchasing internationally trusted certificates

  - Using the new Jordan PKI to issue new certificates (in the future)

  - Using self-signed certificates (this option will not be used)

  DataPower supports four different formats when it comes to certificates and key:

- DER
- PEM
- PKCS #8
- PKCS #12

Note: DataPower offers notifications for the box administrators/developers when an SSL certificate is going to expire within a month to insure minimized service downtime and a minimal impact of this event.

- **Web services proxy**

  A 'Web Service Proxy' provides security and abstraction for remote web services. It is the object where most of the implementation will be performed and where the majority of the other features are contained. A Web Service Proxy makes it easier to implement certain features for web services based on a WSDL file.

  The first step of implementing a web service in DataPower is always obtaining the WSDL (by uploading to the device or fetching from WSRR), after doing so the Web Service Proxy starts offering options starting with specifying the end point to be exposed and the protocol to be used. After that one can start applying the required policy. In the current scenario we have two policies to be applied per service the first (client to server) at the service level and another policy to apply on the way back but on a lower level and that is the operation level.

  On the client to server policy:

  - Within the AAA action the service credentials will be extracted from the message (Password-carrying UsernameToken element from WS-Security header), this identity will be validated against LDAP to decide whether the consumer is eligible to consume the service based on whether the identity is a member of the service group or not.
  - At this stage the SLA is enforced.
  - An attribute containing the identity's access level to the services is queried and stored in context variables.
  - The identity within the message is replaced with another identity which is meant to authenticate DataPower boxes at the service provider's side.
  - The destination URL is replaced with the actual service provider's URL instead the one that came with the message here.

  On the way back (server to client) each response to a consumer is filtered based on the consumer's access level to a service using a transformation action (an XSLT style sheet) and finally the response is returned to the consumer here.

PRODUCTION

The production environment will include the following components:

- IBM Data Power Gateway Appliance
- IBM WebSphere Service Registry and Repository (WSRR)
- IBM DB2 (for WSRR web service meta data)
- IBM Smart Cloud (Monitory and data ware house servers)
- LDAP (Microsoft Active directory)

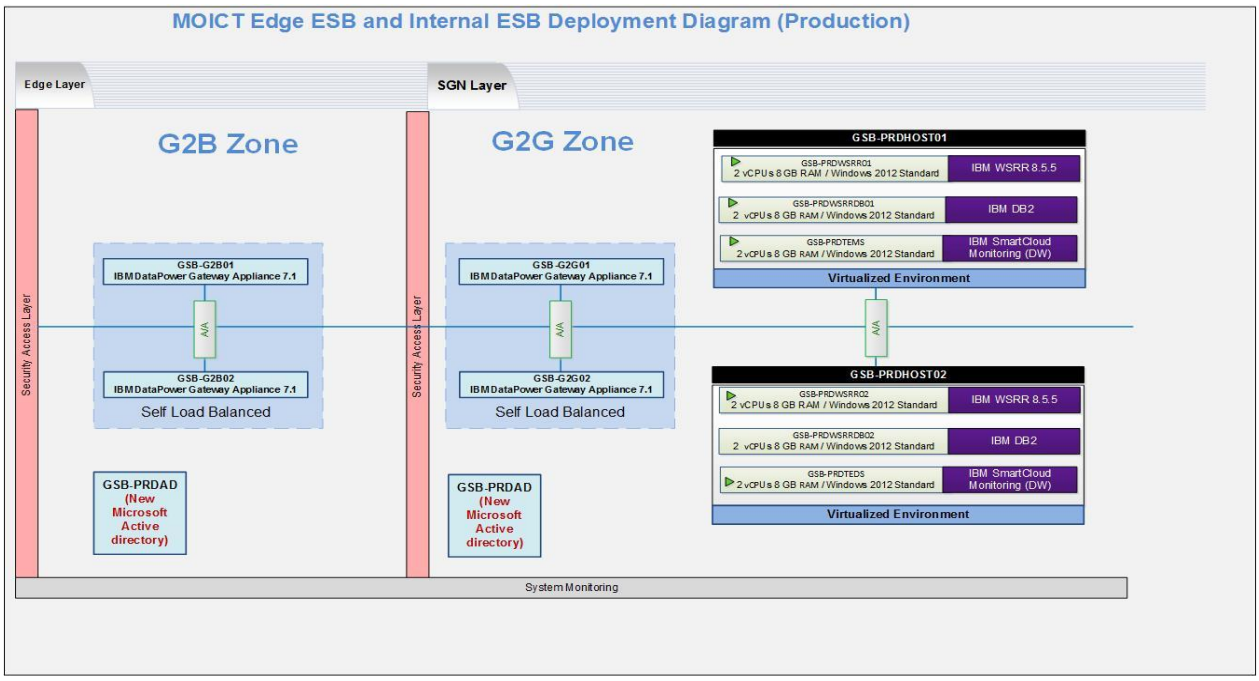
The WSRR will be deployed into two virtual servers running in active/active mode using clustering which is based on the WebSphere Application Server ND capability.

There will be a network load balancer in front of the WSRR nodes to load balance and handle failover scenarios and the DataPower appliances will connect with the WSRR using the NLB.

IBM SmartCloud Monitoring (formerly known as IBM Tivoli Composite Application Manager) provides monitoring of system parameters, and provides service usage graphs and reports (for example, web service invocation graphs, round trip times, total duration, etc.)

The WSRR will be configured with the DB2 for the configuration of the WSRR and web services Meta data, this DB2 will be deployed in active/passive mode using windows cluster technique.

The below diagram shows the main components in the production environment for both the G2G and G2B:



The two DataPower appliance in the G2G will be configured to self-load balanced between each other and will be connected to two VLANs, one will be used for the management of the appliances and the other will be used for the data in the SGN.

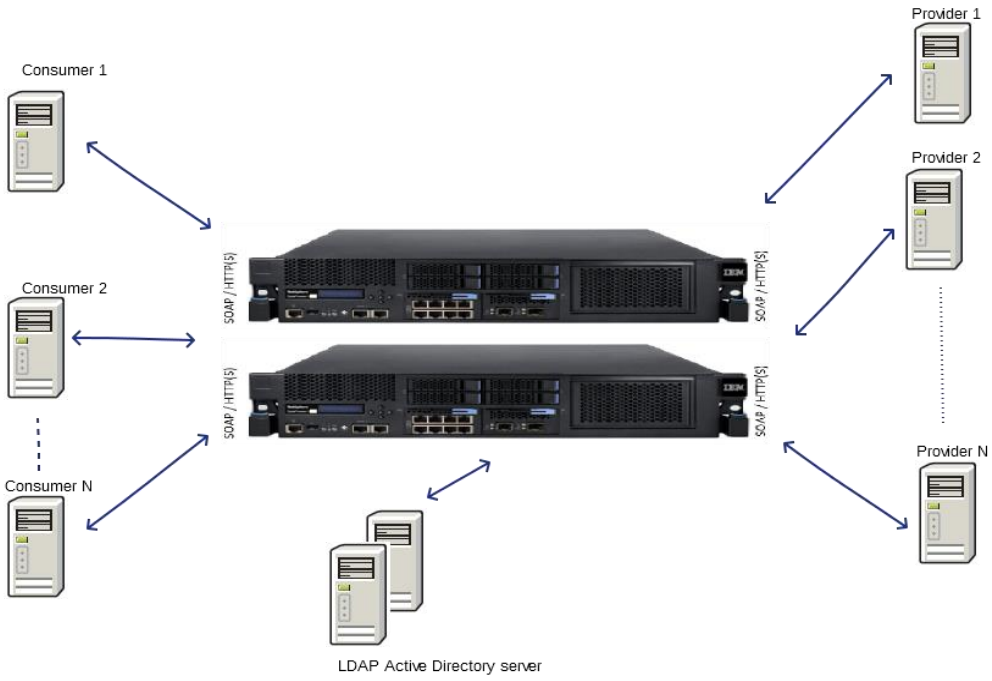
The two DataPower appliance in the G2B (Edge) will be configured to self-load balanced between each other and will be connected to three VLANs, one will be used for the management of the appliances and the other two VLANs one will be used for the data in the Edge (with the consumers) and the other will be used for the data in the SGN (with providers).

The below diagram shows the VLANs for all the components in the production environment for both the G2G and G2B.

G2G - Technical Specification

This document cover DataPower design in the MOICT solution for the Government to Government service calling.

The Below diagram describe how in general the DataPower will be used to integrate Service Provider with the Service consumer.



As it looks in that diagram, The Government to Government (G2G) is going through HA DataPower appliance, messages are sent as SOAP/HTTPS using SSL channel between both the consumer to DataPower and DataPower to Provider, hence the DataPower will be configure to expose services on the default ports as port 80 and 443 for both the HTTP and HTTPS respectively.

Each consumer will send a ws-security username token in the message in which the DataPower will extract to authenticate this token against LDAP Active Directory server (Microsoft Active Directory).

Then DataPower replace this user name token with another token to communicate with the Service provider.

On response flow DataPower will filter the returned message to extract set of fields (web service operation) that the consumer will be interested only.

- Technical Specification

This section describes DataPower design in the MOICT solution for the Government to Business service calling in high level.

The consumer will call any desired web service through the DataPower in this zone and the DataPower will directly forward the request to it related provider.

Messages from the consumer are sent as SOAP/HTTPS using SSL channel between both the consumer to DataPower and DataPower to Provider.

SSL Mutual authentication will be used only between the consumer and the DataPower for identity authentication of both the consumer and the DataPower.

Each consumer will send a ws-security username token in the message in which the DataPower will extract to authenticate this token against LDAP Active Directory server (Microsoft Active Directory).

Then the DataPower will replace this user name token with another token to communicate with the Service provider and authenticate himself with the Provider.

The Below diagram describes how in general the DataPower will be used to integrate Service Provider with the Service consumer.

Integration with Active Directory

APPROACH

The Active directory will contain a list of user accounts representing each service consumers; where each consumer will have single unique account. In addition to that the Active directory will contain also a list of LDAP groups representing each service provider, where each service provider will have a single unique LDAP group.

Each consumer represented by a user account will be member in the LDAP group for each provider if he has access to the service provider services (web service operations).

As per the requirement of MoICT to have a centralized place for all the access control and filtering roles, a new custom attribute will be defined for each user account, this custom attribute will be used to define a comma separated values where each value represent different set of fields to be returned by each service provider which he has access to (access role) representing for each service operation.

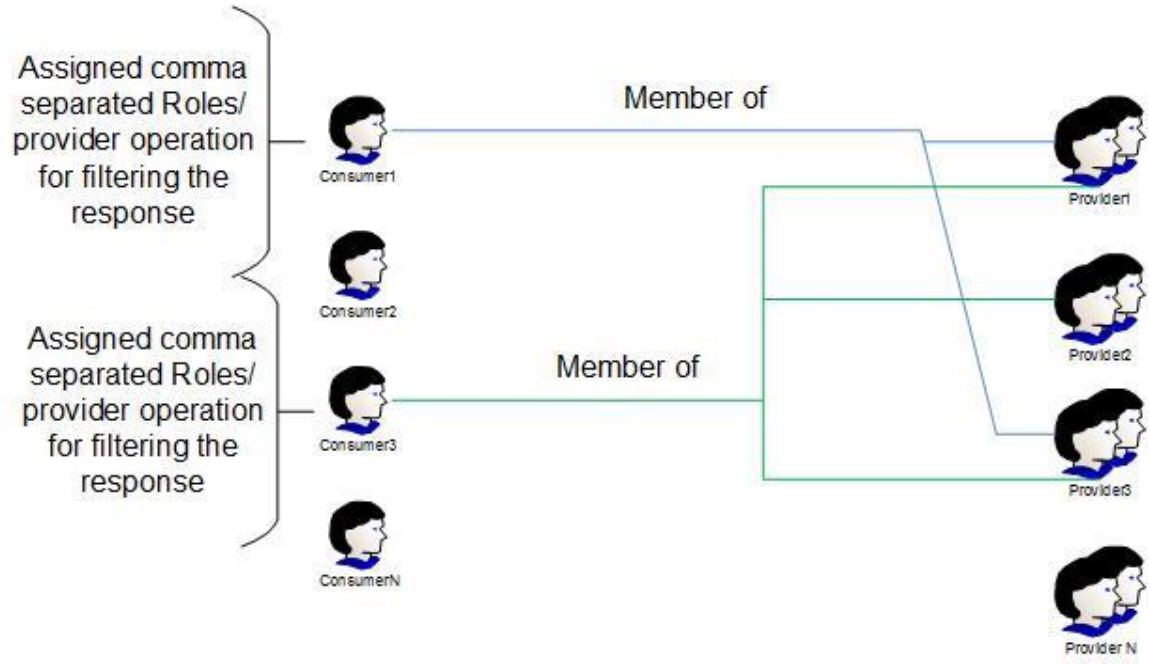
The access role will be defined as '*ServiceProviderName_OperationName*_XXX' where XXX is the access level of the consumer for this service operation which is one to one relation.

For example:

Provider name: CSPD

Consumer name: ISTD

Access role: CSPD_getFamilyRegistrybyNationalNo_All, CSPD_getFamilyRegistrybyNationalNo_05



For example if the ISTD wants to have access on service provider CSPD on the getFamilyRegistrybyNationalNo operation. So the defined role would look like "**CSPD_getFamilyRegistrybyNationalNo_All**", where **CSPD** is the service provider name, the **getFamilyRegistrybyNationalNo** is the operation name in the WSDL as provided by the CSPD, and '**All**' is the access level to retrieve all fields.

SUPPORTED LDAP SPECIFICATION

IBM Data Power can integrate with Active Directory that comply with LDAP V2 or V3.

Below are the details of the LDAPs which IBM Data Power will integrate with:

Domain name: GSB.LOCAL

Functional level: Microsoft windows server 2012 standard R2

DataPower Service Design

The used protocol is SOAP/HTTP(S) where the solution is based on WSDL file to proxy back-end web service, so the best DataPower service to be used is Web service proxy.

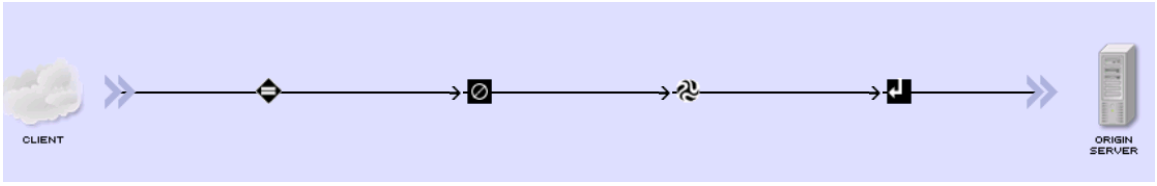
It will be single Web service proxy with multiple WSDL files and each file will be exposed with different URI. This will allow Consumer to have single IP and port used for communication with DataPower, and for different service only the URI part to be change to switch to another service call.

Each WSDL contain multiple operation, where each operation return certain set of data fields. And service consumer has access on the Level of WSDL not operation (access per provider). For the service consumer he will be able to send the request to any operation within the WSDL as he is authorized on the service provider level, but on response level of operation the returned response will be empty response if user has no defined role for this service operation.

In order not to fail in response schema validation in case of empty response all the returned fields should be defined as optional fields in the WSDL schema file (minOccurs="**0**") or at least the fields to not be returned.

The below section describe the request response flow design.

REQUEST FLOW DESIGN



The above digram represent the request message (Client to server) Per WSDL.