

PGP SupportPac for IBM Integration Bus v9

Part-2: PGP Encrypter Node Properties

By

**Dipak Kumar Pal
(dipakpal.opentech@gmail.com)**

Summary

This article is the second in a multi-part series of articles describing PGP security implementation in IBM Integration Bus v9. This series of articles introduces an industry standard solution to Data Security in IBM Integration Bus, enforcing data confidentiality and integrity by implementing PGP cryptographic solution. This solution is developed as a custom pluggable feature (or SupportPac) of IBM Integration Bus v9. This article illustrates node properties of the **PGP Encrypter Node** offered by this **SupportPac** (v1.0.01).

Introduction

PGP Encrypter Node is primarily used to sign (optional) and encrypt messages and files as per OpenPGP standard (RFC 4880). PGP SupportPac plugins for IBM Integration Bus Toolkit is required to be applied before using this node at messageflow. Once PGP supportPac plugins is applied to the IBM Integration Bus Toolkit, PGP Encrypter node will be available in the PGP drawer of the message flow node palette, and is represented in the IBM Integration Bus Toolkit by the following icon.

Figure-1: PGP Encrypter Node icon



PGP Encrypter

Using the PGP Encrypter node in a message flow

PGP Encrypter node supports both message and file encryption. By default, PGP Encrypter node places encrypted data at output message tree, but the node can be configured to write encrypted data into file system. In case of message encryption, node reads data from input message tree and serializes into bit-stream prior to encryption, make sure you provide appropriate CCSID, Encoding and/or MessageSet details (if required) at Properties folder of node's input message tree. This node requires a User Defined Configurable Service to load PGP private/public key repositories and default signature key/passphrase information. By using a user defined configurable service, you can change the PGP private/public key repository details and default signature key/passphrase information without the need to redeploy the messageflows. Refer to first article (Part-1) of this series to download SupportPac and sample messageflows.

Coordinated Transactions

PGP Encrypter node does not participate into local transaction initiating by Input node of the messageflow. But if downstream nodes connected to it's output terminal end up with unhandled exception, PGP Encrypter node does not take any action (Delete/Archive) on input file, even if the node is configured to do that.

Terminals and properties

The properties of the node are displayed in the Properties view. Few mandatory properties that do not have a default value defined are marked with an asterisk. But some properties are not marked with asterisk though these properties are mandatory for File encryption and PGP Signature. Please refer to node properties for detail configuration.

The terminals of the PGP Encrypter node are described at Table-1.

Table-1: PGP Encrypter Node Terminals

Terminal	Description
In	The input terminal that accepts the request message.
Out	The output terminal to which the message is routed upon successful completion of the PGP encryption, and if further processing is required within this message flow.

The following tables describe the node properties. The columns headed M indicate whether the property is *mandatory* (marked with an asterisk on the panel if you must enter a value when no default is defined); the columns headed C indicate whether the property is *configurable* (you can change the value when you add the message flow to the BAR file to deploy it).

The PGP Encrypter Node *Description* Properties are described at Table-2.

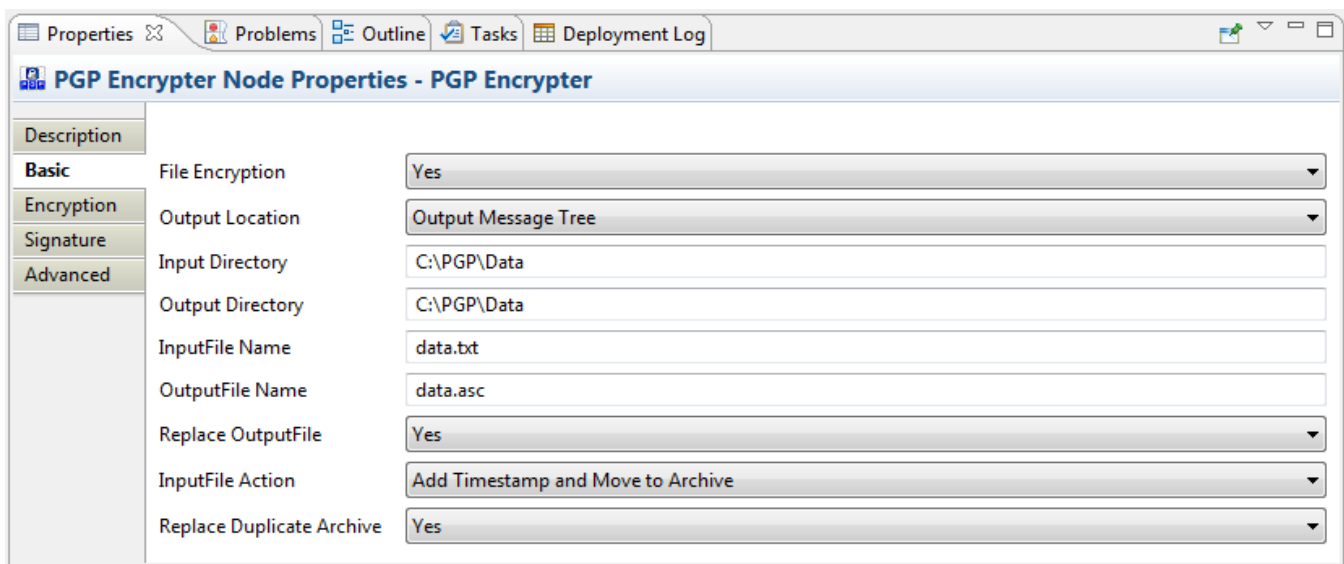
Table-2: PGP Encrypter Node *Description* Properties

Property	M	C	Default	Description
Node name	No	No	The node type, PGP Encrypter	The name of the node. Please provide a unique name if multiple nodes are used at same messageflow.
Short description	No	No		A brief description of the node.

Property	M	C	Default	Description
Long description	No	No		Text that describes the purpose of the node in the message flow.

Following figures represent IBM Integration Bus Toolkit screen-shots of PGP Encrypter Node Properties.

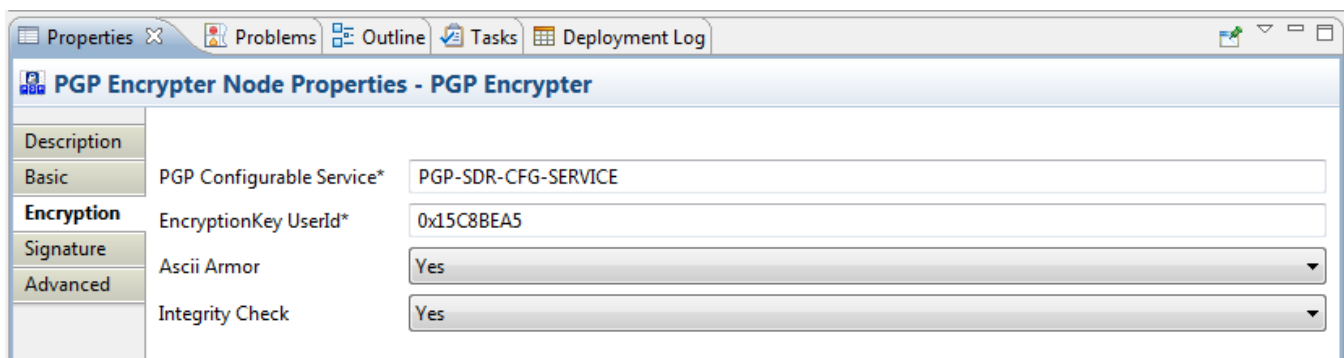
Figure-2: PGP Encrypter node **Basic** properties screen-shot



The screenshot shows the 'PGP Encrypter Node Properties - PGP Encrypter' dialog box with the 'Basic' tab selected. The 'Description' tab is also visible. The 'Basic' tab contains the following properties:

Property	Value
File Encryption	Yes
Output Location	Output Message Tree
Input Directory	C:\PGP\Data
Output Directory	C:\PGP\Data
InputFile Name	data.txt
OutputFile Name	data.asc
Replace OutputFile	Yes
InputFile Action	Add Timestamp and Move to Archive
Replace Duplicate Archive	Yes

Figure-3: PGP Encrypter node **Encryption** properties screen-shot



The screenshot shows the 'PGP Encrypter Node Properties - PGP Encrypter' dialog box with the 'Encryption' tab selected. The 'Basic' tab is also visible. The 'Encryption' tab contains the following properties:

Property	Value
PGP Configurable Service*	PGP-SDR-CFG-SERVICE
EncryptionKey UserId*	0x15C8BEA5
Ascii Armor	Yes
Integrity Check	Yes

Figure-4: PGP Encrypter node *Signature* properties screen-shot

The screenshot shows the 'PGP Encrypter Node Properties - PGP Encrypter' dialog box with the 'Signature' tab selected. The 'Basic' tab is also visible. The 'Signature' tab contains the following properties:

Property	Value
Signature Required	Yes
Use Default SignKey	Yes
SignKey UserId	0xEAFCEB2D
SignKey Passphrase	sdrpassphrase

Figure-5: PGP Encrypter Node *Advanced* properties screen-shot

The screenshot shows the 'PGP Encrypter Node Properties - PGP Encrypter' dialog box with the 'Advanced' tab selected. The 'Advanced' tab contains the following properties:

Property	Value
Hash Algorithm	SHA224
Cipher Algorithm	AES_256
Compression Algorithm	BZIP2

The PGP Encrypter node **Basic** properties are described at Table-3.

Table-3: PGP Encrypter Node *Basic* Properties

Property	M	C	D e f a u l t	Description	mqsiapplyb aroverride command property
File Encryption	Yes	No	N o	Specify whether the node will be used for message encryption or file encryption. Valid values are:	

Property	M	C	D e f a u l t	Description	mqsiapplyb aoverride command property
				<ul style="list-style-type: none"> Yes: select this value for file encryption. Make sure you provide following property values – Input Directory, InputFile Name. No: select this value for message encryption. Node reads data from input message tree and serializes into bit-stream prior to encryption. Make sure you provide appropriate CCSID, Encoding and/or MessageSet details (if required) at Properties folder of node's input message tree. 	
Output Location	Yes	No	O u t p u t M e s s a g e T r e e	<p>Specify whether the node will place encrypted data into output message tree or file system.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> Output Message Tree: node places encrypted data into output message tree in BLOB message domain. Note that, the node first copies entire input message tree as-is into output message tree, then it just replaces last child of output message tree with encrypted data. File System: encrypted data is written into file system. Make sure you provide following property values – Output Directory, OutputFile Name. Note that, 	

Property	M	C	D e f a u l t	Description	mqsiapplyb aroverride command property
				node copies entire input message tree as-is into output message tree.	
Input Directory	No	Yes		<p>Absolute path of the input directory in the broker's file system. For example, on Windows systems, the directory path starts with the drive letter prefix (such as C:).</p> <p>This property is mandatory for file encryption. However you can override the property value at node's input local environment tree.</p>	inputDirector y
Output Directory	No	Yes		<p>Absolute path of the output directory in the broker's file system. For example, on Windows systems, the directory path starts with the drive letter prefix (such as C:).</p> <p>This property is mandatory if you select Output Location property value as File System. However you can override the property value at node's input local environment tree.</p>	outputDirecto ry
InputFile Name	No	Yes		<p>Specify input file name which is required to be encrypted.</p> <p>This property is mandatory for file encryption. However you can override the property value at node's input local environment message</p>	inputFileNam e

Property	M	C	D e f a u l t	Description	mqsiapplyb aroverride command property
				tree.	
OutputFile Name	No	Yes		Specify output file name. This property is mandatory if you select Output Location property value as File System . However you can override the property value at nodes input local environment message tree.	outputFileNa me
Replace OutputFil e	Yes	No	Y e s	Specify whether the node will replace output file in specified output directory if the file already exists. This property is relevant only if Output Location property value is File System . Valid values are: <ul style="list-style-type: none"> • Yes: node replaces existing file. • No: node throws exception if file already exists. 	
InputFile Action	Yes	No	N o A c t i o n	The action performed to the input file on successful completion of PGP encryption. Valid actions are: <ul style="list-style-type: none"> • No Action: do nothing to the file. • Delete: delete the file. • Move to Archive: move the file to archive sub-directory 	

Property	M	C	D e f a u l t	Description	mqsiaapplyb aoverride command property
				<p>(pgparchive).</p> <ul style="list-style-type: none"> • Add Timestamp and Move to Archive: Archive with timestamp - move the file to the archive sub-directory (pgparchive) and add a timestamp. <p>In case of Archive, the node creates a sub-directory (name: pgparchive) at input directory specified at Input Directory property.</p> <p>If downstream nodes connected to PGP Encrypter node's output terminal end up with unhandled exception, this node does not take any action (Delete/Archive) on input file.</p>	
Replace Duplicate Archive	Yes	No	Y e s	<p>Specify whether the node will replace duplicate archive file in pgparchive sub-directory.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Yes: node replaces duplicate archive file. • No: node throws exception if the archive file already exists in pgparchive sub-directory. 	

The PGP Encrypter node *Encryption* properties are described at Table-4.

Table-4: PGP Encrypter Node *Encryption* Properties

Property	M	C	D e f a u l t	Description	mqsipplyb aoverride command property
PGP Configurable Service	Yes	Yes		<p>Specify name of the user defined Configurable Service containing PGP key repository details.</p> <p>PGP Encrypter node load PGP private/public keys from respective repository files specified at this configurable service.</p> <p>Node also load default signature key/passphrase details if specified at this configurable service.</p>	pgpConfigService
EncryptionKey UserId	Yes	Yes		<p>Specify the encryption key (recipient's public key) user Id or hexadecimal key Id (e.g. 0xF4C5D24A)</p> <p>Node searches for a suitable encryption key in PGP public key repository based on this specified key Id. If the public key is not found, node throws exception.</p> <p>You can override this property value at node's input local environment message tree.</p>	encryptionKey UserId
Ascii Armor	Yes	No	Y e s	<p>Specify whether encrypted data format will be ASCII armored or binary.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> Yes: encrypted data format will be ASCII armored. 	

Property	M	C	D e f a u l t	Description	mqsiapplyb aoverride command property
				<ul style="list-style-type: none"> No: encrypted data format will be binary. 	
Integrity Check	Yes	No	y e s	<p>Specify whether additional integrity check information is required to be added into the encrypted data.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> Yes: node adds additional integrity check information to the encrypted data. No: node won't add any additional integrity check information to the encrypted data. 	

The PGP Encrypter node *Signature* properties are described at Table-5.

Table-5: PGP Encrypter Node *Signature* Properties

Property	M	C	D e f a u l t	Description	mqsiapplyb aoverride command property
Signature Required	Yes	No	N o	<p>Specify whether the data is required to be signed.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> Yes: PGP signature is required. No: PGP Signature is not 	

Property	M	C	D e f a u l t	Description	mqsiapplyb aoverride command property
				required. You can override this property value at node's input local environment message tree.	
Use Default SignKey	Yes	No	Y e s	<p>Specify whether node will use default sign key and passphrase specified at DefaultSignKeyUserId and DefaultSignKeyPassphrase properties of user defined configurable service.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Yes: node ignores the sign key/passphrase specified at SignKey UserId/SignKey Passphrase properties of the node, and uses the value from user defined configurable service. • No: node uses values specified at SignKey UserId/SignKey Passphrase properties of the node. <p>Note: If you override SignKey UserId and SignKey Passphrase property values through node's input local environment, node ignores this (Use Default SignKey) property.</p>	
SignKey UserId	No	Yes		<p>Specify the sign key (signer's private key) user Id or hexadecimal key Id (e.g. 0xF4C5D24A).</p> <p>This property is relevant only if</p>	signKeyUserId

Property	M	C	D e f a u l t	Description	mqsiapplyb aroverride command property
				<p>Signature Required property value is Yes.</p> <p>This property is ignored if Use Default SignKey property value is Yes.</p> <p>You can override this property value at node's input local environment tree by using a Compute or Java Compute node prior to this node. Value specified at local environment tree has highest precedence, but is applicable to the current invocation (transaction) of the messageflow only.</p> <p>Node searches for a suitable signature (private) key in PGP private key repository based on this specified key user Id. If the private key is not found, node throws exception.</p>	
SignKey Passphrase	No	Yes		<p>Specify the sign key (signer's private key) passphrase.</p> <p>This property is relevant only if Signature Required property value is Yes.</p> <p>This property is ignored if Use Default SignKey property value is Yes.</p> <p>You can override this property value at node's input local environment tree by using a Compute or Java Compute node prior to this node. Value specified at local environment</p>	signKeyPassph rase

Property	M	C	D e f a u l t	Description	mqsipplyb aroverride command property
				<p>tree has highest precedence, but is applicable to the current invocation (transaction) of the messageflow only.</p> <p>Node extracts a suitable private key from PGP private key repository based on the specified key uses Id (SignKey UserId) by using this passphrase. Make sure you provide correct combination of sign key user Id and passphrase.</p>	

The PGP Encrypter node Advanced properties are described at Table-6.

Table-6: PGP Encrypter Node *Advanced* Properties

Property	M	C	D e f a u l t	Description	mqsipplyb aroverride command property
Hash Algorithm	Yes	No	S H A 1	<p>Specify the name of Hash (Digest) algorithm. This is required for generating PGP Signature.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • SHA1 • MD5 • RIPEMD160 • MD2 • SHA256 • SHA384 	

Property	M	C	D e f a u l t	Description	mqsiapplyb aoverride command property
				<ul style="list-style-type: none"> • SHA512 • SHA224 	
Cipher Algorithm	Yes	No	C A S T 5	<p>Specify the name of Cipher algorithm. This is required for Symmetric Key encryption.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • CAST5 • IDEA • TRIPLE_DES • BLOWFISH • DES • AES_128 • AES_192 • AES_256 • TWOFISH 	
Compression Algorithm	Yes	No	Z I P	<p>Specify the name of Compression algorithm.</p> <p>If you do not need encrypted data to be compressed, select Uncompressed value.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • Uncompressed • ZIP • ZLIB • BZIP2 	

Using local environment variables with PGP Encrypter node.

You can override following node properties through node's input local environment tree by using a Compute or Java Compute node prior to **PGP Encrypter** node. Properties specified at local environment tree have highest precedence, but property values are applicable to the current invocation (transaction) of messageflow only.

Following table (Table-7) describes the **LocalEnvironment.PGP.Encryption** elements:

Table-7: PGP Encrypter Node Local Environment variables

Element Name	Element Data Type	Node Property [Property Tab]	Description
InputDirectory	CHARACTER	Input Directory [Basic]	Absolute path of the input directory in the broker's file system. For example, on Windows systems, the directory path starts with the drive letter prefix (such as C:).
InputFileName	CHARACTER	InputFile Name [Basic]	Name of the input file.
OutputDirectory	CHARACTER	Output Directory [Basic]	Absolute path of the output directory in the broker's file system. For example, on Windows systems, the directory path starts with the drive letter prefix (such as C:).

Element Name	Element Data Type	Node Property [Property Tab]	Description
OutputFileName	CHARACTER	OutputFile Name [Basic]	Name of the output file.
EncryptionKeyUserId	CHARACTER	EncryptionKey UserId [Encryption]	Encryption key (Recipient's public key) User Id or hexadecimal key Id (e.g. 0xF4C5D24A)
SignatureRequired	CHARACTER	Signature Required [Signature]	Specify whether Signature is required or not. Valid values are: <ul style="list-style-type: none"> • Yes • No
SignKeyUserId	CHARACTER	SignKey UserId [Signature]	Signature key (Signer's private key) User Id or hexadecimal key Id (e.g. 0xF4C5D24A)
SignKeyPassphrase	CHARACTER	SignKey Passphrase [Signature]	Signature key (Signer's private key) passphrase.

Creating User Defined Configurable services

PGP Encrypter/Decrypter nodes read default sign key user Id and passphrase, default decryption key passphrase and PGP private/public keys from respective key repository files specified at User Defined Configurable Service. By using a configurable service, you can change the PGP private/public key repository details, default sign key user Id and passphrase, decryption key passphrase information without the need to redeploy the messageflow. You need to restart the execution group for the change of property value to take effect.

You can use the IBM Integration Bus Explorer to view, add, modify and delete the configurable service.

Alternatively, use the following commands to create the user defined configurable service:

```
mqsicreateconfigurableservice <Broker Name> -c UserDefined -o <Configurable  
Service Name> -n  
PrivateKeyRepository,PublicKeyRepository,DefaultSignKeyUserId,DefaultDecryp  
tionKeyPassphrase,DefaultSignKeyPassphrase -v <Absolute path of private key  
repository file>,<Absolute path of the public key repository file>,<Sign (private)  
key User Id>,<Decryption (private) key passphrase>,<Sign (private) key  
passphrase>
```

Note that **DefaultSignKeyUserId**, **DefaultSignKeyPassphrase** are not required for PGP decryption. Similarly **DefaultDecryptionKeyPassphrase** is not required for PGP Encryption. However same Configurable Service can be used for both Encryption and Decryption process.

Conclusion

This series of articles provides an industry standard solution that mitigates a huge gap in IBM Integration Bus Data Security zone, where this article primarily illustrates the node properties of **PGP Encrypter** Node supplied with the SupportPac. Current version (v1.0.0.1) of this SupportPac supports integrated signature generation combined with PGP encryption process. However future version will provide isolated signature generation functionality.

You can post any query regarding to this PGP SupportPac at following IBM DeveloperWorks public community forum, author of this article will address those queries.

PGP SupportPac for IBM Integration Bus

<https://www.ibm.com/developerworks/community/groups/community/pgpsupportpaciib>

References

- **PGP Basics**
 - **PGP Basics: PGP basic concepts** (<http://www.pgpi.org/doc/pgpintro/>)
 - **Bouncy Castle: Bouncy Castle Resources** (<http://www.bouncycastle.org/>)
 - **Gpg4Win: PGP encryption/decryption command line and GUI tool** (<http://www.gpg4win.org/index.html>)
 - **Portable PGP: Java based GUI tool for PGP** (<http://ppgp.sourceforge.net/>)
 - **GnuPG: GnuPG PGP library** (<http://www.gnupg.org/>)
 - **GitHub: Samples and other Artifacts** (<https://github.com/dipakpal/MyOpenTech-PGP-SupportPac>)

- **Public Community at IBM DeveloperWorks**

- [PGP SupportPac for IBM Integration Bus:](https://www.ibm.com/developerworks/community/groups/community/pgpsupportpaciib)
<https://www.ibm.com/developerworks/community/groups/community/pgpsupportpaciib>

- **IBM Integration Bus resources**

- [IBM Integration Bus product page](#)
Product descriptions, product news, training information, support information, and more.
- [IBM Integration Bus V7 information center](#)
A single Web portal to all IBM Integration Bus V6 documentation, with conceptual, task, and reference information on installing, configuring, and using your IBM Integration Bus environment
- [Download free trial version of IBM Integration Bus](#)
IBM Integration Bus is an ESB built for universal connectivity and transformation in heterogeneous IT environments. It distributes information and data generated by business events in real time to people, applications, and devices throughout your extended enterprise and beyond.
- [IBM Integration Bus documentation library](#)
IBM Integration Bus specifications and manuals.
- [IBM Integration Bus forum](#)
Get answers to technical questions and share your expertise with other IBM Integration Bus users.
- [IBM Integration Bus support page](#)
A searchable database of support problems and their solutions, plus downloads, fixes, and problem tracking.

- **WebSphere resources**

- [developerWorks WebSphere](#)
Technical information and resources for developers who use WebSphere products. developerWorks WebSphere provides product downloads, how-to information, support resources, and a free technical library of more than 2000 technical articles, tutorials, best practices, IBM Redbooks, and online product manuals. Whether you're a beginner, an expert, or somewhere in between, you'll find what you need to build enterprise-scale solutions using the open-standards-based WebSphere software platform.
- [developerWorks WebSphere application integration developer resources](#)
How-to articles, downloads, tutorials, education, product info, and other resources to help you build WebSphere application integration and business integration solutions.
- [Most popular WebSphere trial downloads](#)
No-charge trial downloads for key WebSphere products.
- [WebSphere forums](#)
Product-specific forums where you can get answers to your technical questions and share your expertise with other WebSphere users.
- [WebSphere demos](#)
Download and watch these self-running demos, and learn how WebSphere products can provide business advantage for your company.
- [WebSphere-related articles on developerWorks](#)
Over 3000 edited and categorized articles on WebSphere and related

technologies by top practitioners and consultants inside and outside IBM.
Search for what you need.

- [developerWorks WebSphere weekly newsletter](#)
The developerWorks newsletter gives you the latest articles and information only on those topics that interest you. In addition to WebSphere, you can select from Java, Linux, Open source, Rational, SOA, Web services, and other topics. Subscribe now and design your custom mailing.
- [WebSphere-related books from IBM Press](#)
Convenient online ordering through Barnes & Noble.
- [WebSphere-related events](#)
Conferences, trade shows, Webcasts, and other events around the world of interest to WebSphere developers.