IBM® Tivoli® Software

Reconfiguration Tool for 7.5.x IBM Maximo Administrative Workstations

Document version 1.2

Rob Binns
Software Engineer

© Copyright International Business Machines Corporation 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

CONTENTS

LIST OF TABLES

REVISION HISTORY

Date	Version	Revised By	Comments
10/31/11	1.0	C.E.L.	Initial version
03/23/12	1.1	C.E.L.	Additional actions added.
12/13/12	1.2	C.E.L.	New functionality. For 7.5.x installs only. Document title change.

1 Introduction

When you install a fix pack or otherwise upgrade an existing Maximo-based product, the installation program uses values recorded from the previous deployment. These values are stored on the administrative system in the install.properties and maximo.properties files located under the *maximo_install_location*\etc and *maximo_install_location*\maximo\applications\maximo\properties directories, respectively.

If you have made any environmental changes to any of the systems used for the original deployment, they must be recorded in the install.properties and maximo.properties files. Typically these types of changes would include changing a host name or updating a password, for example.

You can update these values manually, or you can use the reconfiguration command line interface tool to update configuration values for your existing deployment when they change. Properties specified when using the reconfiguration command line interface tool, either as parameters, or in an input properties file, replace existing properties in the maximo.properties and install.properties files. Properties are encrypted upon saving.

The reconfiguration command line interface tool can be used in the following scenarios:

- Change the security model chosen for the original deployment. For example, you can migrate from Maximo-based security to WebSphere Application Server security. Note that this option is not available for Oracle WebLogic Server.
- Confirm that updated property values conform to required input domains. Validate credentials, host names, and available ports.
- Update database or J2EE server configuration settings without the server being available. Note that these values cannot be validated in this scenario.
- Clone an existing environment and use the reconfiguration command line interface tool to reconfigure the administrative workstation to use the new servers. The cloned environment must use the same directory structure as the original.
- Create a new environment (non-cloned) and use the reconfiguration command line interface tool to create all required artifacts database, table spaces, and j2ee objects, for example.

2 Access the reconfiguration command line interface tool

The reconfiguration command line interface tool can be downloaded from the Integrated Service Management Library located at
https://www.ibm.com/software/brandcatalog/ismlibrary/

Once downloaded, uncompress the archive on the administrative workstation. Inside the archive are two additional compressed files. The Maximo_750x_ReconfigurationTool_for_AdminWorkstation.zip file includes the reconfiguration command line interface tool that can be used with v7.5 Maximo-based products.

Uncompress the appropriate zipped file into the product installation directory. Within the newly created Reconfig directory. The reconfiguration command line interface tool are launched on the administrative workstation:

Windows: `reconfigurePae.bat <command-line-parameters>`

UNIX: `reconfigurePae.sh <command-line-parameters>`

3 Validation

The reconfiguration command line interface tool validates input in the same way the product installation program validates input.

The following list details the validation checks performed by the reconfiguration command line interface tool.

- Host names or IP addresses are correctly formatted and are reachable.
- User IDs and passwords meet length and character set criteria.
- Credentials supplied are used to authenticate to WebSphere.
- Port values supplied are listening on the corresponding host, are numeric, and fall into the correct range.
- Middleware installation directories supplied already exist
- Pre-configured middleware can authenticate to the product database.
- Required objects such as JMS queues, SIB destinations, databases, and table spaces exist.
- Required VMM users exist.
- Sufficient authority is available to create VMM users.
- Remote login credentials are valid.
- Sufficient space in the supplied directories is available to create database objects.

4 Input properties files

There are sample input property files that can be used as input for the reconfiguration command line interface tool. These files contain comments and properties you can update and then use as input for the reconfiguration command line interface tool using the –input parameter. In addition, there property files contain properties that can only be updated through the use of this input file. Most properties cannot be used as parameters from the command line.

Four input sample files are found in the `reconfig/samples` directory of the reconfiguration command line interface tool packages.

- DB2_Sample_input.properties

- Oracle_Sample_input.properties
- SQLServer_Sample_input.properties
- WebSphere_App_Server_Sample_input.properties

Each of these sample files contain properties associated with a specific database or application server type.

All input properties, introduced from either the command line or located in the input properties file, are validated before they are used. Once validation has passed successfully, then the maximo.properties and install.properties files will be updated.

5 Command line interface parameters

The following table contains a list of parameters that can be used with the reconfiguration command line interface tool.

Table 1: Command line interface parameters

Parameter name	Description
-validateUsers	Used in conjunction with the enableAppSecurity action to validate users exist in the LDAP repository. If the users do not exist, the existing security model is not modified.
-action	The type of configuration action being performed by the tool. Possible values are: • updateDatabaseConfiguration – Used to update existing database configuration values. • validateDatabaseConfiguration - Used to validate database configuration values specified as input for the reconfiguration command line interface tool. • validateAndUpdateDatabaseConfiguration – Used to both validate reconfiguration command line interface tool input and then update existing database configuration property values. • deployDatabaseConfiguration – Used to both validate reconfiguration command line interface tool input and then define configuration property values for a new database to be used with the currently deployed product. • updateJ2eeConfiguration - Used to update existing application server configuration values. • validateJ2eeConfiguration - Used to validate application server configuration values specified as input for the reconfiguration command line interface tool. • validateAndUpdateJ2eeConfiguration - Used to both validate reconfiguration command line interface tool input and then update existing application server configuration property values. • deployJ2eeConfiguration - Used to both validate

	reconfiguration command line interface tool input and then define configuration property values for a new application server. • enableAppSecurity – Enables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of1, and updates the mxe.ldapUserManagement flag. This value is written to the database when updated. • disableAppSecurity - Disables application security for the application. Security is handled entirely through Maximo. This action sets the mxe.useAppServerSecurity property to a value of 0. This value is written to the database when updated. The actions that modify the security setting used by Maximo also updates Maximo web.xml files.
-force	The -force option updates the properties file and skips the validation of parameters input to the command line tool through an input properties file. When using this parameter, you are not prompted for confirmation of the property update task.
-buildAndDeployEAR	Rebuilds and deploys application EAR files. Application EAR files must be rebuilt and redeployed for configuration changes to take effect in the application.
-dbserverhost	Host name of the database server.
-dbserverport	Port name of the database server.
-dbname	Name of the database.
-dbuser	User ID that accesses the database.
-dbpwd	Password for the user ID that accesses the database.
-dbrxauser	User ID used to access a remote middleware server.
-dbrxapwd	Password for the user ID used to access a remote middleware server.
-j2eeserverhost	Host name of the J2EE domain manager server. If deployment manager host name or server port is specified the thinwsadmin scripts will be updated accordingly.
-j2eeserverport	Port name of the J2EE domain manager server. If deployment manager host name or server port is specified the thinwsadmin scripts will be updated accordingly.
-wasuser	WebSphere administrator user ID. This is the User ID that is used to log into the WebSphere administrative client application. Typically, this user ID is defined as wasadmin.
-waspwd	WebSphere administrator user ID password.
-wasrxauser	Operating system user ID used to access remote WebSphere server host. Typically this user ID is defined either as Administrator or root.
-wasrxapwd	Password for user ID to access remote WebSphere server host.
-applicationServerNode	Name of the application server node.

-applicationServerName	Name of the application server.
-usermanagement	Used to change the security configuration of the existing Maximo deployment. Possible values are: • j2ee – Use this value to change the security setting in Maximo so that both Maximo users and Maximo groups are managed through application server security mechanisms. • mixed – Use this value to manage users through application server security mechanisms, and manage groups using Maximo.
-inputfile	Fully-qualified path to the properties file being used to set properties in a cloned environment. Values specified as command line parameters for the reconfiguration command line interface tool supersede those from the input file.
-validateForNewDeploy	Used to validate middleware configuration. When this parameter is specified, validation is performed as if the tool was configuring the middleware. Additional configuration details are checked, including disk space availability and remote access credentials. If this parameter is not specified, validation is performed in the context of a component that is already established in the environment.

If the application server type is configured as Oracle Weblogic Server, the tool exits with an error message. This tool does not allow you to change database types.

6 Action scenarios

The following sections detail various scenarios for the reconfiguration command line interface tool supported actions.

6.1 updateDatabaseConfiguration

The updateDatabaseConfiguration action is used to update existing database configuration values.

```
-action updateDatabaseConfiguration [-force] [-buildAndDeployEAR] [-
dbserverhost hostname] [-dbserverport port] [-dbname name] [-dbuser
dbuser] [-dbpwd dbpassword] [-dbrxauser remoteuser] [-dbrxapwd
remotepassword] [-inputfile fullyqualifiedpath]
```

6.2 validateDatabaseConfiguration

The validateDatabaseConfiguration action is used to validate current database configuration properties. This action can be used to verify database properties before they are updated, or following an update action.

`-action validateDatabaseConfiguration [-validateForNewDeploy] [-dbserverhost` *dbhostname*`] [-dbserverport` *port*`] [-dbname` *dbname*`] [-dbuser` *dbuser*`] [-dbpwd` *dbpassword*`] [-dbrxauser` *remoteuserID*`] [-dbrxapwd` *remoteuserIDpasswd*`] [-inputfile` *fullyqualifiedpath*`]`

The following properties are required if the -validateForNewDeploy parameter is used:

- Database.DB2.InstanceAdminGroup
- Database.DB2.InstanceAdminUserName (Windows only)
- Database.DB2.InstanceAdminPassword (Windows only)
- Database.DB2.FencedUser
- Database.DB2.FencedUserPassword
- Database.DB2.FencedGroupName

These are new properties that must be added manually to the install.properties file.

6.3 validateAndUpdateDatabaseConfiguration

The validateAndUpdateDatabaseConfiguration action is used to both validate reconfiguration command line interface tool input and then update existing database configuration property values.

`-action validateAndUpdateDatabaseConfiguration [-validateForNewDeploy] [-force] [-buildAndDeployEAR] [-dbserverhost` *hostname*`] [-dbserverport` *port*`] [-dbname` *name*`] [-dbuser` *dbuser*`] [-dbpwd` *dbpassword*`] [-dbrxauser` *remoteuser*`] [-dbrxapwd` *remotepassword*`] [-inputfile` *fullyqualifiedpath*`]`

The following properties are required if the -validateForNewDeploy parameter is used:

- Database.DB2.InstanceAdminGroup
- Database.DB2.InstanceAdminUserName (Windows only)
- Database.DB2.InstanceAdminPassword (Windows only)
- Database.DB2.FencedUser
- Database.DB2.FencedUserPassword
- Database.DB2.FencedGroupName

These are new properties that must be added manually to the install.properties file.

6.4 deployDatabaseConfiguration

The deployDatabaseConfiguration action is used to both validate reconfiguration command line interface tool input and then define configuration property values for a new database to be used with the currently deployed product.

Before using this action, ensure that you rename the tpae.xml.orig file found in the install_home\maximo\applications\maximo\properties\product directory to tpae.xml. This allows the database update action to create required Maximo users in the database.

```
-action deployDatabaseConfiguration [-buildAndDeployEAR] [-
createResourcesIfMissing] [-dbserverhost hostname] [-dbserverport port]
[-dbname name] [-dbuser dbuser] [-dbpwd dbpassword] [-dbrxauser
remoteuser] [-dbrxapwd remotepassword] [-inputfile fullyqualifiedpath]
```

The following properties are required if the -createResourcesIfMissing parameter is used:

- Database.DB2.InstanceAdminGroup
- Database.DB2.InstanceAdminUserName (Windows only)
- Database.DB2.InstanceAdminPassword (Windows only)
- Database.DB2.FencedUser
- Database.DB2.FencedUserPassword
- Database.DB2.FencedGroupName

These are new properties that must be added manually to the install.properties file.

If you have application security enabled on the application server, and you are using the deployDatabaseConfiguration action in the context of recovering an environment where the originally deployed database is corrupt, being replaced, or no longer available, you must invoke the enableAppSecurity action. Invoking the enableAppSecurity action after the deployDatabaseConfiguration action ensures that the mxe.useAppServerSecurity and mxe.ldapUserManagement properties found in the maximo.properties file are set to values that reflect the settings contained in the web.xml file used by the application server. If your original deployment did not use application security, you do not have to use the enableAppSecurity action.

6.5 updateJ2eeConfiguration

The updateJ2eeConfiguration action is used to update existing application server configuration values.

```
-action updateJ2eeConfiguration [-force] [-buildAndDeployEAR] [-
j2eeserverhost fullyqualifiedDMgrhostname] [-j2eeserverport port] [-wasuser
WebSphereAdminuser] [-waspwd WebSphereAdminuserpassword] [-wasrxauser
WebSphereRemoteuser] [-wasrxapwd WebSphereRemoteuserpassword] [-
applicationServerNode NodeName] [-applicationServerName
applicationservername] [-inputfile fullyqualifiedpath]
```

6.6 validateJ2eeConfiguration

The validateJ2eeConfiguration action is used to validate application server configuration values specified as input for the reconfiguration command line interface tool.

```
-action validateJ2eeConfiguration [-validateForNewDeploy] [-
j2eeserverhost fullyqualifiedDMgrhostname] [-j2eeserverport port] [-wasuser
WebSphereuser] [-waspwd WebSphereuserpassword] [-applicationServerNode
NodeName] [-applicationServerName applicationservername] [-inputfile
fullyqualifiedpath]
```

6.7 validateAndUpdateJ2eeConfiguration

The validateAndUpdateJ2eeConfiguration is used to both validate reconfiguration command line interface tool input and then update existing application server configuration property values.

```
-action validateAndUpdateJ2eeConfiguration [-force] [-
validateForNewDeploy] [-buildAndDeployEAR] [-j2eeserverhost
fullyqualifiedDMgrhostname] [-j2eeserverport port] [-wasuser WebSphereuser]
[-waspwd WebSphereuserpassword] [-applicationServerNode NodeName] [-
applicationServerName applicationservername] [-inputfile fullyqualifiedpath]
```

6.8 deployJ2eeConfiguration

The deployJ2eeConfiguration action is used to both validate reconfiguration command line interface tool input and then define configuration property values for a new application server.

```
-action deployJ2eeConfiguration [-buildAndDeployEAR] [-
createResourcesIfMissing] [-j2eeserverhost fullyqualifiedDMgrhostname] [-
j2eeserverport port] [-wasuser WebSphereuser] [-waspwd
WebSphereuserpassword] [-applicationServerNode NodeName] [-
applicationServerName applicationservername] [-inputfile fullyqualifiedpath]
```

6.9 enableAppSecurity

The enableAppSecurity action enables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of 1, and updates the mxe.ldapUserManagement flag according to the setting of the –usermanagement parameter. This value is written to the database when updated.The `maximouiweb`, `maxrestweb`, `meaweb`, and `mboweb` web.xml files are updated during this action.

```
-action enableAppSecurity -usermanagement {j2ee,mixed}  [-
buildAndDeployEAR] [-validateUsers] [-force]
```

If you have application security enabled on the application server, and you are using the deployDatabaseConfiguration action in the context of recovering an environment where the originally deployed database is corrupt, being replaced, or no longer available, you must invoke the enableAppSecurity action. Invoking the enableAppSecurity action after the deployDatabaseConfiguration action ensures that the mxe.useAppServerSecurity and mxe.ldapUserManagement properties found in the maximo.properties file are set to values that reflect the settings contained in the web.xml file used by the application server. If your

original deployment did not use application security, you do not have to use the enableAppSecurity action.

6.10 disableAppSecurity

The disableAppSecurity action disables application security for the application. This action sets the mxe.useAppServerSecurity property to a value of 0. This value is written to the database when updated. Using this action reverts the security implementation to Maximo-based security for users and groups. The `maximouiweb`, `maxrestweb`, `meaweb`, and `mboweb` web.xml files are updated during this action.

```
-action disableAppSecurity [-buildAndDeployEar] [-force]
```

7 Properties

The following table contains a list of properties that can be modified using the reconfiguration command line interface tool through the use of an input.properties file.

Table 2 Properties available to be reconfigured through the reconfiguration command line interface tool

Category	Property	Definition
Shared database properties	mxe.db.schemaowner	Owner of the database schema. For example, maximo. This value is written to the database when updated.
	mxe.db.user	User ID that accesses the database.
	mxe.db.password	Password for the user ID that accesses the database.
	Database.RemoteAccessUserName	Database server system user ID that is used for configure the database remotely. This property is only required if the createResourcesIfMissing flag is specified.
	Database.RemoteAccessPassword	Password for user ID named in Database.RemoteAccessUserName. This property is only required if the createResourcesIfMissing flag is specified.
DB2 Properties	Database.DB2.ServerHostName	Fully qualified host name of the DB2 server. For example, mymachine.mydomain.com. This value is written to the database when updated.
	Database.DB2.ServerPort	Database server port. For example, 50005. This value is written to the database when updated.
	Database.DB2.InstanceName	Name of the database instance. For example, ctginst1.

		This value is written to the database when updated. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.InstanceUserPassword	Password for the database instance owner. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.InstanceAdminGroup	Group for the instance administrator. For example, ctgiadm1. This property is required if the validateForNewDeploy or createResourcesIfMissing parameter is specified.
	Database.DB2.DatabaseName	Name of the database. For example, maxdb75. This value is written to the database when updated.
	Database.DB2.InstallLocation	Install location of the database. For example, /opt/IBM/db2/V9.7 This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.LogFileSize	Set the size for transaction logs. For example, 8192. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.AppCtlHeapSize	Application control heap size. For example, 1024. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.ApplHeapSize	Application heap size. For example, 1024. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.LockListSize	Size allocated to the lock list. For example, AUTOMATIC. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.LogSecond	Number of secondary log files allowed. For example, 100. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.ServiceUser	User ID used to autostart. This property is only required if the createResourcesIfMissing flag is specified. This property is only required if DB2 is installed on

		a Windows system.
	Database.DB2.ServicePassword	Password for Database.DB2.ServiceUser. This property is only required if the createResourcesIfMissing flag is specified. This property is only required if DB2 is installed on a Windows system.
	Database.DB2.ExtentSize	Number of pages per extent (group of pages). For example, 32. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.FencedUser	Fenced user ID for DB2 on Linux® or UNIX systems. For example, db2fenc1. This property is required if the validateForNewDeploy or createResourcesIfMissing parameter is specified. The Database.DB2.FencedUser property must be manually added to your install.properties file. It is not created automatically during a v7.5 installation.
	Database.DB2.FencedUserPassword	Password for the fenced user ID for DB2 on Linux® or UNIX systems. This property is required if the validateForNewDeploy or createResourcesIfMissing parameter is specified.
	Database.DB2.FencedGroupName	Default group for database fenced user. For example, ctgfgrp1. This property is only required if the createResourcesIfMissing flag is specified. This property is only required if DB2 is installed on a UNIX or Linux system.
	Database.DB2.AuthType	Method DB2 uses to authenticate users. For example, server. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.DataTablespaceName	DB2 table space name for the product database. For example, maxdata.
	Database.DB2.BufferPoolName	DB2 buffer pool name. For example, MAXBUFPOOL. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.BufferPoolLocation	Location of the buffer pool.
	Database.DB2.BufferPoolSize	Size of the buffer pool. For example, 4096. This property is only required if the

		createResourcesIfMissing flag is specified.
	Database.DB2.DataTablespaceLocation	Location of DB2 database table space data files. For example, CTGDAT. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.DataTablespaceSize	Table space size, measured in Mb. For example, 5000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.TempTablespaceName	Temporary table space name. For example, maxtemp. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.TempTablespaceLocation	Location of temporary table space. For example, CTGTMP. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.TempTablespaceSize	Temporary table space size, measured in Mb. For example, 1000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.IndexTablespaceName	Index table space name. For example, maxdata.
	Database.DB2.IndexTablespaceLocation	Location of index table space. For example, CTGDAT. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.IndexTablespaceSize	Index table space size, measured in Mb. For example, 5000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DB2.InstanceAdminUserName	Administrative user or the database instance. For example, db2admin. This property is required if the validateForNewDeploy or createResourcesIfMissing parameter is specified. This property is only required if the database is hosted on a Windows system.
	Database.DB2.InstanceAdminPassword	Password for the user ID specified for Database.DB2.InstanceAdminUserName. This property is required if the validateForNewDeploy or createResourcesIfMissing parameter is specified. This property is only required if the database is

		hosted on a Windows system.
Oracle	Database.Oracle.SchemaPassword	Password for the schema owner.
	Database.Oracle.InstanceName	Oracle instance name. This value is written to the database when updated.
	Database.Oracle.SoftwareOwner	Owner of the software installation. For example, oracle. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.SoftwareOwnerPassword	Password for the user ID listed in Database.Oracle.SoftwareOwner. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.InstallLocation	Oracle installation location. For example, /opt/app/oracle/product/10.2.0/db_1. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.DataTablespaceName	Oracle table space name for the product database. For example, maxdata.
	Database.Oracle.InstanceLocation	Oracle instance location. For example, /opt/app/oracle/ product/10.2.0/db_1. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.DataTablespaceLocation	Location of Oracle database table space.
	Database.Oracle.DataTablespaceSize	Tablespace size, measured in Mb. For example, 5000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.TempTablespaceName	Temporary table space name. For example, maxtemp. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.TempTablespaceLocation	Location of temporary table space.
	Database.Oracle.TempTablespaceSize	Temporary table space size, measured in Mb. For example, 1000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.IndexTablespaceName	Index table space name. For example, maxdata.
	Database.Oracle.IndexTablespaceLocation	Location of index table space.
	Database.Oracle.IndexTablespaceSize	Index table space size, measured in Mb.

		For example, 1000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.Oracle.ServerHostName	Fully qualified host name of the Oracle server.
	Database.Oracle.ServerPort	Port number used by Oracle. For example, 1521. This value is written to the database when updated.
	Database.DBAUserName	Oracle DBA user name. For example, sys. This property is only required if the createResourcesIfMissing flag is specified.
	Database.DBAPassword	Password for user ID listed for Database.DBAUserName. This property is only required if the createResourcesIfMissing flag is specified.
SQL Server	Database.SQL.DatabaseName	Name of the database. For example, maxdb75. This value is written to the database when updated.
	Database.SQL.DataFileName	A way to specify the name of the data file used for the database. For example, maxdb75_dat. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.DataFileMaxSize	Maximum size for data file for the database.
	Database.SQL.DataFileSize	Initial size for data file for the database in kb. For example, 5000. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.LogFileName	A way to specify the name for the database transaction log file. For example, maxdb75_log. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.LogFileSize	Microsoft SQL Server Database transaction log file size. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.DataFilegroupName	Database logical name file group. For example, PRIMARY. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.ServerHostName	Host name of the database server. For example,

		myhost.mydomain.com.
	Database.SQL.ServerPort	Database server port. For example, 1433. This value is written to the database when updated.
	Database.SQL.InstanceAdminUserName	Administrative user for the Microsoft SQL Server instance. Used during installation for creating and modifying the database and database user. For example, sa. This property is only required if the createResourcesIfMissing flag is specified.
	Database.SQL.InstanceAdminPassword	Administrative users password. This property is only required if the createResourcesIfMissing flag is specified.
WebSphere	WAS.InstallLocation	Installation location for WebSphere Application Server Network Deployment. For example, C:\\IBM\\WebSphere\\AppServer. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.DeploymentManagerHostName	Host name of the WebSphere Application Server Network Deployment deployment manager. This value is written to the database when updated.
	WAS.DeploymentManagerProfileName	WebSphere Application Server Network Deployment profile name. For example, ctgDmgr01. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.DeploymentManagerProfileRoot	Location of the WebSphere Application Server Network Deployment profile. For example, C:/IBM/WebSphere/AppServer/profiles/ctgDmgr01 This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.ServerProfileName	WebSphere Application Server Network Deployment application server profile name used with the service integration bus. For example, ctgAppSrv01
	WAS.NodeName	WebSphere Application Server Network Deployment node name. For example, ctgNode01
	WAS.ApplicationServerName	WebSphere Application Server Network Deployment application server name. For example, MXServer. This value is written to the database when updated.
	WAS.CellName	WebSphere Application Server Network

		Deployment cell name. For example, ctgCell01.
	WAS.AdminUserName	WebSphere Application Server Network Deployment administrator name. For example, wasadmin
	WAS.AdminPassword	WebSphere Application Server Network Deployment administrator password.
	WAS.RemoteAccessUserName	WebSphere Application Server Network Deployment deployment manager system user ID used for tasks such as copying ISC WAR files and fetching the keystore. This property is only required if the WAS.SibPersistMessages property is set to 'true'.
	WAS.RemoteAccessPassword	WebSphere Application Server Network Deployment deployment manager system user password. This property is only required if the WAS.SibPersistMessages property is set to 'true'.
	WAS.SOAPConnectorPort	SOAP port for WebSphere Application Server Network Deployment manager. For example, 8879.
	WAS.VirtualHost	Name of the WebSphere Application Server Network Deployment virtual host. For example, maximo_host.
	WAS.VirtualHostPort	Port for virtual host for listening for HTTP server. For example, 80.
	WAS.WebServerName	Host name where the HTTP server is located.
	WAS.SibName	Name of the service integration bus. For example, intjmsbus.
	WAS.SibHiMsg	Service integration bus high message count. For example, 500000. This property is required if the createResourcesIfMissing flag is specified.
	WAS.WebServerName	Name of the WebSphere Application Server Network Deployment web server. Used to manage HTTP server from within WebSphere Application Server Network Deployment. For example, webserver1.
	WAS.SibPersistMessages	Binary value that indicates if service integration bus messages are persisted in either the product database or a local derby database. A value of true indicates that the messages are persisted. This property is required if the createResourcesIfMissing flag is specified.
	WAS.SibDSName	Service integration bus data source name created

		to access the service integration bus persistence store. For example, intjmsds. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBName	Name of the service integration bus messages database.
	WAS.SibDBInstance	Instance name of the service integration bus database. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBInstancePassword	DB2 Instance users password for the SIB DB2 data store This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBServerName	Server name of the system hosting the service integration bus message database. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBServerPort	Database server port for the database containing the service integration bus messages. For example, 50005. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBUserName	User ID used to access the persistence data store database for service integration bus messages. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBUserPass	Password for user ID named in WAS.SibDBUserName. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDBInstallDir	Where the service integration bus database is installed. For example, c:\\program files\\ibm\\sqllib. This property is only required if the WAS.SibPersistMessages property is set to ‘true’.
	WAS.SibDbFencedUser	Fenced user ID for the service integration bus database. This property is only used for databases hosted on UNIX® systems. For example, db2fenc1. This property is only required if the WAS.SibPersistMessages property is set to ‘true’. This property is only required if the database is hosted on a UNIX system.
	WAS.SibDbFencedPassword	Password for the fenced user ID for the service integration bus database.

		This property is only required if the WAS.SibPersistMessages property is set to 'true'. This property is only required if the database is hosted on a UNIX system.
	WAS.SibDbInstanceAdminUser	Instance owner for the service integration bus database. This property is only required if the WAS.SibPersistMessages property is set to 'true'. This property is only required if the database is hosted on a Windows system.
	WAS.SibDbInstanceAdminPassword	Password for the instance owner of the service integration bus database. This property is only required if the WAS.SibPersistMessages property is set to 'true'. This property is only required if the database is hosted on a Windows system.
	WAS.SibDbRemoteAccessUser	Database server system user used to configure the service integration bus remotely. This property is only required if the WAS.SibPersistMessages property is set to 'true'.
	WAS.SibDbRemoteAccessPassword	Password for user ID named in WAS.SibDbRemoteAccessUser. This property is only required if the WAS.SibPersistMessages property is set to 'true'.
	WAS.VmmGroupRDN	Relative Distinguished Name of the location of VMM groups. For example, ou=groups,ou=SWG,o=IBM,c=US.
	WAS.VmmUserRDN	Relative Distinguished Name of the location of VMM users. For example, ou=users,ou=SWG,o=IBM,c=US.

© Copyright IBM Corporation 2011
IBM United States of America
Produced in the United States of America
US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PAPER “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes may be made periodically to the information herein; these changes may be incorporated in subsequent versions of the paper. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this paper at any time without notice.

Any references in this document to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
4205 South Miami Boulevard
Research Triangle Park, NC 27709 U.S.A.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.