



# Workgroup Data Server Administration

**Version 8.5**

**November 2017**

## Contents

Introduction .....	3
Overview .....	3
Recommended Server Requirements .....	4
Installing the Workgroup Data Server .....	4
Using Standard Workgroup Master Databases .....	5
Oracle and Microsoft SQL Server Workgroup Master Databases .....	6
Configuring the Workgroup Data Server .....	7
Authentication and Authorisation of Clients .....	9
Common Authentication and Authorisation Errors .....	10
Connecting Workgroup Clients to the Data Server .....	11
Upgrading the Workgroup Data Server to a New Version .....	12
Archiving in Standard Workgroup Master Databases .....	14
Appendix 1: Creating a Workgroup Database in SQL Server .....	16
Appendix 2: Creating a Workgroup Database in Oracle .....	17
Appendix 3: Updating a Workgroup Database in SQL Server .....	18
Appendix 4: Updating a Workgroup Database in Oracle .....	19

## Introduction

This document is a guide for systems administrators to the Innovyze Workgroup Data Server. The Workgroup Data Server must be installed and configured if using a Workgroup database with InfoNet or InfoWorks ICM (both examples of the Innovyze Workgroup Clients). From Version 7.5, the Workgroup Data Server is also capable of supporting Workgroup Databases for InfoWorks WS Pro and IWLIVE Pro.

The Workgroup Data Server is not required if using a Standalone database.

Note that the Workgroup Data Server was previously known as the Workgroup Co-ordinator.

## Overview

The Innovyze Workgroup Data Server is a server component which manages access to Workgroup databases by InfoNet, InfoWorks ICM, ICMLive, InfoWorks WS Pro and IWLIVE Pro (the Workgroup Clients). The Data Server is designed to improve the performance and reliability of database operations in a Workgroup environment.

Generally, a Workgroup database is recommended when

- more than one user is accessing the same master database
- low network bandwidth exists between the Workgroup Client and the server containing the master database.

The advantages of using a Workgroup Data Server are:

- Less network traffic:
  - Only changed data is sent between Workgroup Client and the Workgroup Data Server
  - Data is compressed
- Better performance:
  - The Workgroup Data Server is the only process accessing the data so it can be located on a local disk on the machine running Workgroup Data Server.

Workgroup databases may be hosted using the Innovyze Standard database or within an Oracle or SQL Server database.

The Workgroup Data Server is normally installed on a different computer to those used to run the Workgroup Client software. The same Workgroup Data Server can be used for many different master databases.

The Workgroup Client software communicates with the Workgroup Data Server using TCP/IP. By default, the port used is 40000. The port number may be changed.

## Recommended Server Requirements

The recommended system requirements for the machine running the Workgroup Data Server are as follows.

The software should be run on a physical or virtual server running a 64-bit Windows Server operating system e.g. Windows Server 2012 R2.

At least two processor cores should be available for either a physical or a virtual server.

A minimum of 4GB of RAM should be available. More RAM is recommended if the database size is large. For standard workgroup databases, to achieve maximum performance on a physical machine you would have more RAM than the size of the largest network database (.wdb) file on the server, up to about 16GB. Generally, it is recommended to have 16GB of RAM for a physical server. For a virtual server, it would be reasonable to start with 4GB of RAM allocated and monitor memory usage and increase if necessary.

For best performance and reliability the directory (default C:\ProgramData\Innovyze\SnumbatData) used to store standard databases should local to the machine running the WDS. It should not be on a file share, except under exceptional circumstances.

Overall storage space cannot be easily predicted, as it depend very strongly on the size of the networks to be managed and the presence of other ancillary data (such as ground models) which can increase the size of a database dramatically (tens of GBs). Be prepared to monitor the storage requirements for the database and expand as necessary.

## Installing the Workgroup Data Server

There are two version of the Workgroup Data Server available, it is important you install the correct version:

WorkgroupDataServer x64 - A 64 bit version for use on Windows x64. This is the recommended version for x64 Windows. If you are connecting to Oracle it requires the 64 bit version of the Oracle client. For SQL Server connectivity it requires the 64-bit Native Client.

WorkgroupDataServer x86 - A 32 bit version for use on Windows 32-bit (x86). If you are connecting to Oracle it requires the 32 bit version of the Oracle client. For SQL Server connectivity it uses the 32-bit Native Client.

The Windows version of the Workgroup Data Server can be installed by running the setup program. This setup will install a Windows service. Once installed the Workgroup Data Server will need configuring and the service started before use.

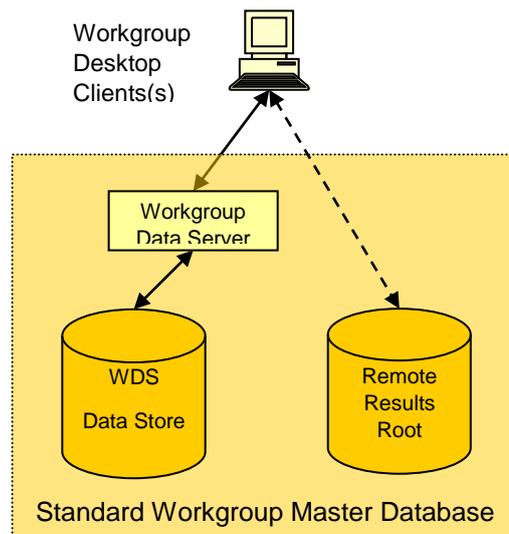
When the Workgroup Data Server starts up, it will send logging information to the Windows Application Event Log, confirming the configuration options that are in force. The source for Data Server events will appear as "Snumbat". It is good practice to review the Event log entries whenever the Data server is restarted, to verify that the expected configuration options have been applied.

## Using Standard Workgroup Master Databases

The Standard Workgroup Master Database is the default type of master database provided by the Workgroup Data Server. It does not require any additional 3<sup>rd</sup> party software. It is designed to provide the best performance for the supported Innovyze Workgroup products and can be used without further configuration of the server.

The architecture when using an Innovyze Standard Workgroup master database is shown below.

Note that the Remote Results Root shown in the diagram is not used for InfoNet clients as it is used to store simulation results which are to be shared amongst database users. This location is accessed via the standard Windows File Sharing protocol and is specified in the Workgroup client.



A standard workgroup master database will be located on a suitable server running the Workgroup Data Server. The default location varies according to the operating system and local configuration. Usually, files will be stored in the following location: "C:\ProgramData\Innovyze\SnumbatData".

The default path in versions of the server prior to 2.0 had "MWH Soft" rather than "Innovyze" in the path. Note that if you are upgrading from an earlier version and have an existing "MWH Soft" directory this will continue to be used and an Innovyze one will not be created.

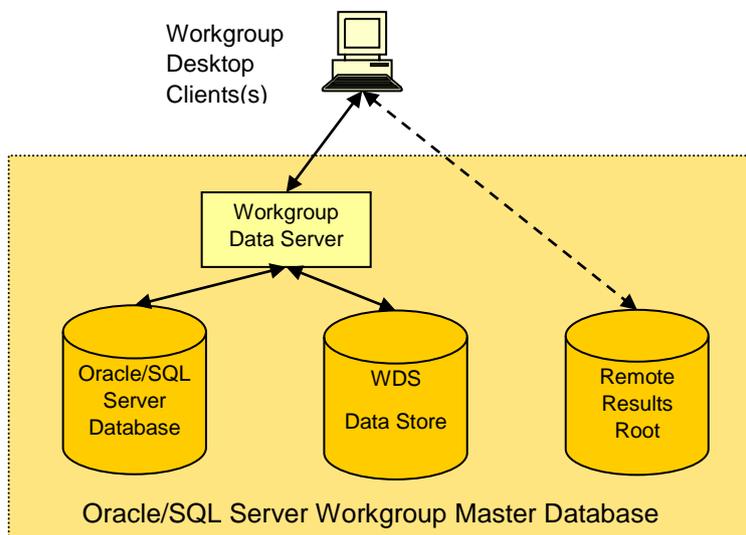
The data for each master database exists in a separate folder below this location (identified by the database name).

The files that make up the master database should not be modified outside of the Workgroup Client software, unless you are directed to do so by Innovyze support.

Only the Workgroup Data Server process needs access to these data files. For best performance they should be located on a disk local to the machine running the Workgroup Data Server. It is not recommended to put these files on a network file share.

## Oracle and Microsoft SQL Server Workgroup Master Databases

The architecture when using an Oracle or SQL Server master database is shown below. In an Oracle or Microsoft SQL Server configuration, the WGC Data Store contains the connection information required for the Oracle or SQL Server database. It also provides storage for photographs and TSDB data, as in the Standard Workgroup Database. All other data is stored in the Oracle/SQL Server database.



The Oracle or SQL Server database schema are created using scripts which can be downloaded from the Innovyze website or obtained by contacting support. Note that the scripts should be updated before use, to provide a unique value for the “database\_guid” field in the “global” table. ALL Oracle or SQL Server databases must have a unique value for this field. It is recommended that a GUID (Globally Unique Identifier) is generated to guarantee uniqueness.

The connection information for an Oracle or Microsoft SQL Server master database must be available to the Workgroup Data Server before it can be used. The connection information is provided by entering the details in a configuration file which exists at the root of the WGC Data Store directory for that database.

In the WDS DataStore directory create a subdirectory with the name you wish to call the database and the extension sndb. E.g. My database.sndb. Inside the subdirectory created above create a text file called master.ini. Inside this file add the required keywords to specify the connection to the Oracle or SQL Server database.

The keywords that follow depend of the type of master database in use:

Oracle Database Keyword Options	
DatabaseType	Always set to Oracle
OracleDatabase	The connect string to use to connect to the Oracle database server. This could a local net name or a URL (e.g. //machine://instance)
TableOwner	The owner of the Oracle tables (e.g. WGCDB)
Username	The database username to connect with. If this keyword is missing or blank then external credentials are used. On Windows this will use the windows user account under which the Workgroup Data Server service is running.
Password	The password to use. Not required if using external credentials

Example master.ini configuration file for an Oracle master database:

```
DatabaseType=Oracle
OracleDatabase=//power:/orcl
TableOwner=WGCDB
Username=WGCUSER
Password=password
```

Microsoft SQL Server Keyword Options	
DatabaseType	Always set to SQLServer
OLEDBProvider	The name of the OLEDB provider to use. Normally SQLNCLI11 for the SQL Server 2012 or SQL Server 2014 native client and SQLNCLI10 for the SQL Server 2008 native client.
Server	Name of the database server including the instance name if required (e.g. myserver\sqlexpress)
Catalog	Database name

Connections to SQL Server always use integrated security. Therefore it is important to run the Workgroup Data Server service under a user account that has access to the required SQL Server database.

Example master.ini configuration file for a SQL Server master database:

```
DatabaseType=SQLServer
OLEDBProvider=SQLNCLI11
Server=(local)\sqlexpress
Catalog=WGCDB
```

The SQL Server database must have Snapshot Isolation enabled. The following SQL command can be used to turn it on. Replace “MyDatabase” with the name of the SQL Server database.

```
ALTER DATABASE MyDatabase SET ALLOW_SNAPSHOT_ISOLATION ON
```

## Configuring the Workgroup Data Server

There are a few optional configuration parameters that may be set for the Workgroup Data Server. These options are set in a simple text file called **snubat.ini**. The Workgroup Data Server installer does not install a default version of this file. You will have to create it yourself if you want to change the default settings. Note it is not necessary to use a snubat.ini if you are using a standard workgroup database. The file should be located in the directory where the Workgroup Data Server is installed, the directory containing snubat.exe, which is normally “C:\Program Files\ Innovyze Workgroup Data Server”. The file should use UTF-8 encoding if it contains non-ASCII characters.

All parameters are optional and have the format keyword=value. Any line that starts with a # in the first column is a “comment” line and is ignored. Any parameters which are changed by this mechanism will generate an entry

in the Windows Application Event Log when the Data Server is started, confirming that the change has been applied. As usual, it is viewed as good practice to review the Event Log after started the Data Server to verify these parameters are in force.

Keyword	Value
Port	Specifies the TCP port number to listen on. The default value is 40000
DataPath	Specifies the data directory for the WDS Data Store. For best performance and reliability this should be on a local drive and not on a network share. A warning will be generated in the Event log if this drive does not appear to be a local drive. The Workgroup Data Server Service will not start if DataPath is set to a location that cannot be accessed. In this case an error will be put in the event log. The default value is C:\ProgramData\Innovyze\SnumbatData
LogToFile	0 - Log output is sent to the Windows Event log. 1 - Log output is sent to a file called snumbat.log in the root of the WDS Data Store directory. Important errors and warning will still also be written to the Windows Event Log. The default setting is 0
LogLevel	Specifies the log level threshold. Each level adds more detail. 4 – Errors only 3 – includes warnings 2 – includes start-up/shutdown information 1 – includes general information about usage (to log file only) 0 – includes debug information (to log file only) The default setting is 2. We do not recommend setting a higher value.
DisableReverseDNS	The Workgroup Data Server uses reverse DNS to lookup the name of incoming connections. If reverse DNS is not setup for your network this lookup might add a second or two to each connection to the Workgroup Data Server. Setting this parameter to 1 will disable the lookup. The default setting is 0
AllowDatabaseCreation	0 – Creation disallowed 1 – Creation allowed The default setting is to allow database creation by clients.
AttachmentPath	Specifies the directory to be used to store InfoNet attachments. The default location is “C:\ProgramData\Innovyze\SnumbatData\Attachments”. This need not be specified as a local drive.

**Example snumbat.ini with the default options set:**

```
Port= 40000
#DataPath=
LogToFile=0
LogLevel=2
DisableReverseDNS=0
AllowDatabaseCreation=1
```

## Authentication and Authorisation of Clients

If the Workgroup Data Server (WDS) and all the clients are using Active Directory it is possible to configure the WDS to perform authentication and authorisation checks on connecting users. Authorisation checks can be done at the server and database level.

Authentication is not available when using older clients. ICM 8.0, InfoNet 18.0 or WS Pro 2.0 or later are required.

By default Authentication is not enabled. If enabled (with the AuthType keyword) it will be attempted each time the client connects to the server. The authentication will be done for the user running the client software, it is not necessary or possible for the user to enter alternative credentials. Note that some products (e.g. ICM Live) have services that access the WDS.

The server can be configured to require the authentication to succeed in order for the connection to succeed (by using the AuthMandatory keyword). If you enable this older clients will not be able to connect to the WDS. The Authorisation check allows the users who can connect to the server or use a database to be controlled. To enable authorisation the AuthRequiredSecurityGroup keyword is used to specify an AD group to which the connecting user must belong.

The AuthRequiredSecurityGroup keyword can be set to restrict access to the whole server by placing it in snumbat.ini and/or for each individual database by placing it in the master.ini for each database. Errors and warnings generated by the WDS will be written to the Event Log or the log file, these can help with diagnosing any problems. Additional diagnostic information is available if the LogLevel is reduced to 1 or 0 and the output is set to be a file.

The following keywords may be specified in the snumbat.ini file to enable authentication and authorisation:  
Keyword in snumbat.ini Description

Keyword in snumbat.ini	Description
AuthType	Blank – No authentication is attempted (default) Negotiate – Authentication will be attempted when the client connects to the server.
AuthMandatory	0 – Client can still connect even if authentication fails (default) 1 – Client will not be allowed to connect if authentication fails. Note this will prevent older clients which do support authentication from connecting to this Workgroup Data Server.
AuthRequiredSecurityGroup	Blank – No authorisation check when connecting to server. Name of AD security group to which user must belong in order to be allowed to connect to this Workgroup Data Server. The client will not be able to connect to the server if authentication failed, the user account does not belong to specified AD group or if the group cannot be found. Note this check will only be enforced if AuthMandatory is 1

The following keywords may be specified in a database master.ini to enable a database specific authorisation check:

Keyword in master.ini	Description
AuthRequiredSecurityGroup	Blank – No authorisation check when opening database Name of AD security group to which user must belong in order to be allowed to use this database. The client will not be able to use the database if authentication failed, the user account does not

	belong to specified AD group or if the group cannot be found.
--	---

The most common configurations of these settings would be to either all full access without authentication (the default), or to restrict access to all databases at the WDS level. To restrict all databases managed by a WDS you would use the following.

**snumbat.ini:**

```
AuthType=Negotiate
AuthMandatory=1
AuthRequiredSecurityGroup=AD Security Group WDS
```

To allow a mixture of unrestricted and restricted databases, you should make the WDS authentication optional and update the master.ini file for each database with restrictions.

**snumbat.ini:**

```
AuthType=Negotiate
AuthMandatory=0
```

For each restricted databases: **master.ini:**

```
AuthRequiredSecurityGroup=AD Security Group DB
```

## Common Authentication and Authorisation Errors

If there are problems with authentication or authorisation the following error messages can be generated by the WDS and returned to the client.

**When connecting to the WDS***Authentication failed on server*

The authentication failed but was required (AuthMandatory is 1). Some additional information about why is included in the error message. Further information will be logged on the server.

*Unable to access server, checking authorisation failed*

The WDS was unable to perform the required authorisation check. More details will be logged on the server. A common cause of this is that group specified by the AuthRequiredSecurityGroup keyword is incorrect and cannot be found.

*User is not authorized to access this server*

The authorisation check was done but the user is not a member of the group specified by the AuthRequiredSecurityGroup keyword.

*Unexpected error checking authorisation*

An unexpected error occurred when performing Authorisation check. The server log will have more details.

**When attempting to open a database**

User authentication is required to access this database

The authentication check done when the user connected to the WDS failed and it was not specified to be mandatory. The database required an authorisation check, but this cannot be done as the authentication failed.

*Unable to access database, checking authorisation failed*

The WDS was unable to do perform the required authorisation check. More details will be logged on the server. A common cause of this is that the group specified by the AuthRequiredSecurityGroup keyword is incorrect and cannot be found.

*User account is not authorized to access this database*

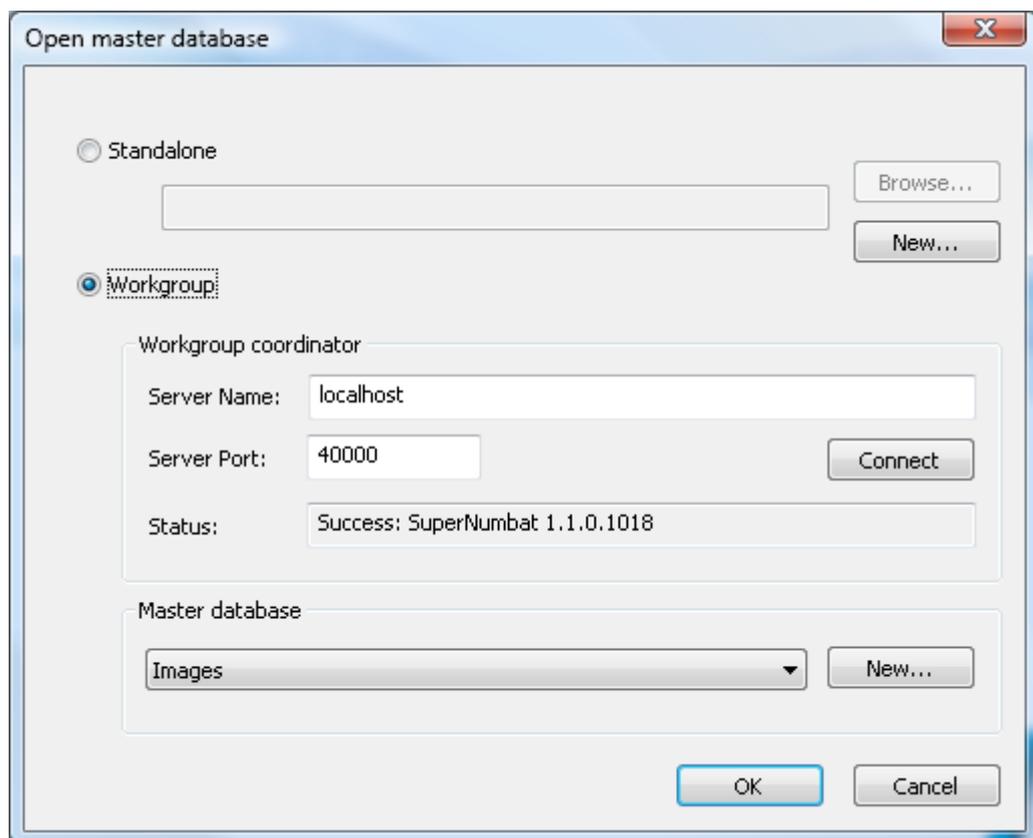
The authorisation check was done but the user is not a member of the group specified by the AuthRequiredSecurityGroup keyword.

*Unexpected error checking authorisation*

An unexpected error occurred when performing Authorisation check. The server log will have more details.

## Connecting Workgroup Clients to the Data Server

To connect to the Data Server Workgroup Clients need to know the hostname of the machine running the Workgroup Data Server and the port to connect to. This information can be specified when opening an existing database or creating a new master database.



- **Server address** - The name or IP address of the computer running the Workgroup Data Server.
- **Server port** - The TCP port that the server is listening on. Leave blank for the default port.

Press the Connect button to check that the client can connect to the Data Server and to populate the combo box listing the master databases which are managed by that Workgroup Data Server.

## Backing up Workgroup Databases

It is important to ensure that the valuable data stored in your Workgroup databases is regularly backed up. For databases stored in Oracle or SQL Server databases, it is assumed that standard server backup techniques will be in operation. These should address the backup requirements for most of your data.

Some data is stored in the local “.sldb” folder for the database, even when using Oracle or SQL Server type databases. Examples of such data include Attachments, Ground Models and TSDB data objects. As a result, independent backup of the Standard Workgroup Database locations is always required (as described below).

For Standard Workgroup Databases, the following information should be observed.

A backup procedure should backup all the files such that if a restore is required a consistent snapshot of the whole set can be restored. Backups should be done whilst Workgroup Clients are not in use. To enforce this, the Workgroup Data Server service can be stopped, a backup that uses Windows Volume Shadow Copy Service started and the service immediately started again. There will only be a very short downtime.

If you are using the default settings, then it is sufficient to back up all the files and folders in the default storage location: C:\ProgramData\Innovyze\SNumbatData. If you have specified an alternative location for the “DataPath” or the “AttachmentPath”, then you will need to back up all files and folders in these specified locations.

It is possible to backup an individual database by copying the files within a specific “.sldb” folder. Note that this will not backup the attachments associated with that database, as attachments are stored in a separate location.

For modelling applications, you may also wish to back up any results stored in the Remote Results Root at the same time to maintain a completely consistent dataset. This step may be viewed as optional, since the ability to re-run simulations at any time means that data in the Remote Results Root can be recreated from the information in the Workgroup Database (see the IT Architecture Guide for more information on the Remote Results Root).

## Upgrading the Workgroup Data Server to a New Version

Before updating your Workgroup Data Server, you should ensure that you have a backup of you data (see *Backing up Workgroup Databases*).

The existing older Workgroup Data Server service should be stopped before attempting to install a newer version. You do this by opening the Control Panel and browsing to the Local Services and stopping the “Innovyze Workgroup Data Server” service. Obviously, this will interrupt the usage for Workgroup Client applications and you will want to choose a time when this interruption with not cause problems.

If you are updating an existing version of the Data Server, you will need to uninstall the current version before you can install the new version.

To upgrade the Data Server all you should need to do is uninstall the old version and run the installer for the new version of the Data Server. The new version of the Data Server should start automatically and existing clients should be able continue working immediately.

Major version numbers for a release are the first two numbers on the version (e.g. 6.5 or 7.0). Versions which differ only in the third number are known as “patch” versions (e.g. 7.0.2).

Newer versions of the Data Server are able to manage databases from older versions of the Data Server and accept connections from older clients to such databases. Clients with major version numbers which are newer than the data server major version will generate an appropriate error if they try and connect.

When a database is created using a Workgroup Client, the database version is set by the client version - not the server version. A client with a newer major version number will be unable to open an older database unless the database is upgraded using the client.

If the data server is being used to manage a database hosted using Oracle or SQL Server, then the Oracle or SQL Server database schema will need to be updated using the update script. The update script provided only updates from the previous major version number to the current major version number. If you are updating across multiple major version numbers, it will be necessary to install the data server for each version in turn and apply the update scripts. The update scripts can be downloaded from the Innovyze website or obtained by contacting support.

## Archiving in Standard Workgroup Master Databases

This section only applies to standard workgroup master databases, not when using Oracle or SQL Server.

In a standard workgroup master database all the version history of a version controlled network is stored in a .wdb file with a file name of the form "sXXX-Y.wdb". Here XXX is a 3 digit number which identifies the network type and Y is the object id as shown in the Workgroup Client User interface (via the Object properties page or tooltip). Useful values for XXX in this context are as follows:

134 - InfoNet Collection Networks

135 - InfoNet Distribution Networks

169 - ICM Model Networks

190 - SWWM Live Model Networks

205 - InfoNet Asset Networks

If you have a large network and make many changes to it, for example via InfoNet Mobile, this .wdb file can get very large (many 10s of Gigabytes). In order to improve the performance of the WDS and reduce the time required for backup there is a command line utility available to move old versions of network objects to an archive file. Other files in the in the workgroup master database will not support archiving.

The following shows an example of how to use the archiving utility wdbarchive.exe.

***Always ensure you have a backup of your master database before doing any archiving.***

The example below show the archiving of a large InfoNet Collection Network for wdb file s134-4.wdb located in the default place for a database called MyDatabase.

- 1) Ensure you are using a user account that has permission to access the WDS data file.
- 2) Open a command prompt.
- 3) Change directory to the location of the file:

```
cd /d C:\ProgramData\Innovyze\SNumbatData\MyDatabase.sndb
```

- 4) Run the archiving utility:

```
"C:\Program Files\Innovyze Workgroup Data Server\wdbarchive" s134-4.wdb
```

- 5) The file s134-4-archive.wdb will either have been created or new data add to the existing one.
- 6) Once the archiving is done it is recommended that the main file is compacted with the command:

```
"C:\Program Files\Innovyze Workgroup Data Server\wdbcompact" s134-4.wdb
```

***Ensure you have a backup of your master database before doing any archiving.***

Network version control operations cannot be done by clients whilst the archiving is in progress. It is recommended to prevent clients from accessing the master database whilst performing archiving, usually by stopping the Workgroup Data Server service.

The archiving may be interrupted by pressing control-C. This will save the archiving done so far, running the archive utility again will resume archiving.

The archive-wdb file is only modified by wdbarchive, therefore incremental file backups of the master database files will be done much more quickly. Although the use of archiving will not reduce the overall storage needs of the master database, it can make significant reductions in backup time where incremental file backups are used.

## Appendix 1: Creating a Workgroup Database in SQL Server

The following is checklist for the creation process of a Workgroup Database in SQL Server.

- 1) Download the appropriate creation script from the Innovyze website (or from the WDS installation directory for versions prior to 8.0). Make sure that you have the correct scripts for your application. Either:
  - a. ICM/ICMLive/InfoNet or
  - b. WS Pro/IWLive Pro/DemandWatch Pro.
- 2) Open the SQL Server creation script, `SQL_Create.sql`, in a text editor.
- 3) Find the line near the end of the script, which starts:  
`INSERT INTO global ...`
- 4) Replace the default database identifier “SQL\_INNOVYZEWG00” to a unique value. This will normally be the last argument in the INSERT statement.
- 5) Select “Snapshot isolation” by removing the comment from the last instruction in the script and replacing MyDatabase with the SQL database name (not the WDS database identifier):

```
ALTER DATABASE MyDatabase SET ALLOW_SNAPSHOT_ISOLATION ON
```

The following steps are usually carried out using SQL Server Management Studio.

- 6) Create an empty SQL Server Database with the same name as used in Step 5.
- 7) Run the scripts.
- 8) Check that all instructions ran without errors and that the global table has a single row.

On the machine running the WDS:

- 9) Create an empty folder in the WDS Datatore directory, using a database name suitable for end users. Ensure that the folder name ends with “.sndb”, so that it is identified as a database folder to the WDS.
- 10) Create the master.ini file within this folder (see earlier in this document for how to do this).
- 11) Clients should now be able to connect to this database in the usual manner.

## Appendix 2: Creating a Workgroup Database in Oracle

The following is checklist for the creation process of a Workgroup Database in Oracle.

- 1) Download the appropriate database and role creation scripts (Ora\_create.sql and Ora\_roles.sql) from the Innovyze website (or from the WDS installation directory for versions prior to 8.0). Make sure that you have the correct scripts for your application. Either:
  - a) ICM/ICMLive/InfoNet or
  - b) WS Pro/IWLive Pro/DemandWatch Pro.
- 2) Open the Ora\_Create.sql script in a text editor.
  - a) Find the line near the end of the script, which starts: INSERT INTO global ...
  - b) Replace the default database identifier “SQL\_INNOVYZEWG00” to a unique value. This will normally be the last argument in the INSERT statement.
- 3) Open the Ora\_Roles.sql script in a text editor.
  - a) Replace the string “CHANGETHIS” with the name of the database Table Owner (as specified in the master.ini file).
  - b) Replace the string “INNOVYZEUSER” with the name of the database User (as specified in the master.ini file).

The following steps are usually carried out using Oracle SQLPlus.

- 4) Log in to Oracle as the Table Owner for the database.
- 5) Run the Ora\_create.sql script.
- 6) Run the Ora\_Roles.sql script.
- 7) Ensure that the database transactions are completed.
- 8) Check that all instructions ran without errors and that the global table has a single row (select \* from global).

On the machine running the WDS:

- 9) Create an empty folder in the WDS Datatore directory, using a database name suitable for end users. Ensure that the folder name ends with “.sndb”, so that it is identified as a database folder to the WDS.
- 10) Create the master.ini file within this folder (see earlier in this document for how to do this).
- 11) Clients should now be able to connect to this database in the usual manner.

---

## Appendix 3: Updating a Workgroup Database in SQL Server

The following is checklist for the update process of a Workgroup Database in SQL Server.

Note that the update scripts for a SQL Server database will always update by a single major version number e.g. 5.0 to 5.5, or 5.5 to 6.0. To update between non-consecutive major version numbers, all intermediate scripts must be run in the correct order.

- 1) Download the appropriate update script(s) from the Innovyze website (or from the WDS installation directory for versions prior to 8.0). Make sure that you have the correct scripts for your application. Either:
  - a. ICM/ICMLive/InfoNet or
  - b. WS Pro/IWLive Pro/DemandWatch Pro.
- 2) The script names identify the products and the from and to versions of the update process, e.g.  
`SQL_update_from_ICM75IN175_to_ICM80IN180.sql`  
Note that no manual editing of the update scripts should be required.
- 3) Using SQL Server Management Studio, run the appropriate update scripts in turn to update from the current version number to the desired version number. Check that no errors are reported.
- 4) Connecting to the database using the Workgroup client should tell you that a subversion update is required. Allow the subversion update to proceed.
- 5) The update is now complete.

## Appendix 4: Updating a Workgroup Database in Oracle

The following is checklist for the update process of a Workgroup Database in Oracle.

Note that the update scripts for an Oracle database will always update by a single major version number e.g. 5.0 to 5.5, or 5.5 to 6.0. To update between non-consecutive major version numbers, all intermediate scripts must be run in the correct order.

- 1) Download the appropriate update script(s) from the Innovyze website (or from the WDS installation directory for versions prior to 8.0). Make sure that you have the correct scripts for your application. Either:
  - c. ICM/ICMLive/InfoNet or
  - d. WS Pro/IWLive Pro/DemandWatch Pro.
- 2) The script names identify the products and the from and to versions of the update process, e.g.  
`Ora_update_from_ICM75IN175_to_ICM80IN180.sql`  
`Ora_update_roles from_ICM75IN175_to_ICM80IN180.sql`
- 3) In the update roles script(s):
  - a. Replace the string “CHANGETHIS” with the name of the database Table Owner (as specified in the master.ini file).
  - b. Replace the string “INNOVYZEUSER” with the name of the database User (as specified in the master.ini file).
- 4) Using SQLPlus, logged in as the Table Owner, run the appropriate update scripts in turn to update from the current version number to the desired version number. Check that no errors are reported. Ensure that the transaction is completed.
- 5) Connecting to the database using the Workgroup client should tell you that a subversion update is required. Allow the subversion update to proceed.
- 6) The update is now complete.