CU2 Global Pty Ltd
The Global Data Conversion Experts

ConvertU2 Technologies
The Data and Software Conversion Experts

2SQL Set-Up in High Security Environments

December 2013

Overview

There are many potential applications of the 2SQL conversion and migration program that can occur in highly secured data environments. This ranges from organizations holding detailed personal and financial information on their customers, to security organizations that have highly confidential and sensitive information.

Under normal conditions much of the 2SQL program is able to be executed remotely given that a customer authorizes a copy of the application and data to be taken off site. However in cases where it is highly unlikely that an organization will allow a copy of their Access application and data to leave their secured environment there are strategies that can be adopted.

It is highly recommended that this documents be read in conjunction with the 2SQL Detective Quick-Start Guide. The latest version of the guide can be obtained from our web site at http://www.cu2global.com/info-store/library

Operational Considerations

2SQL has three key components of its program:

- The MSO Inspector, which audits and reports on a customer's Access and Excel file population.
- The Detective, which conducts a detailed analysis of individual Access applications and databases in order to determine the work effort involved in converting the applications to SQL Server.
- The Genie, which conducts the conversion and migration process, auditing and logging all changes that have been made and reporting on issues that need to be rectified manually.

Each of these components has prerequisite requirements which must be considered in conjunction with the customer's security policies.

MSO Inspector

MSO Inspector requires access to network drives or copies there-of.

The MSO Inspector requires access to a company's network drives, and therefore the data, in order for it to perform its tasks. In high security environments this access can occur either:

- Within the secured corporate environment under the control of 'trusted' users/individuals.
- Or copied to a secured and then isolated virtual/physical machine within the secured environment.

The Detective.

The ***Detective*** can operate onsite either with or without the corporate data.

The Detective can operate in one of two Authorized Access modes in order to perform its analysis:

- Full Data and Application access mode – where the Detective has access to both the corporate MS Access applications and the associated data.

  The resultant analysis of 'Issues to be resolved automatically or manually' is more comprehensive whilst in this mode as both the MS Access applications and data contribute toward 'Issues to be Resolved'.

- Data exclusion mode - where the Detective has access only to the corporate MS Access applications and NOT the data.

The resultant analysis of 'Issues to be resolved automatically or manually' is less comprehensive than in Full access mode as the Detective only has access to the MS Access applications and NOT the associated data. As both the applications and data

contribute toward 'Issues to be Resolved' the resultant issue count from this mode is typically 20% – 30% lower than would otherwise have been reported.

This delivers a very good estimate of conversion complexity albeit not as accurate as the one delivered from the Full access mode.

Both of the Authorized Access modes can occur:

- Within the secured corporate environment under the control of 'trusted' users/individuals,
- Or where the MS Access applications and data have been copied to a secured and then isolated virtual/physical machine within the secured environment.

The ***Detective*** can operate remotely in *Data Exclusion* mode.

Additionally, some organizations may be comfortable to allow The Detective to operate offsite in the Data Exclusion mode as only a copy of the corporate applications are required and NOT the data itself.

The Genie

The Genie needs access to both the MS Applications and its associated data in order to perform its conversion and migration work. As with the MSO Inspector, in high security environments this access can occur either:

- Within the secured corporate environment under the control of 'trusted' users/individuals.
- Or copied to a secured and then isolated virtual/physical machine within the secured environment.

At the end of the automated conversion and migration process there remains 'clean-up' work to be performed. As with the Detective in Data Exclusion mode, this work may be able to be performed offsite as it is not absolutely essential to have access to live data, just the corporate applications are required.

In this way additional expertise may be engaged without compromising security concerns. By having this additional expertise work on only specific issues their visibility of the application as a whole is severely limited, reducing exposure to potential security risks.

However it should be noted that final testing and confirmation of the 'clean-up' resolutions would need to be conducted back onsite again, within the secured corporate environment.

Secured Sandpit Environment

In most cases the logical option is to create a secured and isolated environment within the customer's own secured environment. This can be done quite simply by:

- Creating a VM preconfigured with 2SQL, which now includes the MSO Inspector.
- For the MSO Inspector, depending on the size of the network being scanned, either copying the network drive to the image, or modifying the image to allow access to the network drive and no other networks.
- For 2SQ's Detective and Genie components, moving the Access Application and all dependencies to this image, and disconnecting the image from customer environment.

This basically creates a sandpit environment where the customer's security policies/recommendations can be enforced and one where only the customer or authorised personnel have access to the image.

Activating 2SQL in a Secured Environment

2SQL requires access to the internet to be able to finalize the installation and activation process. Prior to commencing conversion and migration, 2SQL also needs to interrogate its 'Issue' account balance credit in order to confirm the number of issues that have been paid for on behalf of a specific customer.

Some customer environments may not allow access to the internet as a matter of security policy. In this case the activation of the 2SQL components is able to continue through the use of a secondary manual activation process.

Manual activation is a process that is unique to each customer installation. It is therefore conducted under strict control and guidance by CU2 Global support services.