LESSONS LEARNED IMPLEMENTING DOORS IN A CITRIX ENVIRONMENT

By

Marie Bussman

SCIENCE SYSTEMS AND APPLICATIONS, INC.

Prepared for the 2005 Telelogic Americas User Group Conference

Lessons Learned Implementing Doors in a Citrix Environment

Abstract

NASA's James Web Space Telescope (JWST) Project is a large multi-national project with geographically dispersed contractors that all need access to the Projects requirement database. Initially, the project utilized multiple DOORS databases with the built-in partitions feature to exchange modules amongst the various contractor sites. As the requirements databases matured the use of partitions became extremely difficult. There have been many issues such as incompatible versions of DOORS, inefficient mechanism for sharing modules, security concerns, performance issues, and inconsistent document import and export formats. Deployment of the client software with limited IT resources available was also an issue.

The solution chosen by JWST was to integrate the use of a Citrix environment with the DOORS database to address most of the project concerns. The use of the Citrix solution allowed a single Requirements database in a secure environment via a web interface. The Citrix environment allows JWST to upgrade to the most current version of DOORS without having to coordinate multiple sites and user upgrades. The single requirements database eliminates a multitude of Configuration Management concerns and facilitated the standardization of documentation formats. This paper discusses the obstacles and the lessons learned throughout the installation, implementation, usage and deployment process of a centralized DOORS database solution.

Author Biography

Marie Bussman

As a Senior Systems Administrator I have over twenty years of Information Technology experience and hold a Bachelors of Science in Information Systems Management. Fifteen of the twenty years of experience have been within the NASA environment at Goddard Space Flight Center (GSFC). I have experience in network and server administration primarily in the Windows world and client server application deployment and management. I have four plus years experience in working with the Doors software and various components as the Administrator and user support person.

Contact: Marie Bussman, Senior Systems Administrator, SSAI, 301-286-0868,

marie.busman@gsfc.nasa.gov.

1   Introduction

JWST is an infrared observatory that will study galaxy formation in the universe. It will consist of multiple instruments each with different functions and design requirements and built at different locations. JWST is a complex project that requires a simple and efficient way to track the complex requirements with a high degree of accuracy and efficiency and a low degree of risk.

1.1   Initial Environment

The initial environment at GSFC consisted of DOORS 6.0 SR 1 with multi-site licenses installed on an older Fileserver with Windows 2000 Server Operating System along with DOORSnet, SYNERGY/Change, SYNERGY/CM, ECPS, Doc Express Factory and Word.

1.1.1   User Scenario

Seventy-Five users accessed the JWST DOORS database server from the DOORS client software installed on each workstation. If the user was on a wireless network at GSFC or was an offsite user, Virtual Private Network (VPN) software had to be installed and a Domain account created in addition to the DOORS Client. In most cases additional support people were brought in to resolve firewall issues and workstation issues.

In addition to the JWST DOORS users accessing the GSFC DOORS database, there were additional remote users at the various contractor and partner sites accessing their own local DOORS databases to track requirements and produce modules.

Sharing of modules was required between GSFC and other contractor sites and was done through partitioning with the prime contractor being the 'Master' and controlling the partitioned modules. The partitioned modules were placed on a file repository to be retrieved and restored into the appropriate DOORS database.

The Authors/Project Administrators would export the modules from DOORS using Telelogic DOC Express Word or Factory as a MS Word document and mark the document with changes expecting the document to import back into DOORS without any problems. The problem with this was that requirement numbering would change and linking if any was done would be broken. There was also a strong possibility of content error, such as missing or duplicated text as well as formatting and style issues.

Placement of the information from the Module into the MS Word document was determined by a DOORS enumerated attribute setting, DE Code. The DE Code included such enumerators as Requirement, Rationale, and Figure Caption.

1.1.2   Support Scenario

The initial process for support and maintenance of the DOORS implementation at JWST was a single person who was the central administrator that was responsible not only for server administration but also DOORS administration and client deployment. This person was also

responsible for trouble shooting user issues. As a result of the limited resources installation and troubleshooting could take more than a day or two from when request for support were made.

2   <u>Defining the Problem</u>

The requirements tracking process for JWST presented some challenges such as the distribution of the users across the continent, Canada and Europe. Each location has a different process in place for documentation, configuration management and requirements tracking. The one factor most of the sites had in common was the Telelogic DOORS software. Unfortunately the DOORS versions varied by location, as did the format of the documentation and the configuration management process used to manage the information. Reports produced at the different locations did not necessarily contain the same attributes and information required for tracking.

Several of the remote DOORS servers were company based and the ability to upgrade to new versions of the software without impacting other projects made it difficult. The companies also were very hesitant in allowing remote users access to their DOORS servers. The remote contractors had firewalls at their location and were unable to open the ports necessary to use the application directly or in some cases through the VPN software. DOORSnet was evaluated as an alternative, but found to be lacking in its capabilities. The DOORSnet display did not allow easy or quick viewing of the information depending on the size of the modules. Importing and exporting of documents was also a concern with DOORSnet.

Distribution of the client software and patches was difficult and time consuming requiring visits to the local user workstations at GSFC or providing the remote users the software and talking them through the process via telephone.

A key element in the requirements tracking process, linking, was limited because it could not be done at the needed levels if the modules were in different DOORS databases at different sites. DOORS has the partition function and archiving functions to bridge some of the gaps of sharing data. The dynamic nature of the information made the partitioning difficult to maintain and left uncertainty about where the latest information was located for any particular module. Efforts were made to have a centralized partition management schema with one site being the 'Master' but that limited control and access by the JWST Project at GSFC. The archiving function meant the loss of linking information and the constant need for taking snapshots of the modules and re-sending them. The GSFC Configuration Management office also had concerns about documents under their control residing on other DOORS servers.

In addition the requirement numbering and formatting were often not compatible with the format required, manipulation and time consuming auditing of the work to verify accuracy and to produce the document output in a format acceptable to our Configuration Management office was needed.

3   <u>Evaluating and Determining a Proposed Solution</u>

It was necessary to come up with an alternative that was secure, with acceptable performance and that could be accessed from anywhere without having to open ports in remote firewalls at the contractor or vendor sites. The solution also had to include the capability for common templates and agreed upon standards to be used by all groups as well as a process to import and export documents in a format acceptable to Configuration Management. Telelogic's recommendation was to implement a Citrix solution. Citrix is a software application that allows the distribution and hosting of applications via a central location across various types of networks and remote access points. We chose to go with the Citrix Enterprise version (Xpe) that allowed growth and provided additional resources to manage the Citrix farm. A Citrix farm is a pool of servers that allow the distribution and load balancing of applications in this environment.

3.1 The Potential Options

Multiple meetings were held with the local firewall and network groups to discuss the best and most secure Citrix configuration. We had a third party vendor assist in these meetings and also setup the initial environment. The solution was only the start of the process. The next step was to sell the solution to the project management and the remote contractors who were authoring the majority of the requirements documents. Several presentations were prepared and presented. A trade study was done with several alternatives analyzed. They were:

- Stay the same
- Host at a third party site
- Host at the prime contractor site
- Host at Goddard Space Flight Center (GSFC)

Each option had pros and cons. The decision was made to host it here at GSFC because of the security requirements as well as cost benefit. The third party site and prime contractor sites' would have to buy additional licensing and upgrade their licensing from single site to multi-site licensing. GSFC had GSA pricing and enough software licenses in place. The other options would also have to procure additional hardware and modify their network infrastructure to accommodate the environment and still meet their company restrictions.

3.2 Questions About the Solution

Even after the presentations and meetings several questions were raised and needed to be explained. Questions like: Why Citrix? Why Windows 2003? Doesn't DOORS have a Relational database backend? Answering these questions helped solidify the best scenario for the solution. Those questions were answered with the following responses:

Why Citrix and not just Terminal Server? At the time Microsoft's RDP protocol didn't seem to us to be as robust in performance and compatibilities as the Citrix ICA protocol was in handling memory and caching. Why not the Full Citrix Client? The Full Citrix client would require ports be opened on the remote firewalls and the contractors were not willing to do that. Ports being open was the same reason Virtual Private Network client software was not chosen. The use of the web client did not require any vendor specific ports and was easy to install and update.

Why not DOORS XT? Although having an Oracle back end to the data would be nice DOORS XT did not have all the functionality needed and currently being used within DOORS. DOORS XT will be re-evaluated at a later time.

Why did we choose Windows 2003 server? Windows 2003 server is the NASA recommendation and had more security features than Windows 2000 server.

Does Telelogic have a tool that is integrated within DOORS for Configuration Management Reporting usage? Telelogic Synergy Integration can be used as a CM tool with DOORS. It requires CM Synergy, Change Synergy and DOORS in order to work. We have all those components and are planning on utilizing the DOORS integration for some of the CM process in the future.

3.3 New Environment

Through the course of discussions and meetings an optimum configuration was determined. Three servers were ordered with an option to expand the system to support more users over time. The Secure Gateway was a very basic server configuration and ordered with the Standard Windows 2003 operating system while the Citrix Metaframe Presentation Server and the DOORS application server were ordered with more memory and disk space and they both had the Enterprise version of the Windows 2003 Server software for increased memory and CPU scalability.

The new environment consist of DOORS 7.1 multi-site licenses on a new Fileserver with Windows 2003 Operating System and SYNERGY/Change, SYNERGY/CM, SYNERGY/DOORS Integration and WEXP. Additionally there are two servers with the Citrix software components in the environment.

This configuration allowed for a secure environment yet limited the accessibility to specific individuals and groups. Although it was not recommended we combined several of the Citrix components as a cost saving measure. We felt we could combine the web interface and Secure Gateway features on one server without a performance hit because the server was only going to be used for authentication, which does not require heavy resources. There was also some concern about jeopardizing security but because we knew there was controlled access to the secure sub network as well as firewalls and access control list where the server was located it was not a major concern. Performance would be handled as the environment grew by adding more Citrix Presentation Servers to the Citrix Farm as needed. Since we were just starting out we were not sure of the number of concurrent users but figured 8-10 concurrent DOORS users per Citrix Server initially as a starting point.

3.4 User Scenario

All users including remote users at the contractor and partner sites log in via a secure Citrix web interface to DOORS using an Internet Web Browser. The following is a generic diagram of the scenario implemented.
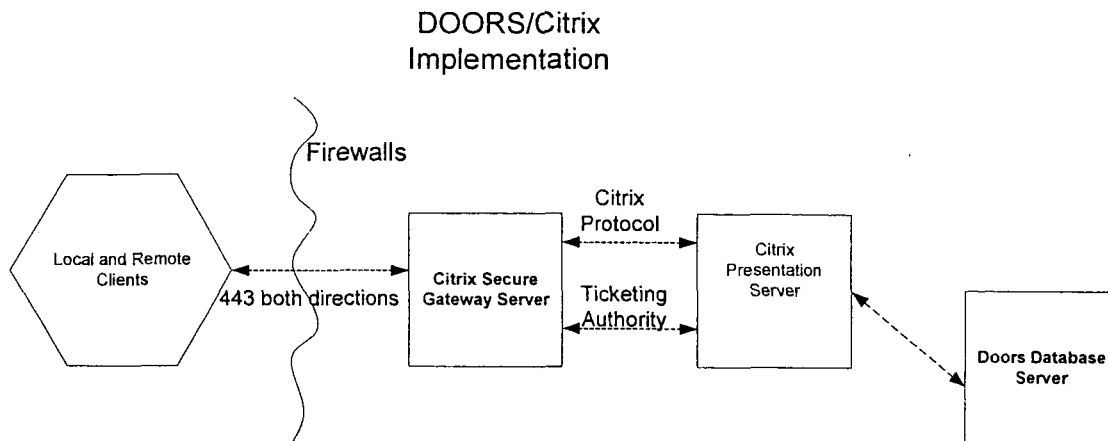
DOORS/Citrix
Implementation

Figure 1. DOORS Implementation

The first time the user accesses the interface they download the client plug-in. Access to the interface is still controlled by firewalls and Access Control List. Once the Citrix plug in is installed and DOORS is accessed, module access is determined by individual and group permissions. There are two areas in DOORS, one for the users to use as a sand box or play area for learning or works in progress, and it is setup by folders for each vendor/remote site and then subfolder for each user. The other area is the 'Production' area for modules that have been through the Configuration Control at the appropriate remote site. The modules in the Project area are in a hierarchy based off the JWST Project document tree.

3.5   Support Scenario

In addition it was necessary to implement a support architecture to allow for at least one if not several Point of Contacts (POC) at each location. The POC is called the Project Administrator. The Project Administrator is aware of the unique requirements and processes at their site as well as the process for gaining access to the GSFC site. The Project Administrator tries to resolve issues prior to contacting the Doors Administrator at GSFC.

4   Lessons Learned During Planning and Setup

During the setup and implementation process there were hurdles to over come. The following information is an overview of the processes and steps taken to implement the proposed solution and some of the lessons learned along the way.

During the setup and design of the environment a lot was learned about licensing of both DOORS and the Windows Terminal Services Client as well as the configuration requirements of Terminal Services and the Citrix software. Implementation of a more organized structure and process was established, including creating a module template for authors to copy and use for new modules, Glossary Module for project terminology, and a Document Listing Module for

locating modules within the DOORS hierarchy. Enhancements were also made using DXL scripting language to augment the decision to use WEXP instead of Doc Express Factory and Word for document output.

4.1 DOORS and Microsoft Software Licensing

One of the first lessons we encountered was learning the difference between a single site license and a multi-site license of DOORS. A single site license entitled us to have concurrent users from within a 40-mile proximity of the database location. The multi-site license entitles us to have concurrent users from within the continental United States and Canada. The one area that we have not covered is the global users in Europe. DOORS does have a separate licensing scheme for global licensing.

After understanding the DOORS licensing the next step was to understand Microsoft licensing. Microsoft had a different way of licensing Terminal Services than in previous versions of the operating system. This new licensing approach required addressing the issue of all new Terminal Services Client Access Licenses (CALs) for all the users. Although the users may have Microsoft Terminal Services capability with the Windows 2000 workstation and Windows XP those licenses were not supported by the Windows 2003 Terminal server license agreement. The decision was also made to choose User CALs instead of Device CALs because users can be remote and can have more than one workstation to access from and selecting Device CALs would limit the user to a particular workstation.

The other change from previous Microsoft licensing is that we received an email from the vendor who sold us the Microsoft Products with information on how to activate and retrieve the activation and product code information from the eOpen.microsoft.com website.

4.2 Server Preparation and Citrix software installation

We paid a third party vendor to come in and setup the initial Citrix environment and several of the System Administrators attended Citrix Administration training classes in preparation. Prior to the vendor arriving the servers were setup with the Windows 2003 server operating system, specifying a 16 GB Operating System partition, and a separate area for applications as a minimum. Although Citrix recommended implementing RAID 5 technology we decided not to implement it, mainly for performance reasons. The servers were joined to the existing domain that currently uses Active Directory.

On the server that was to be the Citrix Presentation Server the drives were renamed from C, D and E, to other drive letters so that the users would not be confused with the local hard drives when accessing while in a Citrix session. There is a utility that is provided with Citrix called driveremap.exe that can assist with the renaming. There is also a Citrix article (CTX 950520)[1] with information. At this time we also requested the appropriate ports be open between the Citrix Presentation Server where the DOORS Client resides and the DOORS database server. We also reviewed the list of DOORS Accounts and requested that those users who needed a domain account apply for one. Once the users had a domain account they could be added to the Remote Desktop Group on the local Citrix Presentation Server. It was also necessary to get details on the

users firewall or proxy server as well because in addition to adding them to appropriate access control list the proxy server information had to be added in the Citrix Web interface Administration.

4.2.1 Citrix Presentation Server Setup

User authentication and certification required not only providing user accounts but also obtaining certificates of authenticity for the servers. We decided on using Certificates from a Certificate Authority so we applied for two certificates one for the Secure Ticketing Agent and the other for the Secure Gateway. The next step was to setup the Citrix Presentation software and the Terminal Services and Terminal Service CALS. Terminal Services must be setup in Application mode for Citrix to work. Currently the way the CALS work is that if you do not have CALS and users connect they get temporary access. We also had issues with being part of a bigger Active Directory that was a mixed mode environment with Windows 2000 servers and 2003 servers and the existence of a Terminal Service Server under Windows 2000 operating system. We ran a utility called LSView that determined the Terminal Server License Server being used. We had to use the MS article (279561)[2] for locking down the 2003 Terminal Server so that the correct server would identify the Citrix users.

Although we had the Citrix CDs for the software installation we had to go to the MyCitrix website to get the licenses needed for the installation. We received access to this site when we purchased the Citrix software. There were several licenses, one for the Feature Release of XPe and one for the Connectivity pack that had to be downloaded. Internet Information Server (IIS) was installed for the Secure Ticketing Authority (STA), and then one of the Certificates was installed, prior to the Citrix Presentation server software. The STA is the mechanism used to pass tokens of authentication between the Citrix components. The STA is not a resource intense program and is a very simple program to install.

After the Certificate is installed a decision needs to be made on what database the Citrix server is going to use. Citrix has the ability to use the Microsoft Access database that comes with Citrix or also SQL Server. We chose to use the Microsoft Access database.

4.2.2 Secure Gateway Setup

The Secure Gateway and Web Interface server required installing IIS, the second of the Certificates, the Secure Gateway Software and then the Web Interface software. Because we chose a configuration that combined some of the Citrix components we had problems with sharing port 80 between more than one service so as a result we had to change the port assignment for the Citrix XML service. After testing the Web Interface software the Secure Gateway software was installed. If you have access to Telnet you can test your installation connectivity by teleneting to the fully qualified name and specifying the port number, you should get a flashing cursor.

During the initial setup we experienced some problems with Citrix Secure Gateway and did a test installation on the Citrix Metaframe Presentation Server and it worked without any

problems. This was not recommended but in the event there is a problem with the Secure Gateway this can be done.

4.2.3 Installing the DOORS Client

The DOORS and Synergy licenses were applied for and received from Telelogic. DOORS was installed on the new server and the old data directory (c:\Telelogic\DOORS60\data) was copied to the new server overwriting the existing data directory. It was also necessary to edit the license.dat file for DOORS and add a specific port at the end of the daemon line for security reasons ("port=xxxx" where xxx is a non blocked port).

After all the Citrix sofware was installed the next steps were to setup the desktop view that would be displayed for the users via the web interface, by installing the DOORS Client on the Citrix Presentation Server and allowing the remote desktop users access to the DOORS client software. The DOORS client was installed in seamless mode. Seamless mode launches the application within a desktop and looks like you are running the application locally. In order to export from DOORS, Word and EXCEL had to be installed on the server as well. Basically you need to use the Add Remove Program option in the Control Panel to install any software through Citrix. After the client was installed we installed Microsoft Word 2000 and EXCEL as well because DOORS cannot redirect to the local hard drive copy of the software. Windows 2003 Microsoft Terminal Service requires the use of the transform file for installing any of the Microsoft 2000 products. A transform file fixes compatibility problems and is provided by Microsoft or the third party vendors if they support Citrix. The transform file (i.e. termsvr.mst) is located in the Office Resource Kit and the MS article (283675)[3] provides additional information on how to perform the installation.

4.2.4 Preparation for Installing the SYNERGY /DOORS Integration

The SYNERGY/DOORS Integration component could not be installed within the DOORS Client until SYNERGY/CM and SYNERGY/Change were installed on the server. The order of installation was installing SYNERGY/CM, which is the database component, SYNERGY/Change that is essentially the middleware component that utilizes Jetty Open source Web server behind the scenes with DOORS and then the SYNERGY/DOORS Integration component. These components required several Windows Domain accounts to be established and placed in the right groups with the right permissions. Once the accounts were correct we chose to manually create the databases using information from the SYNERGY/CM Users Guide and notes from the previous installation of SYNERGY/DOORS Integration known as ECPS. SYNERGY/Change was installed after we verified the installation of SYNERGY/CM. SYNERGY/Change required some patches be installed for the latest version of SYNERGY/DOORS Integration to work correctly with Windows 2003 Server. The SYNERGY/DOORS Integration was installed and with the help of a Telelogic System Engineer the appropriate process packages were installed so that a template could be established within DOORS to apply to the modules. An issue we ran into was the exporting of users from DOORS to SYNERGY/Change; the passwords of the users are not exported. The default passwords in SYNERGY/Change are the DOORS ID number of the user. The ID number is based on the order the user was created originally within DOORS.

4.2.5　Citrix Client Support

The nice thing about the Citrix web clients is that you can set up the PC clients so that they are automatically downloaded to the PC when updates are available. The Citrix Article (CTX104546)[4] explains how to make the appropriate changes to the Citrix Web Interface. Although Telelogic does not support the use of Macintosh computers we have been able to get them to work. Several changes have been made with the Mac configuration. Initially the Macs did not support the certificate we were using so the root certificate information had to be imported into the MACs key store. See Citrix Article (CTX101697)[5] for further information. Also the .asp extension on the Mac is associated with Apple System Profiler so we referred to Citrix Article (CTX102463)[6] to force the launch.ica client to understand that Citrix should be launched.

There was one other issue to overcome with MAC clients and that was the difference between the default Safari browser on OSX and Internet Explorer and the way the client browsers installed Citrix. Accessing the Secure Gateway URL and selecting the OSX client to install, downloads the .dmg (disk image file) to the desktop. Users have to double click on the .dmg file to open the window and drag the Citrix ICA Client folder to the Applications folder on the MAC. The installations differ from this point forward, on Safari when you access the URL and login to the Secure Gateway a launch.ica file is installed on the desktop each session and you have to click on the launch.ica client after clicking on the DOORS icon. The launch.ica file will expire and need to be downloaded again if not accessed within a minute or so.

Internet Explorer does not download the launch.ica file each time but does require additional steps during installation the first time. A File Helper has to be setup in order for the MAC OS to recognize how to handle the ica file type. Setting up a File Helper is done by:

1) Open Internet Explorer Preferences and selecting Add
2) Specifying a description for Citrix
3) Extension: of ica
4) MIME type: application/x-ica
5) Selecting View with Application and browsing and selecting the Citrix ICA Client.
6) Selecting OK to the next prompts

5　Lessons Learned during Implementation and Deployment

Once the environment was setup getting the users to work within DOORS and feel comfortable was the key. Because we had problems with importing and exporting we focused on coming up with a solution for both. The solution for importing was to be specific with the users on what needs to be in their document or spreadsheet prior to importing. We also stressed that once the document was imported into DOORS they needed to make all future changes within DOORS and not try to export and re-import the information. It was more a process improvement rather than a software solution. Exporting from Doors required a software solution. Doc Express Word and Factory had known issues with fonts and performance and required a separate application, so we decided to go with the WEXP tool for output. WEXP was a Word Exporter

tool we obtained from Telelogic Professional Services. Using the WEXP tool would make it easier for the users because once installed it is a menu option within DOORS. Telelogic did the initial customization of the WEXP tool and the Word template and showed us how the tool worked and we then further customized the template and the WEXP init file to output the entire requirement document including appendices. The user only needs to specify 3 pieces of information and that is the view to export from, the location of the word template and where to place the output.

The issue that we had with Word and the output is that because DOORS cannot locate the user's workstation copy of Word you have to browse and change the output to the local client drive or it tries to write the newly created output to the server. We recently implemented a separate Active Directory Organizational Unit and put the Citrix Presentation Server in this Unit, so that the Group Security policies for Microsoft Word and Excel to redirect the File Save As location to the local client C drive could be applied to just this server and the users who access. It is still up to the user to specify where on the client drive to save the document. These Group Security Policies are not part of any existing template in Active Directory by default. These policies should be part of the Microsoft Office Resource Kit or can also be located on the website thin.net.

We also had to educate the users to understand that currently the authentication method required logging into a Windows Domain and then logging into DOORS and that this required two separate accounts. We also had to education the users to allow the Citrix application to access the local hard drives when the Citrix Security message appears, other wise they got an error when trying to save the document. There was another option being looked at which was the ability to implement a roaming profile, but the Domain Administrators did not want to implement this for security reasons.

5.1 Setting up a Place to Share Scripts and Templates

Some modules/documents are authored and under Configuration Management at other sites, the output format can be different than the WEXP output format used by GSFC JWST modules and documents. The WEXP tool for exporting has been integrated into DOORS on the central server but other remote sites also use different Microsoft Visual Basic (VB) scripts for out put as well. We created a share that the users could access from the application menu as a central location to put the templates and scripts created at the different locations. There were two ways we could have done this and one was to create a mapped drive on the Citrix Presentation server, the other was to modify the usrlogon.cmd file that is part of the terminal service login process and add the manual connection to the network share so that an application icon could appear in the users Citrix desktop menu.

5.2 Miscellaneous Importing Issues

We ran into some other issues with the different DOORS sites having different Views and Attributes and we had a meeting with all the key users at the different sites. We negotiated a common set of Views, Attributes and a linking schema that would be used for all modules. There is also a standard Requirements Template module with all the agreed upon Attributes and Views that can be used to create any new modules. We also established a method for handling

the Acronym and Abbreviations section of the requirements document so that each module would not have a separate glossary with 90% of the same terms as the other modules. The glossary terms were extracted into a separate Glossary Module with an attribute within the module that can be used to specify whether that specific document module requires the use of that acronym.

Figure 2. Glossary Module

There is also a Document Listing modules that can be used to locate and check on the status on whether a module has been imported into DOORS, or the current version of the DOORS module as well as who is the author and what prefix is being used for the requirement numbering.

File Edit View Insert Link Analysis Table Tools User JWST WEXP ChangeSynergy Help

Main View   All levels

Module Locator and Status	Document Number	Identifie	Rev	Responsib	In DOOR	Ready for DOO	Estimate	Level	CM By:	Audited By C
1 JWST Folder										
JWST Program Plan	JWST-PLAN-000633	L1	Basic	Lynch	Yes	Yes		1	Goddard	
JWST Project Mission Requirements Document	JWST-RQMT-000634	MR	J	Person	Yes	Yes		2	Goddard	No
JWST Mission Operations Concept Document	JWST-OPS-002018	MO	A	Person	Yes	Yes		2	Goddard	No
JWST Project Science Requirements Document	JWST-RQMT-002558	SR	Draft	Person	Yes	Yes		2	Goddard	No
Document Listings				Person	No	Yes				

Username: mbussman   Exclusive edit mode

Figure 3. Document Listings Module

Other issues that caused us problems when exporting is the need to verify what versions of Word is supported with what versions of operating system with what versions of DOORS. Currently we have some graphics issues and also have had some symbols issues. Basically we tell users up front to utilize the Latin-1 symbols in Word when creating symbols. We also tell the users to try not to scale any drawings and diagrams and use the Insert Picture option when inserting pictures into DOORS that do not look correct or display correctly after initial import. These are not Citrix related problems, these problems have come up as a result of upgrading or choosing not to upgrade versions of Microsoft software to allow for the least common software factor at the remote sites.

5.3   Configuration Management and DXL Enhancements

DXL scripts were utilized to help the authors. The following is information on the DXL scripts and what the functions are for each one.

We also moved away from using the automatic numbering schema of DOORS because the preference was to number the requirements manually for a more manageable numbering schema. The Prefix Checker script was used to check for duplicate prefixes. The numbering was done manually so that a requirement was not limited to one paragraph but instead if you wanted to combine text under one heading you could do that and there was also a script created for these special cases.

5.4   Disaster Recovery and Contingency Planning

In order to ensure and minimize downtime two additional servers were purchased as redundant servers for the DOORS and Citrix servers. These servers will be located in a separate building from the current environment. They will be accessible via the network. An additional DOORS license was purchased for the separate installation. This server will be used as a backup to the real server with a weekly copy of the data being transferred over. This server can also be used as a test server. The additional Citrix server will be added to the farm in the event the main server

goes down the users will still be able to get a DOORS Client and access the database. Switching the users to the backup server is a matter of creating a separate published application and adding a –d 36677@servername to the end of the executable line when creating the published application in Citrix.

6   What's Next

Remaining issues are the need for multiple logins between Citrix and DOORS and SYNERGY/Change and we are hoping to make use of the Active Directory login support when Telelogic includes that support. We are also hoping to utilize the SYNERGY/Change Integration piece in DOORS to produce the Configuration Change Request information and further simplify the requirements reviewing process. We will also be addressing the possibilities of using DOORS XT with the Oracle back end support at some point in the future. We need to come up with an acceptable solution for the International Partners to access whether it be implementing DOORSnet or paying for a Global License. We have to work out a way that the global license could be done separate from our existing license pool.

Evaluation of when and if to transition to version 8 of DOORS and all the components is under discussion and this will require input from the partners and contractors before proceeding or implementing any changes.

Currently we are also looking at software and hardware redundancy in the event of a failure of one of the servers. These redundant servers would be located at another site. Sufficient server backups are done so that the DOORS database could be restored to another server.

7   Benefits and Results

Using DOORS through the Citrix environment so far has been successful and performance does not seem to be an issue. Deployment is much easier and very quick to do. Establishing, setting up and deploying DOORS through the Citrix environment involved a lot of initial up front work but once setup it is fairly straightforward to maintain. The benefits from this environment include:

- Cost Savings in resources required maintaining and deploying the DOORS software. A dedicated person is not needed to deploy and maintain the client software on each workstation because the software is installed and updated only once.
- Performance increases because the Doors Client talks directly to the Doors Database server and there is no need for VPN software. The use of a web interface with Citrix sends snapshots of the information. There was a latency delay of a few seconds with VPN client that was cut in half with the Citrix environment.
- Flexibility to allow vendors with strict security and firewall practices access to the environment through standard secure ports
- Time and Cost Savings in Administration, not having to have a full DOORS Administrator for the Project at each location. 2 to 4 hours a week was spent working with partitioning of modules and troubleshooting problems that occurred between remote

DOORS databases. Only one DOORS Administrator for JWST needed at the central location saving the cost of additional administration support at other sites.

- More efficient and consistent Configuration Management – everyone has the ability or access to the same templates, attributes and views. Consistency in producing information in the same way allows for better quality output and reporting. Also once people are familiar with what is expected there is a timesavings in producing future modules.
- Ability to support Macintosh OSX users
- Quicker turnaround on Requirements Review and Auditing. Everyone is on the same page when doing the reviews and they have access to the same information.

References

1. Citrix Article: CTX 950520, support.citrix.com , July 2003.
2. Microsoft Article: Q279561, www.microsoft.com, April 2004.
3. Microsoft Article: 283675, www.microsoft.com, November 2004
4. Citrix Article: CTX 104546, support.citrix.com, November 2004.
5. Citrix Article: CTX 101697, support.citrix.com, April 2003.
6. Citrix Article: CTX 102463, support.citrix.com, June 2004.