



ICS and You

This document has been created as follow-up information to Fred Woodbridge's presentation on May 29, 2009, on the Idaho Consolidated Services' Consolidate Messaging Project (CMP).

With hindsight, the choice of nomenclature was possibly unfortunate in that it may have led some who heard it to believe this project only concerned Messaging, i.e. email. It is true that the project primarily started with the goal of consolidating messaging. With time and consultations with Microsoft, Dell and other key state business partners, the goal of the project naturally grew to include other things; the most important of which is the Directory.

Consider that Microsoft has done something interesting with Messaging. It has made it part and parcel of the larger Active Directory infrastructure unlike other systems (such as UNIX), which has a clearly delineated line between email clients and any sort of authentication systems or certainly Directory services. Additionally, future statewide consolidation efforts are made possible with a common Directory infrastructure, so it made sense for this project to also include Active Directory.

With that in mind, several ideas were floated as to the design we should implement. In fact, there were three:

1. One domain, one forest.
2. An Exchange resource forest with each agency continuing to maintain its own forest.
3. One domain with child domains belonging to the different agencies.

There are pros and cons to each of these designs as you can imagine. They will be covered here following in reverse order.

One domain with child domains

The child domain design was, on the surface, quite attractive because each sub- or child-domain is controlled by its own domain administrators. In addition, since each child domain can create mailbox-enabled accounts in the one Exchange organization that can only exist, we have achieved the goal of making this a true "Consolidated Messaging Project."

The downfall with this idea is that a migration will need to happen, but that's all right. But, and it's a huge but, due to the inherent security concerns of Active Directory in such a design, any one Domain Admin in a child domain definitely has the capability of affecting the operations--and by "affecting" meaning negatively for the most part--of other child domains.

The security gates between child domains in a multi-domain environment are made of cream cheese, to quote Joe Richards, Microsoft MVP and co-author of the O'Reilly book *Active Directory, 4th Edition*. It is truly shocking how almost trivial it is for an administrator in one child domain to gain elevated privileges in this scenario.

Why is this?

Simple; each domain controller in a forest has a read-write copy of the configuration partition of the entire forest and each child domain has transitive trusts in place. Everyone trusts everyone else. Think about what this means for the Exchange forest. Think about what this means for gaining the ability to modify information within Active Directory that then gets replicated throughout the forest.

All DCs replicate the same configuration and schema partitions between themselves. This means that a malicious admin from one child domain can potentially leverage his own DCs to impact DCs in any other child domain of the forest. As an administrator of his own DCs, the domain admin can easily elevate his privileges by making code run with the credentials of his domain controller. While only members of the Enterprise Admins group have explicit permissions to change the configuration partition, the DCs themselves also have this privilege.

Outlined below is an example process of just such an elevation of privilege made possible without too much work. This is included because some have asked specifically how this is even possible. In addition to that, since this information is readily available to even the least discerning AD administrator, it should serve as a warning for those who manage Active Directory.

Step 1: The domain admin of the Child1 domain logs on to a DC of Child1. As an administrator of the DC, he can execute code with the credentials of the DC, for example, by launching any executable with the AT command:

```
at 15:00 /interactive "mmc.exe"
```

This AT command will trigger the execution of an empty MMC console at 3pm; it will be launched by the task scheduler service that runs on the DC in the security context of the Local System account. Child processes started by the task scheduler service will inherit this security context. The `/interactive` switch will make the MMC console visible and active in the user session of the Child1 domain admin, who can then add any MMC snap-in to the console. Simply adding the AD Sites and Services MMC snap-in allows the editing of crucial data, such as AD replication

settings stored in the configuration partition. However, this includes potentially malicious changes, such as editing the permissions on data stored in the configuration partition in order to make the data inaccessible to other DCs in the forest.

Step 2: Changes performed by Child1's domain admin to the configuration partition on a DC in the Child1 domain are replicated to all other DCs in the forest via the normal AD replication mechanisms.

Step 3: All DCs in the forest update their configuration partition with the changes they received through replication from a Child1 DC. Depending on the changes performed by the Child1 domain admin, there could be a negative impact on the functionality of the whole AD forest and any application (hint: Exchange!) relying on it.

It is no wonder the technical sub-committee nixed this idea quickly, as you may imagine.

The Exchange Resource Forest

This is another functional idea and one we also had to reject in light of the fact of those two immovable constraints on any design project, time and money. In addition, there's also the fact of complexity of implementation and ease-of-use.

Implementing an Exchange Resource Forest is time-consuming due to the complexity of the design. The Domain Administrator who will be creating an account in their separate forest will require a mailbox and all the proper Exchange-specific attributes to be stamped on that account. This process requires a method by which the newly-created account also gets created in the Exchange Resource Forest and as of the time we were tackling the design issues, the best way to achieve this goal was by buying and implementing MIIS (now known as ILM, Identity Lifecycle Management).

What our design objective included was a cost-aware design which the Resource Forest scenario was quickly showing we wouldn't achieve easily and we decided to test out the next design solution instead. Additionally the technical sub-committee visited other states that had migrated to a consolidated effort in a Resource Forest environment and each state recommended staying away from this model due to the complexity and the Trust related issues they encountered. All had since transitioned or were in the process of transitioning to a one forest, one domain architecture.

One forest, one domain

Microsoft's best practices have always suggested the goal of domain consolidation for several reasons, many of which they have outlined in the various White Papers available for download from their site.

Consideration for this design followed those best practices and gave us as we saw it then, a relatively economical and technologically secure way of achieving the goal of consolidation. In

this scenario, there would be one Enterprise Administration Team in charge of the centralized Active Directory (and Exchange) with the agencies as Organizational Units (OUs) in that AD structure.

Agency IT personnel would continue to have the kind of control over their internal users and computers as they had in the past, but shared services state-wide would now be easily achievable. Security comes built-in as OU administrators are not able to easily elevate their privileges and disrupt operations as they could in the other design scenarios.

After some thought and discussions with Microsoft and others, this was the design recommended by the ICS Technical Sub-committee and approved by the ICS Oversight Committee. Bear in mind that with all but one of the above designs, a domain migration would need to happen (the Exchange Resource Forest is the only one not involving a migration) and so the search was on to find a suitable tool for the job.

Microsoft's ADMT (Active Directory Migration Tool) was not up to the task in the time we had available so the next alternative was the one we ultimately chose, the Quest Migration Manager.

Quest Migration Manager (QMM)

This tool is considered best-in-class by many who have used it and is recommended for large-scale migrations of the sort in which we are currently involved. Microsoft also recommended the Quest Migration Manager tool. More thorough information about it can be found on Quest's website at <http://www.quest.com/migration-manager-for-active-directory/>.

In addition to providing a good way of migrating AD objects, this software suite also included a way to migrate Exchange data as well with its Migration Manager for Exchange (<http://www.quest.com/migration-manager-for-exchange/>). Boasting a feature they have named ZeroIMPACT, Quest's tools promise that the one aspect of these migrations which should be inconvenienced as little as possible, the user, must be spared any disruption.

In running the QMM these past few months, it is hard to agree completely with their assertion. Users do get inconvenienced, but admittedly this process has not been quite as bad as originally envisioned.

The main view of the QMM is shown in Fig. 1.

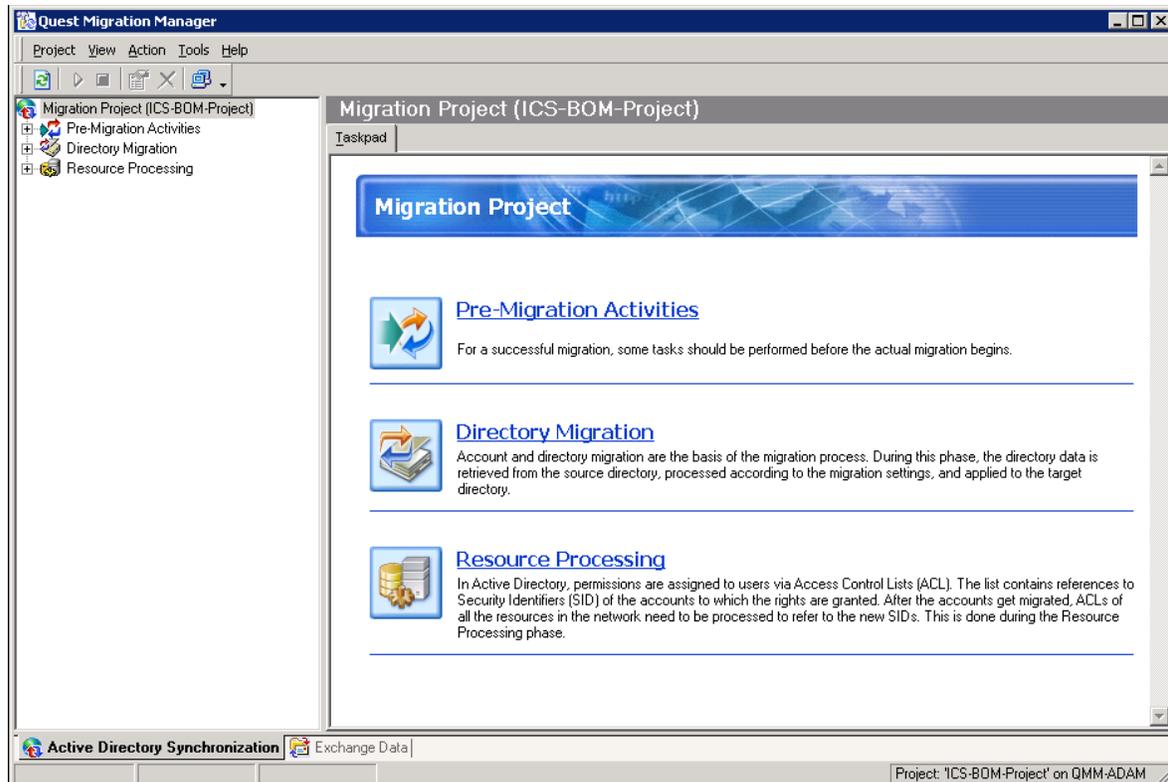


Figure 1

Anything more thorough than a high-level overview is impossible due to space and time constraints. However, the controlling idea is transactional, just as in the banking sector.

Just as a banking transaction actually consists of several different sub-transactions, so does the Migration Manager go about its business. With a very simplified example from banking, when you pay \$50 to a vendor, you cause a series of small operations to start. First, \$50 is deducted from your account. Second, \$50 is inserted into the vendor's account.

That's all well and good, but imagine a scenario in which something untoward occurs during the transaction and the \$50 is in limbo. You have \$50 already deducted from your account, but not yet inserted into the vendor's account. No one is going to be happy, least of all the vendor, so what happens is there are a series of checks and balances inserted into the process that ensures \$50 doesn't disappear because of transactional problems.

So it is with the QMM.

First, an Active Directory trust is set up. This is simple and easy enough to type and read, but the trust setup belies a great many complex operations that have to occur; such as, but not limited to, setting up the proper network routing, opening the proper ports in any firewalls and so on.

You will be spared the details in this document, but not in any others related to your agency migration.

So essentially, a copy process occurs followed quickly by a synchronization process. A copy of the Active Directory accounts is made from the Source domain into the Target domain and a one-to-one relationship is established. TargetAccountA has a solid relationship with SourceAccountA.

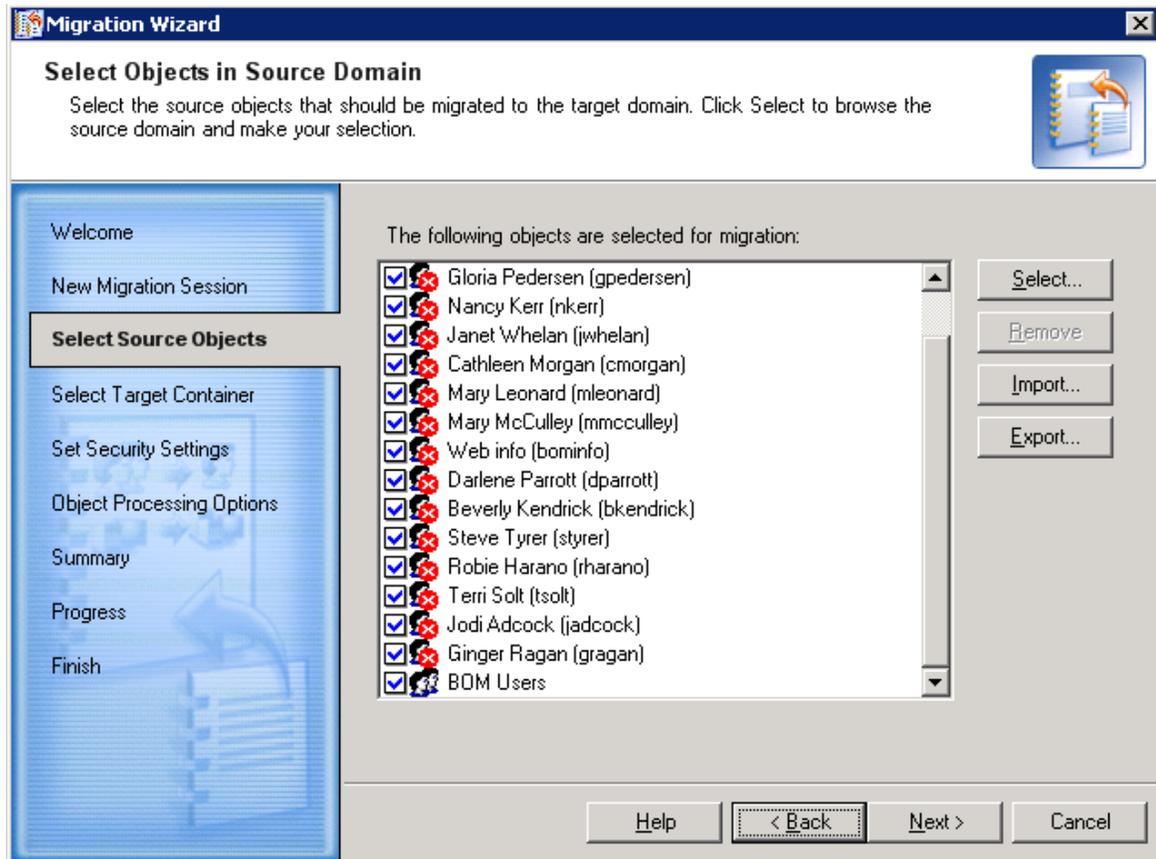


Figure 2

In Fig. 2, we see a copy process from the QMM software in which we have chosen accounts to migrate or better yet, copy.

Once the copy process is complete, a synchronization job is set up such as shown in Fig. 3

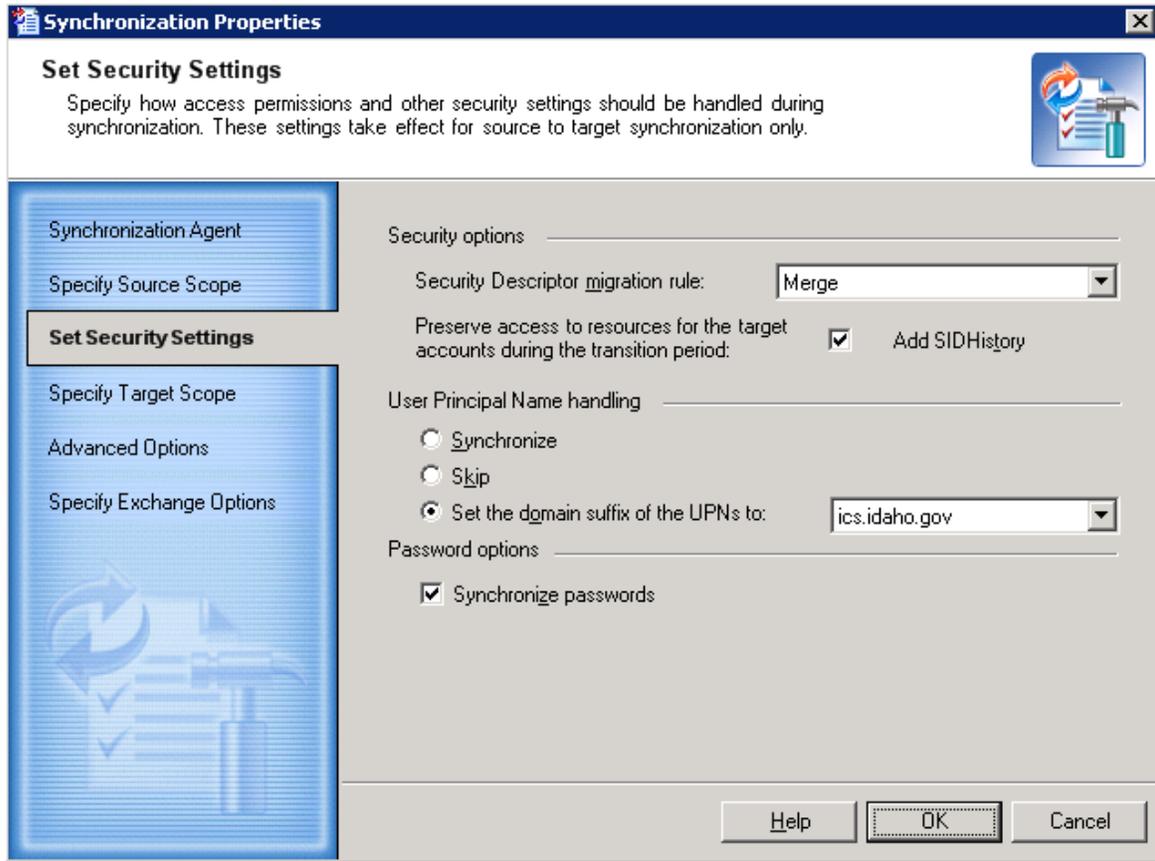


Figure 3

As you can see, this includes such things as synchronizing passwords. This means that whatever changes to the account occur in the source domain, those changes will be synchronized to the target. If a password is changed in the account's source domain, that password will be set in the account's target domain account as well.

The relationship between the source and target domain accounts is kept in an ADAM (AD Application Mode) or ADLDS (AD Lightweight Directory Services) database.

With account synchronization in place, the next step is to set up the workstations using the Resource Updating Manager (RUM) plug-in for QMM, see in Fig. 4.

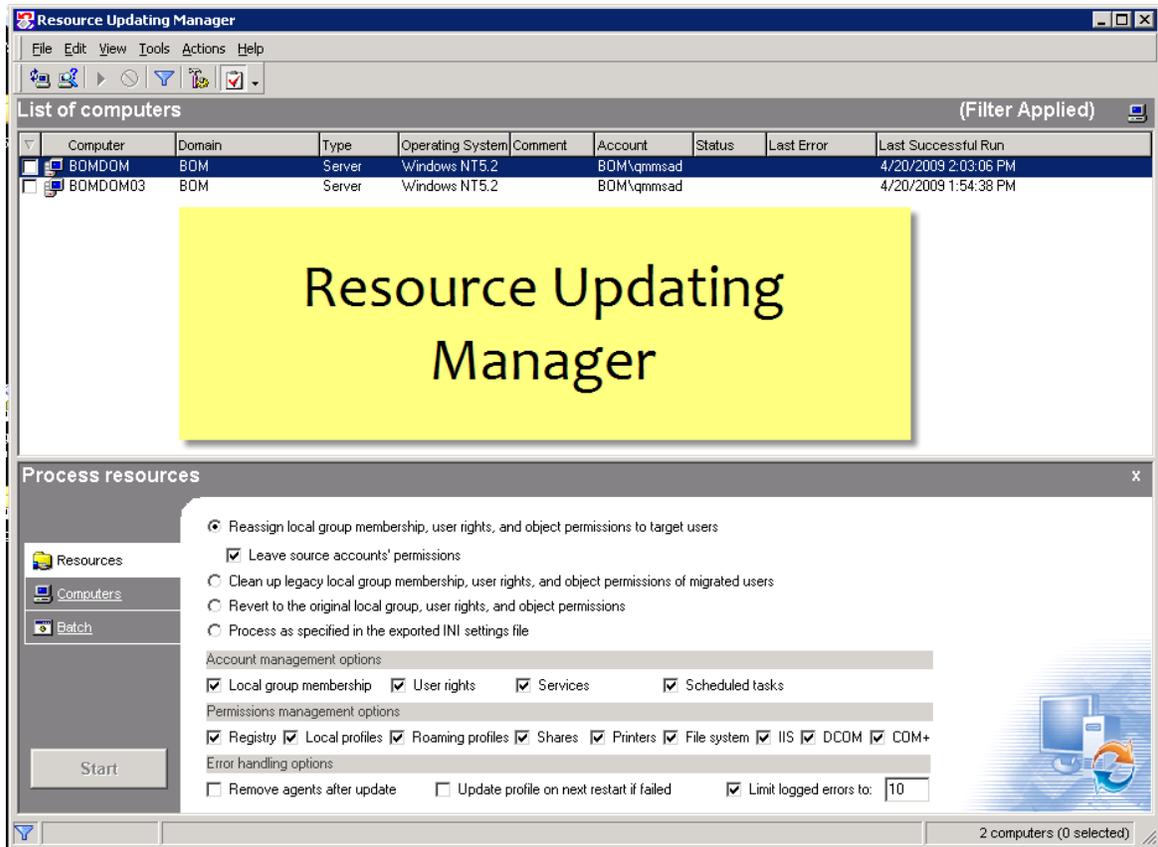


Figure 4

The RUM is an agent-driven application that connects to source domain computer objects and "updates" the files and folders on the computer so that each file and each folder now contain access permissions for each of what we have termed as the Doppelgänger accounts. Once done, each file or folder will contain permissions settings for two accounts such as seen in Figure 5.

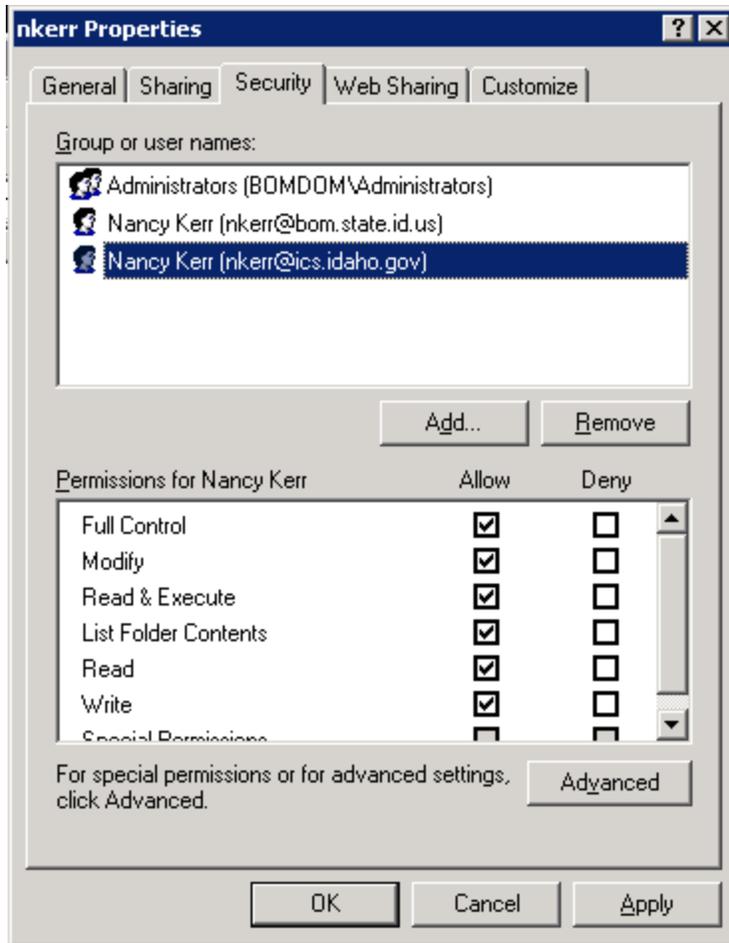


Figure 5

The RUM also has other applications as well. It is possible to process SQL servers for example, as shown in Figure 6.

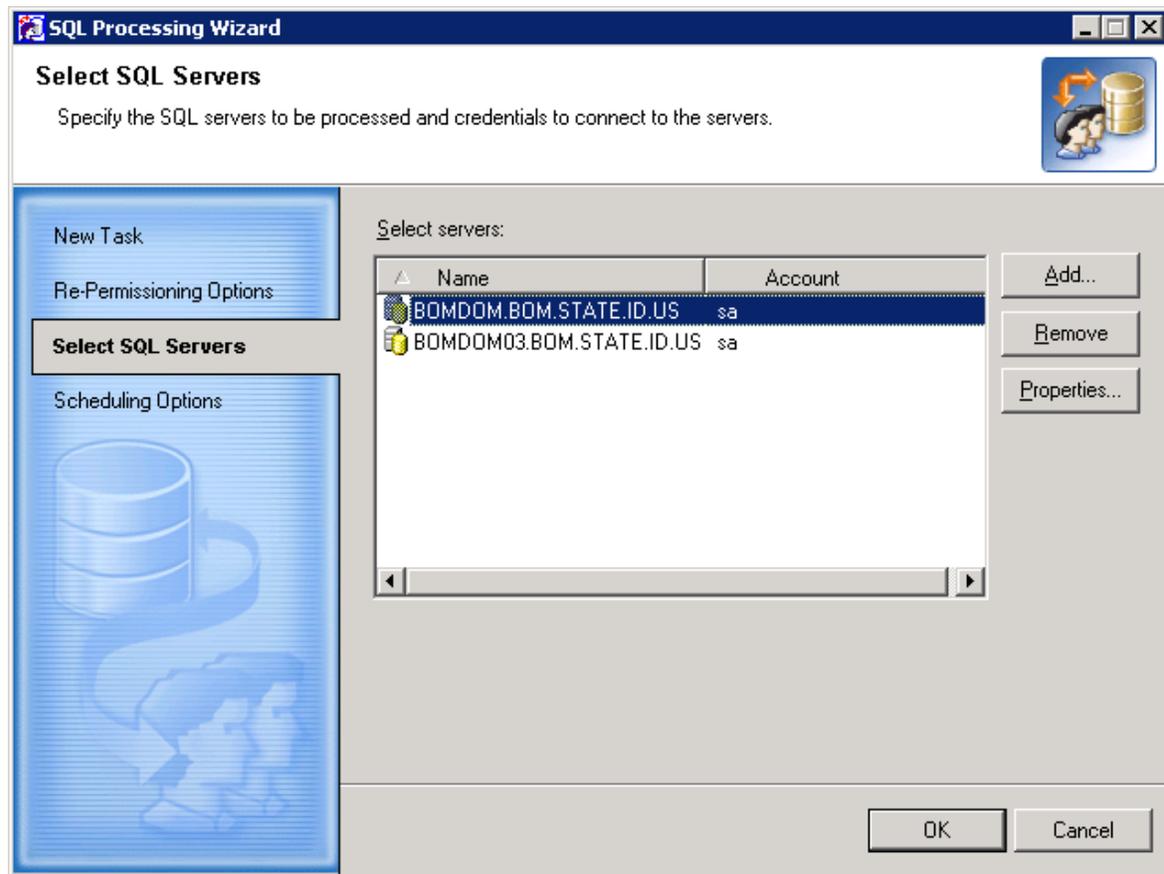


Figure 6

In SQL processing, domain accounts which have been given permissions to perform certain tasks or given access to certain data through the built-in SQL permissions architecture are given the same rights and permissions to those accounts' target accounts as well.

One important point to note is that the RUM can process all these workstations and servers in the background. Users continue to work as normal while all this happens.

Exchange Processing

Because Exchange processing is a somewhat different part of the process and because it actually comes with a different QMM for Exchange tool, it deserves its own subsection.

To pick up from where we left off, the accounts have been given twins so each account has a related account in each domain. The workstations and servers which contain their files and folders have been stamped with each account's permissions and SQL server process has occurred. Now we will tackle their email, the contents of their Exchange mailbox, as we have been working only with the AD accounts until now.

Figure 7 shows what the Exchange portion of the process looks like.

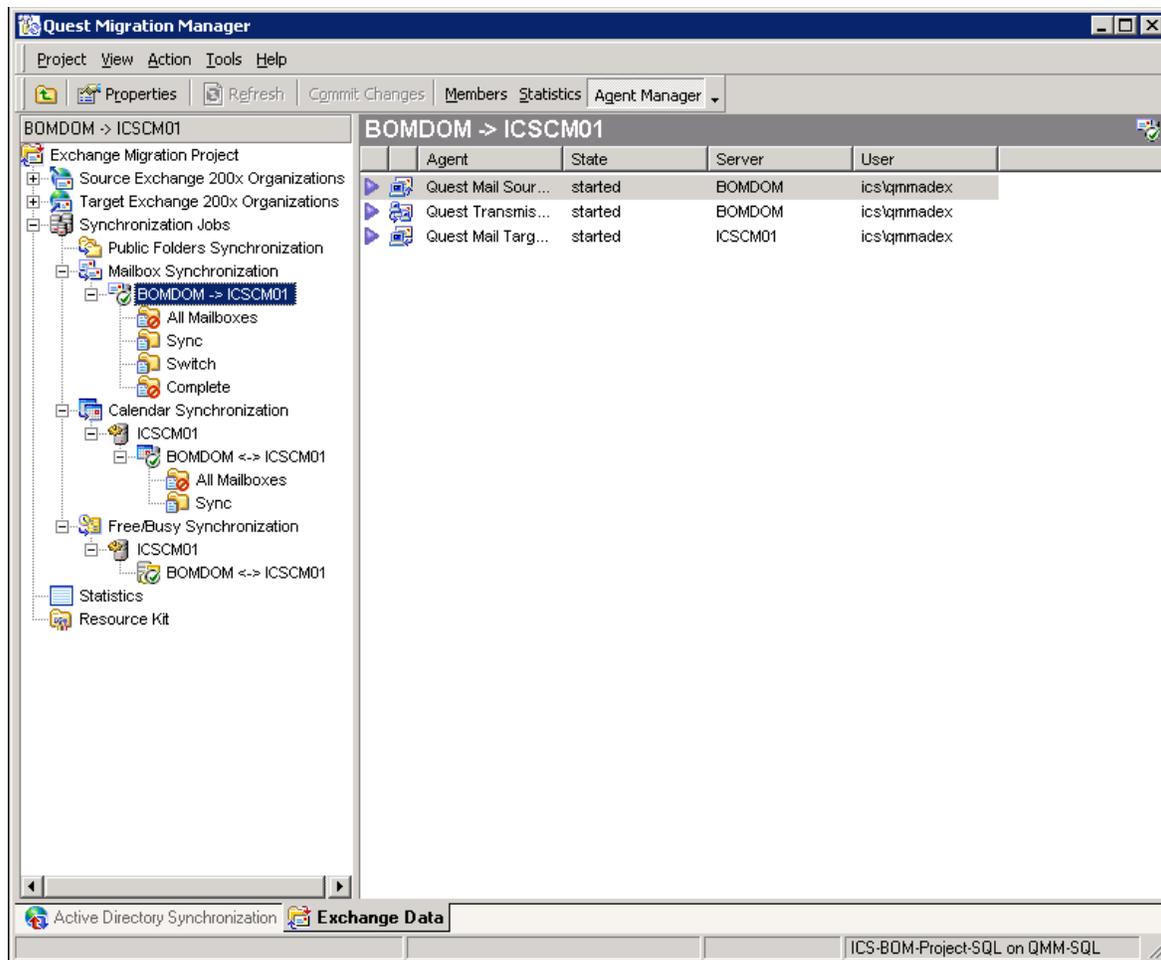


Figure 7

As you can see, there exist several parts to this metaphorical pie. Like with AD, we first create Exchange linked mailboxes for the Doppelgänger account in the Target. Then we start a synchronization so that email contained in the SourceAccount is synchronized into the TargetAccount.

At a certain time, defined by the amount of mail in the SourceAccount's mailbox reaching a small amount, an actual switch operation occurs and all mail now resides in the TargetAccount. When this point is reached, a flurry of activity ensues. We call this part of the operation the somewhat unimaginative name of "Switch."

Switch

It is at this point that we have all the mail from the Source domain in the Target domain. Mail flow is now switched via DNS MX records or, as is more common in the State, the IronMail servers are reconfigured to direct mail traffic to the Target domain's Exchange servers.

As this is happening, the workstations are switched to the Target domain and placed in the proper Organizational Unit (OU), a procedure that requires a restart. The AD accounts in the Source domain are disabled at the same time as they are enabled in the Target domain.

Upon workstation restart in the new domain, users will be able to logon with their normal usernames and passwords (which, remember, have been kept in synchronization so it all remains the same). A special Group Policy Object is applied to these new users so that they get the last piece of the QMM puzzle, the Outlook Profile Migrator or EMWProf.

EMWProf is a small utility that will need to run once. Its job is simply to convert all the local Outlook profiles from the Source domain's Exchange servers to the Target domain's Exchange servers. It performs this operation again using a transactional model.

When the Exchange migration switch happens, a notification post is inserted into the old Source domain account's mailbox to the effect that the account has been switched. EMWProf connects to the Source domain's Exchange server and looks for this important bit of data. If it finds it, EMWProf switches the Outlook profile to the Target Exchange server. If not, it logs its findings and then stops.

This way, it ensures the new "home" for the account is actually ready and 99% of the time it is, and so the switch happens in the background. The user will, of course, have to wait until this process is complete.

So this completes the overview of the process in a small, a very small, nutshell.

Active Directory and Exchange Management in ICS

Microsoft has designed AD with the idea of delegating duties and the rights to perform those duties as well. Delegation of administration is the lynchpin of how the ICS forest will be managed. Fig. 8 shows an example of how each agency will exist as an OU in the ICS domain.

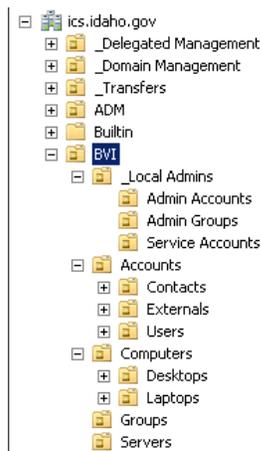


Figure 8

Full Control delegation is implemented at the OU level to what we are calling the OUAdmin group. This group will also be delegated the rights to create and manage mailboxes as Exchange delegation of rights is also a built-in feature of Exchange Server 2007.

You must bear in mind that simply delegating administrative rights over the OU does not come with the rights to manage computers. Therefore, into each agency's workstation's local Administrators group can be placed the OUAdmin Group via Group Policy (or better yet, Group Policy Preference Extensions) or, should they wish to sub-delegate those tasks, another group such as an OUDesktopAdmins group.

An OUServerAdmins group for the stated purpose of managing servers is possible as well. The important idea to understand, however, is that in setting up such a management structure, we are adhering to the security best practice of separating administrative accounts from everyday use accounts.

OUAdmins will have their normal accounts for everyday mail reading and so on, and one other special account which is special only in its membership of any of the management groups, OUAdmins, OUDesktopAdmins, OUUserAdmins, OUServerAdmins, etc.

The creation of and membership in these groups, along with the proper delegated rights, remain in the purview of the OUAdmins which will be created by default for each incoming agency.

Printers

This deserves a special section of its own. Agencies are urged to set up printers with the idea that any printers published to the directory will need to be named appropriately. In addition to naming it with enough description (and of course, the agency's three-character designation), it is important to set the proper permissions in place to disallow unauthorized access.

It is also possible to set up printers which are not published to the directory or served through a particular print server. It is also possible and suggested to contact the Enterprise Administration Team to investigate the possibility of using locations as the basis for what local agency users see first in their search for printers in the directory.

Service Accounts

This is a subset of the groups above. It is important to set up services that provide access to such applications as SQL databases with the proper rights and permissions. As you have OUServerAdmins, a special group or groups for Service Accounts is also possible and their use is highly suggested. These groups can then be inserted into the proper server administrative groups.

A special case is that of BackupExec which requires membership in the Domain Admins group. These service accounts will be managed by the Enterprise Administration Team because of that reason. With the advent of something known as a Managed Service Account in which accounts

of this sort are managed in the same way by AD as computer/workstation accounts, security should improve drastically.

Management Consoles

For managing AD in the ICS domain, it will be necessary to have a Windows Vista or Server 2008 environment. This is required because ICS is based on Windows Server 2008 and Exchange Server 2007 and only those management consoles which feature the RSAT toolset will be able to manage accounts in both AD and Exchange.

An Exchange 2007 environment with Windows Server 2008 split the management functions in such a way that Exchange mailbox management is no longer possible from within the normal Active Directory Users and Computers (ADUC) MMC. There exists an Exchange Management Console separate and distinct from the ADUC.

It is suggested that incoming agency administrators begin the process of working with PowerShell (PoSh) commandlets as each of the management consoles already related prior is heavily dependent on PoSh. In fact, it is possible to conduct all management from the Exchange Management Shell and all GUI commands actually are driven in the background by PoSh commandlets.

Incoming agencies will be given suitable MMCs that will show their respective root OU and Exchange storage group and mailbox database. In addition, we plan to create scripts that will simplify account and associated mailbox management.

Due to the fact of having one storage group (and one mailbox database per storage group), it is possible to maintain one's own Offline Address Books. Creating mailboxes in these storage groups (if an agency is large enough to warrant more than one), will be done either through the Management Shell using commandlets or through properly designed Exchange Management Consoles.

For those agencies not large enough to warrant their own mailbox database, administrative sharing will be implemented and responsibility will fall on each of the administrators of those mailbox databases to be careful in their administration.

While there will be backups and backups of backups taken, nothing beats careful administration so that you do not delete the mailbox of an account in a shared mailbox database over which you are not responsible, for example.

Domain Controllers

The placement of Domain Controllers (DCs) is a very important part of any Active Directory design because of the importance of DCs. Obviously, it is rather silly to install a fully Read-Write DC (as opposed to a Read-Only DC, an RODC) in a far-flung town where public access to such a DC is easy or not managed for security purposes.

However, it is important for usability reasons; local site DCs are used for logon authentication. We certainly do not want a situation where local users have to suffer long logon and Group Policy processing times because of the lack of a local DC.

AD in the Server 2008 era comes with the possibility of using a RODC which eases local logon times, but again, there are also considerations that go beyond the use of a RODC. Placement of Read-Write DCs will be judged per individual situation and will include such factors as number of users, bandwidth and latency of agency location, physical security and so on. Needless to say, Domain Controller management will continue to remain with the Enterprise Administration Team which, it is planned, will contain IT administration from the various agencies.

DNS

The importance of DNS in Active Directory simply cannot be understated. For performance reasons amongst many others, the design for the ICS domain will include placing secondary DNS servers at each location that is not getting a full RWDC or RODC. These secondary DNS servers will pull by good old-fashioned DNS zone transfer the ICS domain in addition to the `_msdcs` subdomain.

Doing this will speed up access issues and reduce the DNS resolution load on the ICS domain controllers. Nevertheless, dynamic DNS registration will still need to happen at the DCs. Again note that due to the mighty importance of DNS to Active Directory, DNS server administration will rest in the hands of the Enterprise Administration Team.

Secondary DNS servers will be installed as one of the steps of agency migration completion.

DHCP

Agencies will continue to run their own DHCP infrastructure as they see fit. In addition to secondary DNS server setup, authorization of DHCP servers will happen as part of the agency migration completion steps.

Because DHCP can insert records directly into AD, quotas will of necessity be instituted to reign in any runaway DHCP processes. Bear in mind that Linux-based or other DHCP services not running on a domain-joined Windows Server OS computer do not need to be authorized.

At switch time (cf. Switch above), it is necessary and imperative that DHCP services are set to point to the proper ICS domain DNS and Domain Controller IP addresses.

Group Policy Management

Initially, it was expected to have a rather large section covering Group Policy management, but as it turns out, thanks to the power of AD delegation of administration, each OU's administrators will be given the proper rights and permissions to create and link Group Policy Objects to their OUs only and that's pretty much where the story ends!

If you have any further questions or need clarification on this issue, Fred Woodbridge's contact information is at the end of this document.

Certification Authorities

The ICS forest will contain an offline root Certification Authority (CA) under which can be run any number of subordinate Certification Authorities. This root CA, which will be the proper and rightful CA for the State of Idaho, allowing the capability of securely signing and/or encrypting any and all communications (email, web) the state will have with both external and internal entities, requires industry-standard best practices for its installation, use and management.

As such, it is planned to have Hardware Security Modules in place and perhaps have our root CA signed by a world-wide CA such as Verisign, GeoTrust or Chosen Security. This is not a cheap proposition and will require both technical and budgetary planning.

Each subordinate Certification Authority will have the capability of issuing varied certificates to agency users, according to any security settings the OUAdmins deem necessary, while secure in the knowledge that any such certificates will be trusted state-wide. It is important also to ensure that the proper safeguards are in place to stop any unauthorized (i.e. non-agency) access for certificate issuance. All this requires a certain level of knowledge, planning and practice.

Future AD Management

However secure an AD design happens to be (or not to be), it can always be made more secure. Plans are in place to set up and utilize certain third-party tools for the adequate and complete management of Active Directory. Due to the complex nature of this endeavor, it becomes a good idea to invest in tools that will make managing a state-wide AD and Exchange infrastructure easier and perhaps better.

The ICS migration team has been testing a Quest tool, the Active Administrator suite, but is always on the lookout for any others. Suggestions are welcome.

Blackberry Management

Blackberry, by RIM, is an important force in the market today and many of our executive level staff use these devices exclusively.

In the opening stages of the ICS project, the Office of the Governor expressed interest in using a Blackberry Enterprise Server (BES). As such, during the design process, especially the storage design process, we used their provided figure of 50 users and accompanying licenses as one of the limiting factors in how we assign storage LUNs.

What was the point of doing this? Well, tests and documentation show that each Blackberry user extends the Input/Output Operations Per Second (IOPS) by almost 400%. In fact, the total IOPS for an Exchange storage installation can be calculated as follows:

("# of Exchange Mailbox Users" x "IOPS Profile / Mailbox") + ("# of Blackberry Users" x 3.64) = Total IOPs*

*<http://www.mmcug.org/blogs/Lists/Posts/Post.aspx?ID=31>

Research continues into what additional overhead ActiveSync users place on the Exchange store. In addition, BES Administration doesn't exactly follow the delegation of administration model that AD uses, which is yet another challenge.

Lessons Learned in Migrations So Far

This is the section that was called "Ouchies" during the presentation. This is the section which covers some of those things we have run into, buzz saw-like, during some of our many migrations so far.

Groups

The key here is to use them, use them, use them. There were too many times in which we found that the built-in groups were used to assign permissions. The problem with doing this is brutally simple; the migration process will not be migrating any built-in groups. Any permissions assigned to those will automatically invalidate any access users have as a result of membership in those groups.

Create user security groups now with the proper naming conventions. Describe them as adequately as possible, as should be your user accounts, incidentally. Please create full descriptions for your users, including titles, addresses and so on so that they show up properly in the Global Address Lists.

If you are not already familiar with the AGGUDLP format, a Google search will quickly reveal its meaning and, more importantly, its use.

SQL Servers

There have been situations in which access to SQL servers has broken after an otherwise successful migration. The SQL RUM will not and cannot look into Stored Procedures, for example, and if anything is manually coded in, one may have problems after that SQL server has been migrated.

It is vitally important that SQL DBAs contemplating a domain change be cognizant of what influence this will have on their SQL databases. Agencies with SQL DBAs in their employ should start querying them on this issue now.

User Accounts

User account properties have sometimes caused a number of problems. It is important to ensure that user accounts have the proper password complexity now, before the migration, as

you do not want your users to suddenly realize they cannot logon to ICS. Set up your group policies to match those of ICS now. Set up your user accounts to have the proper logon times and to have the proper logon computer restrictions, if you have any.

Ensure they are members of the proper groups and that they have access to the proper utilities and file repositories. Create and use the proper service accounts and put those accounts in the proper groups as well, both in AD and on the local server groups.

Encrypted File Systems

This is related to CAs for one, but not necessarily so. Bear in mind that EFS is inextricably tied to the user account and that once an account has been migrated, it is now, at least to EFS, a new account. Files on an encrypted volume will become unreadable.

Applications

These are the BIG KAHUNA of problems. It is imperative that agencies have their application developers *understand* and be able to answer the question of how a domain name change will affect their applications.

Do not settle for less as doing so will only cause problems in the future after your agency migration has already occurred. While it is possible to perform rollbacks, it is cumbersome and will affect your users more than they already have been as a result of the migration.

Server Names

Properly named according to the conventions in other documents, this should not be a problem. However, the caveat is that if this will end up causing more problems than it will fix, server names can remain the same provided they change as soon as practical.

The reason behind this has to do with the fact you are now in a domain which may already contain a name similar to your server name if you have servers named, for example, APP, SQL or some such.

Offline File Synchronizations

We have run into a few users who have this in place. This will need to be turned off before the migration. It can be turned on afterwards.

Win2K Upgrades to WinXP

Windows 2000 machines when upgraded to Windows XP sometimes go from a FAT file system to an NTFS file system with the effect that the EVERYONE group is given Full Control of the entire file system. For security and practical migration reasons, this is not a good idea and will cause a migration of such a workstation to fail.

File and Printer Sharing

In this, the last of our ouchy series, a word for the migrating wise; do not turn off File and Print sharing on the NIC of your workstations. In addition to causing a lot of heartache for the migration team, it will cause your migration to fail.

Finish?

Hopefully you have obtained a somewhat fully realized picture of the migration and what managing your OU will look like after migration. Any failures in painting a complete picture can be addressed as needed. Fred Woodbridge's email address is fred.woodbridge@cio.idaho.gov. Feel free to send him any email containing your thoughts and questions. You can also send your questions to messaging.project@cio.idaho.gov. We welcome your feedback and will respond quickly.

Thank you for your time.

Fred Woodbridge
Idaho Office of the CIO
Department of Administration