**Auditing with Microsoft Assessment and Planning (MAP) Toolkit 5.0 – Part 1**

By [Sadequl Hussain](http://www.sql-server-performance.com/author/sadequlhussain/)

FROM: <http://www.sql-server-performance.com/2015/auditing-map-5-1/>

Auditing and inventorying is not something new in any IT environment. Depending on the purpose, it can take many forms. Sometimes the auditing is about security and data access. Sometimes it is about software usage and licensing. Often it is about consolidation and cost saving. Whatever the reason, the strategic direction typically comes from top management or decision makers. It is then up to the technical personnel or operation managers to come up with some sort of report that shows the figures.

Consider the following scenarios:

* Your company has decided to upgrade its core business application to SQL Server 2008 R2 and you are the DBA. You are to submit a feasibility study about whether the existing server has sufficient computing resources for an in-place upgrade.
* Your manager has just asked you to send a list of SQL Servers running within the organization. The commercial procurement team needs to have an idea about the number of SQL instances running in the network. They need the version and edition and they also need to know what version of Windows is running in those boxes. The total number will have to be broken down by category.
* As an IT manager, you are considering rolling out Windows 7 and MS Office 2010 on user desktops. You need a starting point, some sort of baseline that will give you an idea if the user workstations are powerful enough for the upgrade. On the server side, you are also considering virtualising some of the physical servers. You want a clear idea about the number of VMWare hosts sitting across the network.
* Experts from a vendor company have recently come and rolled out a system for your organization. The farm consists of web servers, app servers and database servers. You want to monitor the performance of each of the servers and check whether they conform to what the vendor had promised. You want the performance metrics from all these servers collected automatically and you want them to be consolidated in a single report.

The list can go on. Although there are tools for finding the information for each possible scenario, most of them would either require a licensing fee or they have to be custom developed, meaning there will be a dollar figure attached.

Instead of resorting to either approach, IT specialists can take advantage of some of the free tools available from Microsoft.  **Microsoft Assessment and Planning (MAP) Toolkit** is one such free application that can automate the auditing and inventorying process to a great extent. MAP is part of what Microsoft calls **Solution Accelerators**: software applications that help you take tally of what is running on your network and plan for better consolidation strategy.

Like I said, this type of tool is not something new. However, what sets MAP apart is its low footprint. Typically, the auditing software would be running on a centralized server with “agents” running on each machine. These Agents would have to be installed in each server individually and they will communicate with the central server on a set schedule.

MAP does not need any such agent. In fact it does not have to be installed on a server either and there is certainly no need to use a database back-end for which you have to pay a license fee. You can install it on a workstation running Windows XP, Vista or 7 and it will create a repository database running on SQL Server Express edition – which is free. Once installed, configured and running, MAP can go across the network and query each machine (servers or workstations), find its hardware configuration, see what software is running on it, what role it has in the network and then save that information in the local database. In MAP lingo, this process is called “inventorying”. It can then analyze the data collected and provide you with a detailed report and even generate a proposal document.

Although the tool reflects Microsoft’s approach to encourage customers to upgrade to its newer server and client technologies, it has it uses nevertheless. Even if you are not upgrading your servers overnight based on its recommendations, you still will have some useful information at hand.

**System requirements**

At the time of this writing, MAP is in version 5. It is available for free from the [download page](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=67240b76-3148-4e49-943d-4d9ea7f77730).

At a hardware level, the minimum CPU speed of the machine running MAP would have to be 1.6 GHz. Microsoft suggests dual core 1.5 GHz processors or faster. Memory requirement is 1.5 GB while hard drive space requirement is 1 GB.

At an OS level, MAP can run on any of the following client operating systems:

* Windows 7
* Windows XP Professional with SP2 or later

If you want MAP to be installed on a server, the supported OS include:

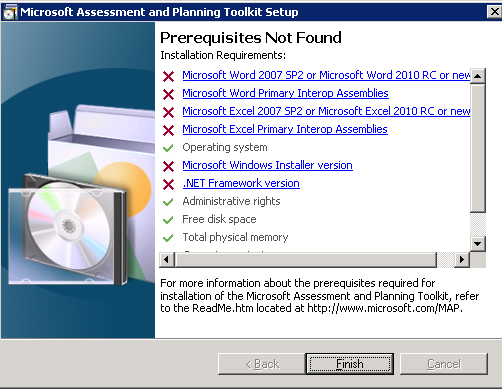
* Windows Server 2008 and 2008 R2
* Windows Server 2003 R2

The following are also required components:

* .NET framework 3.5 SP 1
* Windows Installer 4.5

Now it may sound logical to install such an auditing tool on a centralized server instead of a client workstation. However, MAP also requires MS Word 2007 (SP2) or MS Word 2010 as well as MS Excel 2007 (SP2) or MS Excel 2010 available in the machine where it is running:

Since MS Office is not typically found in server environments, running MAP installation in such cases will be unsuccessful. The following figure shows the error message I received when trying to install MAP in a server that did not have MS Office installed.

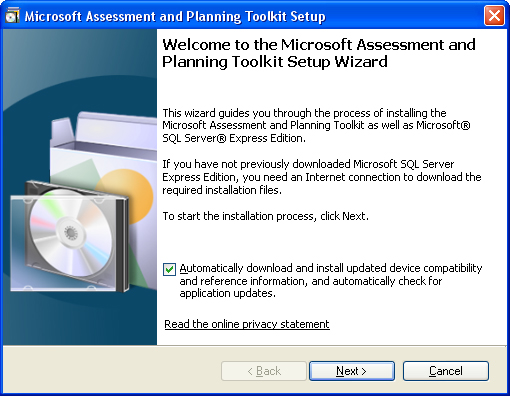


As most client workstations would have MS Office installed, a dedicated workstation can be a viable option. This can be the system administrator’s own workstation. Once the application has gained acceptance from management, a server environment can be allocated and configured.

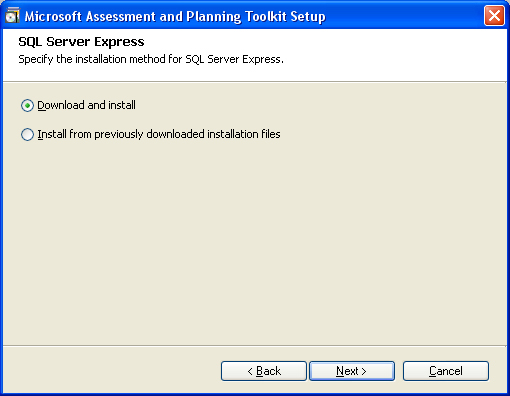
Last but not the least, MAP requires SQL Server 2008 R2 Express Edition for its data storage. Even if the machine already has an instance of SQL Server 2008 R2 Express already running, the setup program will still create a new instance. The instance name will be **MAPS**. MAP ensures this instance is exclusively configured for its purpose: it does not allow connections from remote computers and local access to the instance is limited to members of the local administrators only.

**Installation**

Installing MAP is a fairly straightforward process. If the prerequisites are met, the wizard takes you through only a few screens. I would suggest turning on the checkbox at the very first screen that says “Automatically download and installed updated device compatibility and reference information, and automatically check for application updates”.

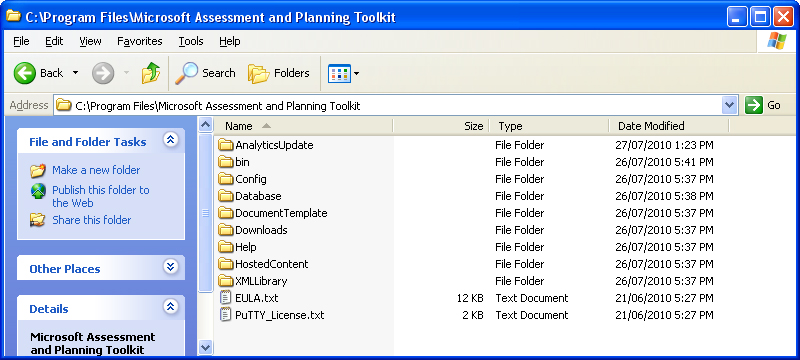


Also, the installer can download and install the SQL Server 2008 R2 Express edition during system setup, but you can direct it to the setup program in the disk.

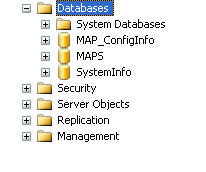


By default, MAP is installed in the Program Files directory. If your Program Files folder is under the C: drive, it will be C:Program FilesMicrosoft Assessment and Planning Toolkit

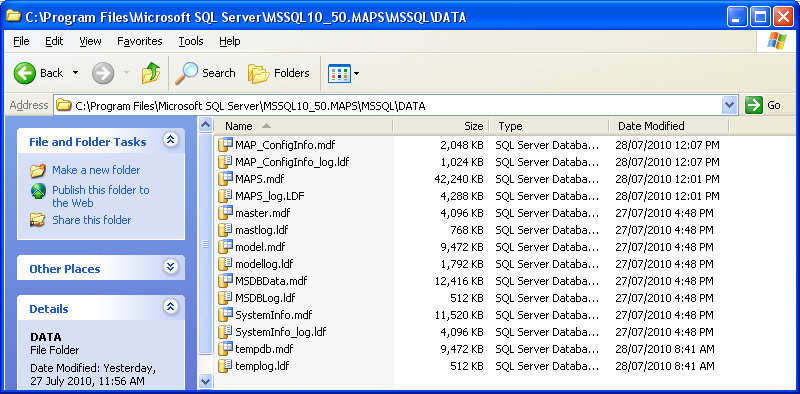
The following figure shows the various subdirectories created under the main folder:



There will also be two databases created in the SQL Server 2008 R2 Express instance: MAP\_ConfigInfo and SystemInfo. The third one will need to be created when you use MAP for the first time.



Although it may seem obvious, the database files for MAP toolkit is not created under the Databases folder of the program directory. They will be under C:Program FilesMicrosoft SQL ServerMSSQL10\_50.MAPSMSSQLDATA



However, I would strongly suggest *not* doing anything manually to the databases outside MAP. It is best you leave it alone the way it is. If you want to backup the database, there are scripts to do that and we will have a look at that later.

[Sadequl Hussain](http://www.sql-server-performance.com/author/sadequlhussain/)

**System configuration**

***Computer discovery methods***

Before going any further, let’s talk about how MAP finds the computers in the network. As I said before, it is an agent-less system, which means it needs to find the list of computers first before it can connect to them.

There are six ways MAP can “discover” the computers in your network (MAP 4.0 used five):

* **The Active Directory Domain Services (AD DS) :** If the computers you are trying to inventory are all in Active Directory, use this method. It is simple and all it requires from the user is a domain name and a domain user account credentials. You just point MAP to the relevant AD domain and MAP will query the domain controller using LDAP (Lightweight Directory Access Protocol) to find the list of computers. What’s more is that you have a finer degree of control over which computers you want MAP to monitor. Large organizations will have hundreds, often thousands of servers and not all of them will be relevant to your audit. Using AD DS, you can drill down the hierarchy of AD and can specify one or more particular domains or all domains in the forest, one or more containers or Organizational Units within a domain and / or other OUs contained under them.  
  The account you specify for MAP must be a domain account and a member of the Domain Users group.
* **Windows Networking Protocol:** This method should be used for legacy systems where you still have servers connected to a Windows NT 4.0 domain or if you have servers connected in workgroups.  
  When using this method, you need to ensure two services are up and running in the machine where MAP is running: the Computer Browser service and the Server Service. MAP makes use of the Computer Browser service to broadcast messages to target computers, and computers running Microsoft Windows will respond to that.   
  What happens if you have a network where majority of servers are connected to the AD and only some are located in workgroups? The answer is to use both methods, or as I would do, run the AD DS method first and then use the second method.
* **Using System Centre Configuration Manager:** The third method makes use of the System Center Configuration Manager (SCCM). If your organization uses SCCM and the servers you are trying to inventory are managed by it, you can point MAP to the SCCM and provide the appropriate credentials
* **Import computer names from a file:** You can also make a list of computer names and provide MAP with that. The file you will create needs to be a plain ASCII text file and have the computer names in each new line, without any commas or other delimiters. The names can be fully qualified domain names (like acctserv.mydomain.com) or NetBIOS names (e.g. ACCTSERV).
* **Specifying an IP range:** You can use this method if the servers you want to monitor belong to a specific subnet. In MAP, you just specify the starting IP address and the ending IP address; MAP will scan the network for the all computers in that range and try to connect to each of them. Microsoft suggests using this method when the AD DS or Computer Browser method cannot find the computers you are after.
* **Manual entry**: The last method you can use is to manually enter the computer names in the MAP wizard interface. You may wonder why or when you should use this method (or other manual methods like importing from a file): after all, MAP is supposed to be doing the finding for us. The answer is, you may be interested about only one or few particular servers. This may be the case if you are part of a large organization and do not have much visibility of the rest of the network apart from the relatively few number of servers you manage.

***Configuring the target computers***

MAP uses two principal methods for connecting to target computers and performing inventory:

* Windows Management Instrumentation (WMI)
* Remote Registry Service

Of these two, WMI is used for querying the remote machine to get information on hardware, software and device drivers. The Remote Registry service is used for discovering the role of the computer in the network. It is also necessary for the Performance Metrics Wizard.

There are two other methods MAP uses. The first one is used to connect to virtual machine hosts like VMWare ESX (VMWare Webservice) and the second is used to connect to Linux servers.

For the purpose of this article, I will assume you are using MAP for auditing your Windows-based computers. For this to work, you will need to ensure your target computers are running both the WMI and the Remote Registry services. There is no way you can either initiate or enable these services from MAP. You will either need to enable and start them manually in each computer from Control Panel > Services applet or you need to have your system administrators do this by setting a Group Policy for the OU or domain.

Next, for each target computer you will need to provide the username and password of an account that is a member of the Local Administrator group of that machine. MAP will use this logon credentials to connect to WMI running in that machine. Even when you are auditing a single OU within your AD, this may mean connecting to dozens or even hundreds of computers. Specifying a separate local administrator account for each of these computers is not practicable. There are two ways you can address this:

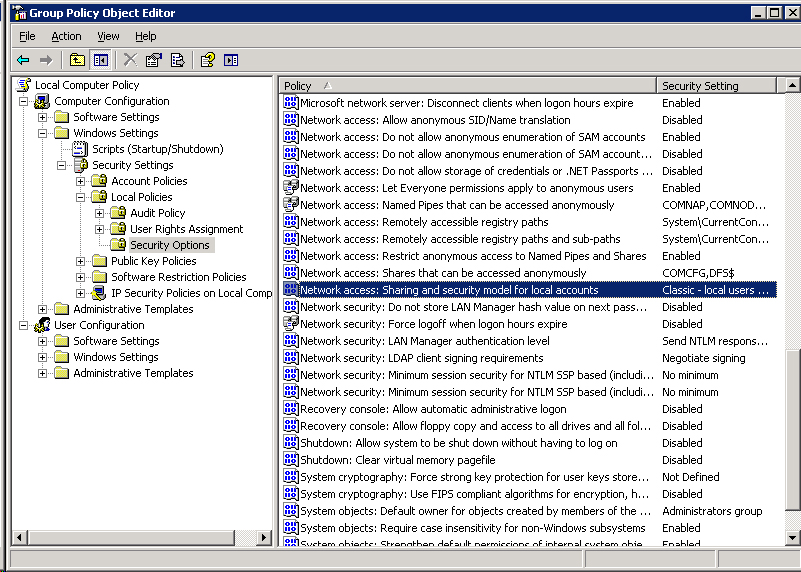
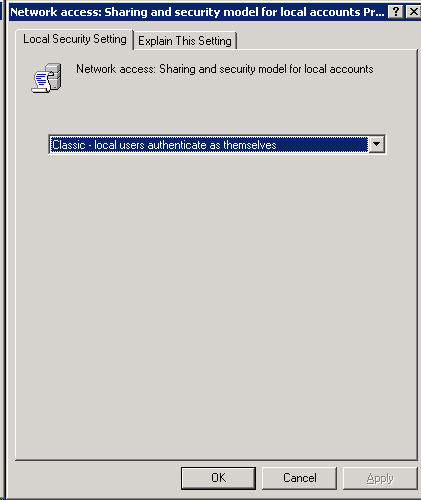
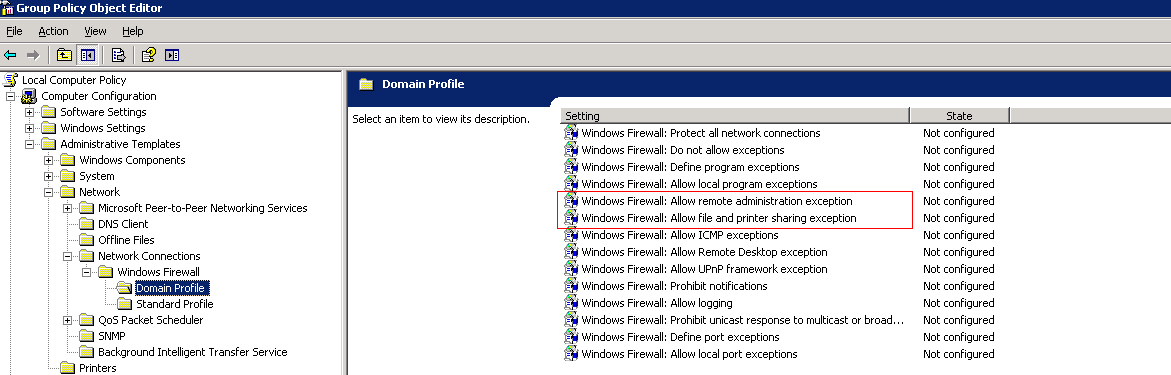
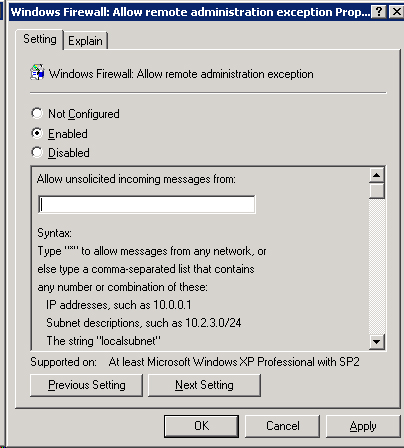
* If your organization has a domain account that is a member of the Local Administrator group in each machine, you can use that. An example would be a generic DBA or support person account.
* You can also use a domain administrator account. By default, Domain Administrators group is a member of the Local Administrator group in Windows servers.

Finally, you will also probably need to perform further tweaking on your target servers if they are running hardware or software-based firewalls, particularly Windows Firewall. This is because there are two things firewalls would not allow that MAP uses: remote administration via WMI and file & printer sharing. To enable both these options, the relevant TCP and UDP ports need to be opened up.

For remote administration, the TCP port is 135. For file and printer sharing, TCP ports are 139 and 445 and UDP ports are 137 and 138.

If your servers are running Windows Firewall, you can enable the ports either from the Local Security Policy or have your System Administrators create the appropriate Group Policy so that it propagates to the machines.

For enabling Windows Firewall exceptions through Group Policy at the AD level (for specific OUs or even domains), you need to follow these steps:

* Start the Group Policy Editor (you can run gpedit.msc from command prompt)
* Expand the Computer Configuration node. Underneath that, expand Windows Settings > Security Settings > Local Policies and then select Security Options. On the detail pane, double click on the entry for “Network access: sharing and security model for local accounts” (see below)  
  
* In the dialogue box that appears, choose “Classic – local users authenticate as themselves” option from the drop down list (see below) and click OK.  
  
* Now from Computer Configuration node again, expand Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile. You will need to enable two options here: *Windows Firewall: Allow remote administration exception* and *Windows Firewall: Allow file and printer sharing exception* (see below).   
  
* When you double click on the Windows Firewall: Allow remote administration exception option from the detail pane, you will see the following dialogue box:  
    
    
    
  Click on the Enabled option. In the Allow unsolicited incoming messages from textbox, type the IP address of the computer where MAP is installed.
* Click OK and follow the same process for Windows Firewall: Allow file and printer sharing exception option.
* The policy will take effect the next time Group Policies are propagated.

All we did here was instruct Windows Firewall to allow specific traffic from the MAP computer which would otherwise be refused.

If your target server is running another firewall (software or hardware based), you will need to follow its own procedures for enabling remote administration and file/printer sharing.

You can now see that although MAP is agent-less, there are a number of configurations prerequisites that need to be satisfied. Some of these will be beyond your control and in the domain of network administrators. That’s why you will need to liaise with your network system administrators and build an effective relationship to get their buy-in. Network administrators will inevitably be reluctant to change a Group Policy or opening a firewall port. You will need to give them the confidence that these exceptions will not be made on a permanent basis, rather only for the duration of the audit.

In fact it would be even better if you can tell them about the specific servers. The approach I would take is to run the MAP toolkit first without enabling any exceptions. This is possible as long as you have access to a domain account (MAP will use that for querying the AD) and an account that is a member of the Local Administrator group in each machine.

Once you have run the Inventory and Assessment Wizard for the first time, you can generate a report (we will see how it is done shortly). In the Excel spreadsheet of the report, you can look up any computers for which the WMI status does not show “Success” or refer to the MAP high level report showing “insufficient data”. You can use this as a starting point for further investigation.