Global Information Assurance Certification Paper

The following is a practical assignment describing the steps taken to automate changing Service account passwords through the use of scripts, batch files, and a program called Service Manager NT.

Strong passwords are critical in the development of security for a network. For this reason I have selected the following topic for my practical.

Setting up a strong password on the Services accounts on your network.

When an account has its password changed, those changes are synchronized throughout the Domain. Accounts that are used as a service, however, do not get the password information updated automatically. For this reason you would have to go to each system in your Domain and manually change the password to match the new Domain Account password. Otherwise the service fails, or generates error logs in the event viewer, particularly after a reboot.

The following procedures are steps that we have taken in order to simplify this task by setting up Scripts and Batch files that will automatically make these changes throughout the network. These scripts also generate log files that will help to identify those systems that did not accept the scripts. At which time an application that can edit services on remote systems will be used to modify the password of the service account. This report will also cover how to change the local Administrator account password throughout the network. An account that, in many cases, is used to run as a service.

Background

All systems are running Windows NT 4.0 Service Pack 4 or greater with Internet Explorer 5.1 SP1. I also have the Windows NT 4.0 Server Resource Kit, with Supplement 4. I have added the \ntreskit path to my path statement under the system properties to make it easier to execute some of the script/commands.
Many of the commands in the batch files and scripts are part of Windows NT Resource Kit. The NT Systems should have at least Service Pack 4.

Step 1.1

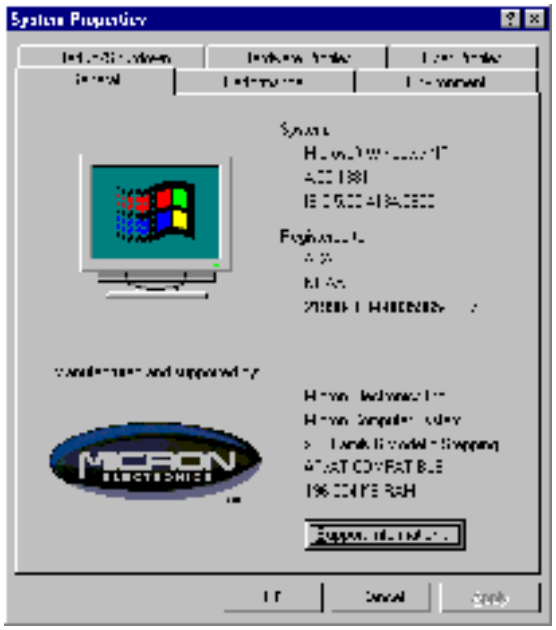
Install Windows NT Resource Kit on your workstation/server.

Step 2.1

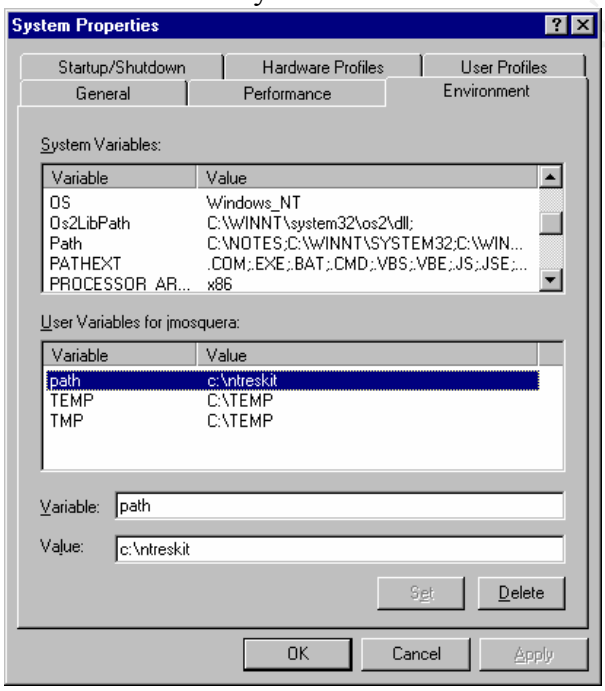
Add the Resource Kit path to your system path or User Variables path.

To add the Resource Kit to your system path perform the following steps.

Right click on the My Computer Icon, select the Properties tab:



Next step is to click on the Environment Tab and add a path statement to the user variables. That path statement should include the path to your Windows NT Resource Kit installation directory.



Plan to place all batch files and scripts in the \ntreskit directory for the sake of simplicity.

Step 3.1

The third step is to synchronize the time on your entire Domain so that the scripts

run on all of the systems at the same time. This may not be possible on Domains that span different time zones. I have found that these scripts submit the commands to be executed based on the system submitting the command. If the time submitted is out of synch or has already passed then the change will take place in 24 hours. You can also include a timed delay in executing the command.

Step 3.2

You will be able to do this by performing the following.
Identify all systems on your Domain. This is done in order to create a list of systems on your Domain. This computer list will be used by the scripts. The following script performs this task. Make certain that the list includes all of your Domain systems. Particularly any servers you want to apply these changes to.

The script was found on the following web site
http://www.jsiinc.com/TIP0600/rh0677.htm

677 » How can I build a file of member computer names in my domain?
The NETDOM utility from Supplement Two of the Resource kit can list members with the NETDOM member command. You can use this feature with the following
member.bat file placed in your path:

```
@echo off
if "%1"=="" goto badp
If exist %1 del /f /q %1
for /f "Skip=5 Tokens=1* Delims=\" %%i in ('netdom member') do if not
.%%j.==.. echo %%j >>%1
@echo Syntax: member "<Drive:>\<Path>\Filename.ext"
```

Copy the above script into a batch file named member.bat, and place it in the \ntreskit folder.

To generate a file of member computer names, type:
Member "<Drive:>\<Path>\Filename.ext"

The output is as follows
SYS-NT-01
SYS-NT-02
SYS-NT-03
SYS-NT-04
SYS-NT-……

Step 3.3

Next I created a batch file that ran the command to all of the remote

systems. I utilized the SOON command from the NT resource kit. The SOON command replaces/augments the AT command. Replace the *server* with whatever system you have as your default timeserver. I would suggest that it be one, which is synchronized with the NIST atomic clock. http://www.time.gov/. Also, be certain that the batch files are run from an account that has administrative privilege on the Domain.

Modify the output in the Filename.ext to reflect the following. Replace SYS-NT-01 with your system names.

soon \\SYS-NT-01 80 CMD /C "net time *server* /set /Y" >> netime.dat
soon \\sys-nt-02 80 CMD /C "net time *server* /set /Y" >> netime.dat
soon \\sys-nt-03 80 CMD /C "net time *server* /set /Y" >> netime.dat
soon \\SYS-nt-04 80 CMD /C "net time *server* /set /Y" >> netime.dat
soon ……..

The command includes an 80 second delay.
The ">> netime.dat" portion of the command will output information about the command to a text file. This generates a log to see if there where any problems communicating with particular systems.

The file netime.dat is an output file showing if the command was successfully delivered. The syntax is as follows.

"Added a new job with job ID = 1

SOON : AT \\SYSTEM-NT-01 06:49:12 CMD /C net time *server* /set /Y"

You can also check what commands are currently queued by the SOON/AT command, on a remote system, by typing the following:

AT *systemname*

This will give you the following output

Status ID	Day	Time	Command Line
1	Next 15	6:49 AM	CMD /C net time *server* /set /Y

The above means that there is command queued to execute @ 6:49 AM on that system.

In order for time change command to finish successfully it may be necessary to wait 24 hours, especially for systems in other time zones, or those that have the wrong time zones configured.

Step 4.1

Changing the Local Administrative Password on all workstations without traveling. Many shops use the same username and password on their Domain and local systems. (At least they do in this shop, even though they shouldn't) In particular, when a system's software is configured it is set-up with an administrative account. That account may have been the local admin account. If so, then we need to change the local account password to match the Domain and Service account passwords.

The following is a step by step description on how to do this.

http://www.jsiinc.com/TIP0100/rh0199.htm

199 » How do I change the local Administrator password on all my Workstations without traveling?
I use the Soon command from the reskit but the AT command will work:
soon \\MachineName cmd /c "net user AccountName NewPassword"
I use a batch file:

echo on >password.log
@echo MachineName1 >>password.log
ping MachineName1 >>password.log
if %errorlevel%==0 soon \\MachineName1 cmd /c "net user AccountName1 NewPassword1" >>password.log
@echo MachineName2 >>password.log
ping MachineName2 >>password.log
if %errorlevel%==0 soon \\MachineName2 cmd /c "net user AccountName2 NewPassword2" >>password.log
*@echo ** end of file ** >>password.log*

Create a batch /script called local.bat from the above and place it in the \ntreskit folder. The next step is to simply replace the "MachineName1" with the name of the system that is in your domain. Then replace AccountName1 and NewPassword1 with the account and password that you want to change.

By synchronizing the time on your domain (Step 3) these commands will take place simultaneously on your network. Except, of course on those systems that are in different time zones. They will likely have a delay of up to 24 hours.

After editing, the Script should look like this:

echo on >password.log
@echo SYSTEM-NT-47 >>password.log
ping SYSTEM-NT-47 >>password.log
if %errorlevel%==0 soon \\SYSTEM-NT-47 180 CMD /C net user Administrator password >>password.log

*@echo ** end of file ** >>password.log*

Where *Administrator* is your local Admin account and *password* is your new Admin password.

You can also check what commands are currently queued by the SOON/AT command, on a remote system, by typing the following:

AT *systemname*

This will give you the following output

```
Status ID   Day                 Time         Command Line
-------------------------------------------------------------------------------
     1   Next 15               6:49 AM      CMD /C net user Administrator password
```

The above means that there is command queued to execute @ 6:49 AM on that system.

There is a problem with this script, in that the AT *systemname* command will display the username and password in cleartext until the AT command runs or is deleted. To delete an AT command remotely, type the following:

AT *systemname* id /delete

The "id" refers to the id number assigned to the command you want to stop. In the above case the id number is 1.

In order for the time change command to finish successfully it may be necessary to wait 24 hours, especially for systems in other time zones, or those that have the wrong time zones configured.

Step 5.1

The next step is to change the password of the service accounts on all of the systems on your Domain. An account that is used to run as a service does not automatically change the password when the account is changed on the local system or on the Domain.

The preferred accounts for service to run under are:

1) System
2) Local
3) Domain

With 1 being the most preferred.

The following is a set of scripts that perform this task without having to

touch each system. The scripts where found at:

http://www.jsiinc.com/TIP0600/rh0691.htm

0691 » How do I reset the password on all services in my domain that run in the "ServiceAccount" context?

If you have services that run in a DomainName/UserName context on multiple machines in your domain, resetting the DomainName/UserName password can be quite a chore.
To totally automate this process using NETSVC and SC from Supplement Two of the Resource kit, add the following batch files to your path (\ntreskit directory):

SetSvcPw.bat >>>>>>>>>>Containing>

```
@echo off
@echo SetSvcPw %1 %2 %3
if exist %1 goto OK
@echo Syntax: Error: SetSvcPw "<Drive:>\<Path>\ComputerName.txt"
DomainName\UserName password
goto end
if .%2.==.. goto bad
if .%3.==.. goto bad
for /f %%i in ('type %1') do call :setsvcpws %%i %2 %3
goto end
:setsvcpws
if exist %temp%\NETSVC.LOG del /f /q %temp%\NETSVC.LOG
for /f "Tokens=1,2* Delims=<>," %%a in ('netsvc \\%1 /list') do echo
%%b >> %TEMP%\netsvc.log
for /f %%s in (%TEMP%\netsvc.log) do call SetSvcPwT %%s %1 %2 %3
if exist %temp%\NETSVC.LOG del /f /q %temp%\NETSVC.LOG
```

SetSvcPwT.bat >>>>>>>>>>>>>Containing>>

```
@echo off
if "%1"=="ECHO" goto end
for /f "Tokens=1,2,3* Delims= " %%i in ('sc \\%2 qc %1') do call :user
%%k %1 %2 %3 %4
goto end
if /i NOT "%1"=="%4" goto end
echo \\%3 %2 %4 %5
sc \\%3 stop %2
sleep 4
sc \\%3 config %2 obj= %4 password= %5
sc \\%3 qc %2
sc \\%3 start %2
:end
```

To run the job and log the results, type:
SetSvcPw "<Drive:>\<Path>\ComputerName.txt" *DomainName\UserName password* >> "<Drive:>\<Folder>\SetSvcPw.log" 2>&1

Where "<Drive:>\<Path>\ComputerName.txt" contains a list of computer names in your domain. Here you can use the file created in Step 3.2.

Output to the .log file is as follows:

```
SetSvcPw "c:\names.txt" DomainName\UserName password
\\system-nt-16 Diskeeper DomainName\UserName password

SERVICE_NAME: Diskeeper
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED

        (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
[SC] ChangeServiceConfig SUCCESS
[SC] GetServiceConfig SUCCESS
```

Error messages of systems that fail the update are also shown here.

STEP 6.1

Change the Domain Administrator password to match the service password that you have just changed. Remember that you should probably wait at least 24 hours to do this in order to allow systems in different time zones to implement the previous scripts.

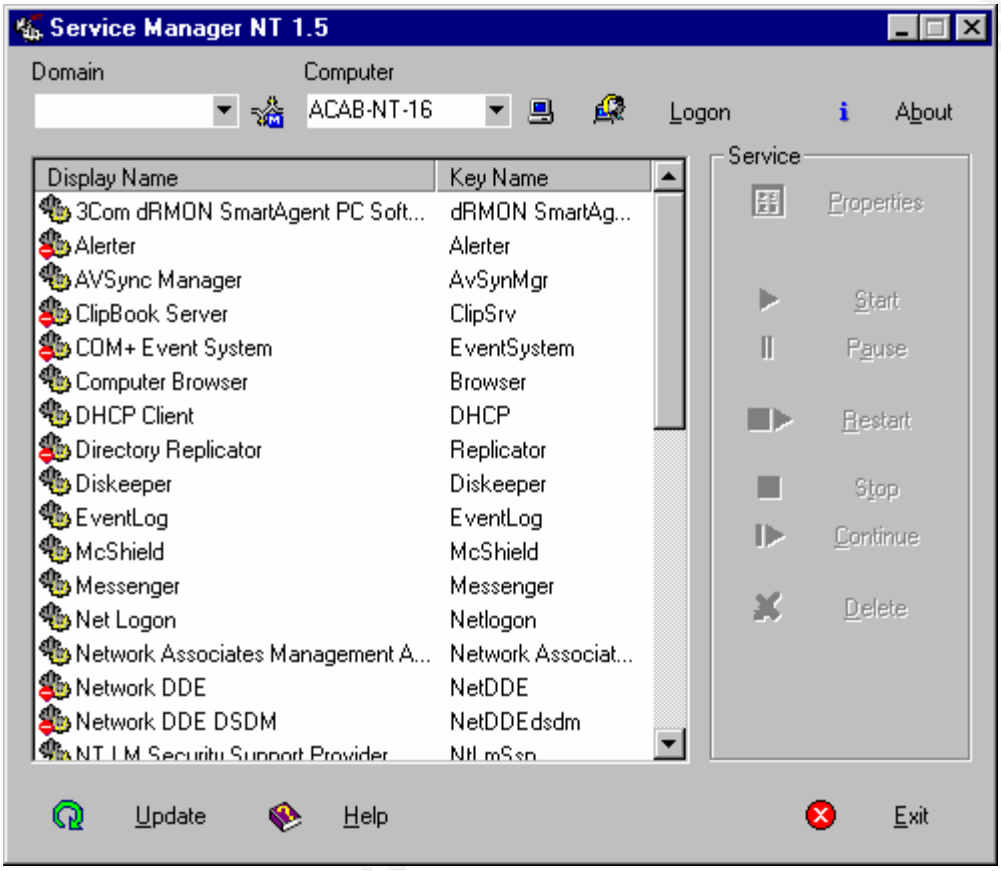
Step 6.2

Reboot the machines to make certain that the update was successful. If any of the services fail to come up when the system re-boots you know that you have a problem. Check the "Event Viewer" for any error messages. I have also found a nice little tool that lets you access the "Services" of remote systems.

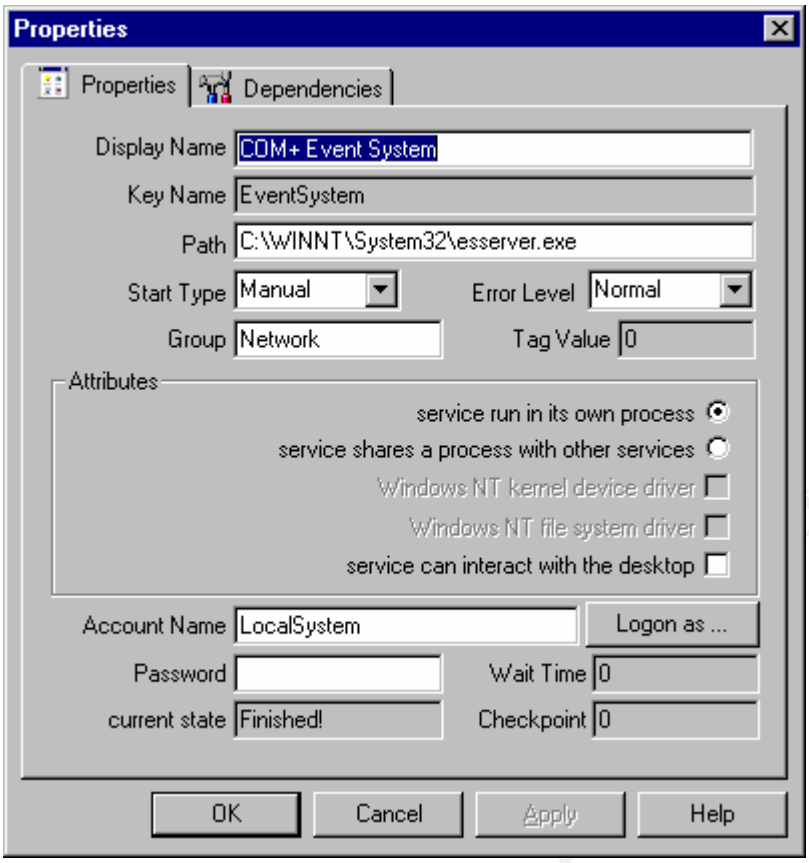
You can even use this to make changes to the Services accounts remotely. It is much more time consuming to go over each system, and each service, one at a time.

The program is called, “Service Manager NT”. It is available for download from the following URL. http://www.nttools-online.de/english/nttools.htm .

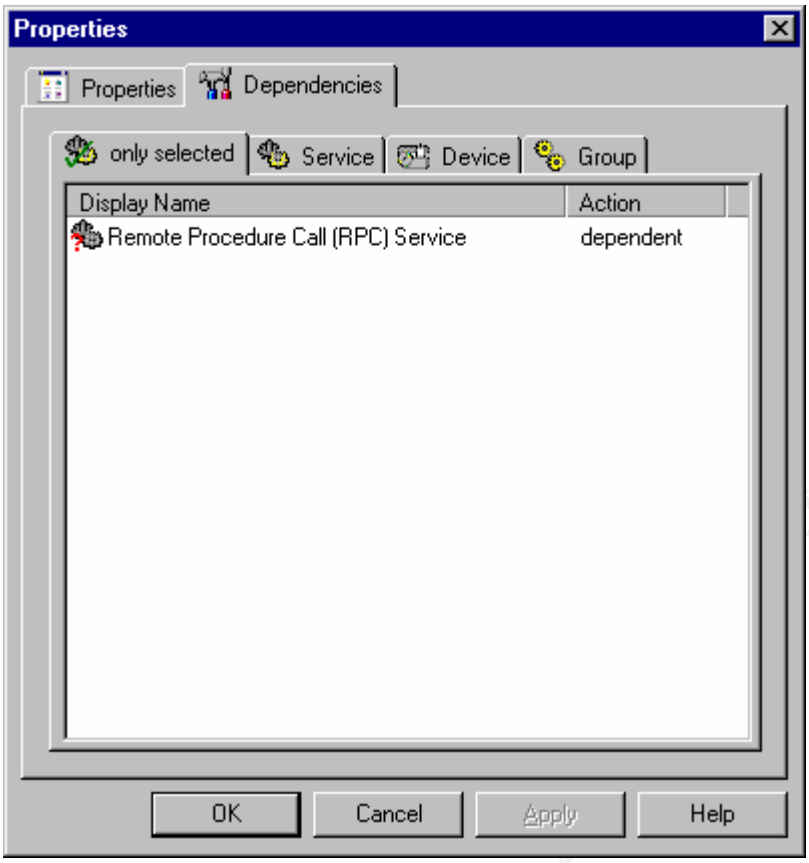
The startup screen looks like the following capture.



The program has areas where a Domain name can be entered, it also has an area that has a list of systems in the current Domain. It has buttons to stop and start the service. This program will allow you make many modifications to a service. By double clicking on a Service you get the following screen.

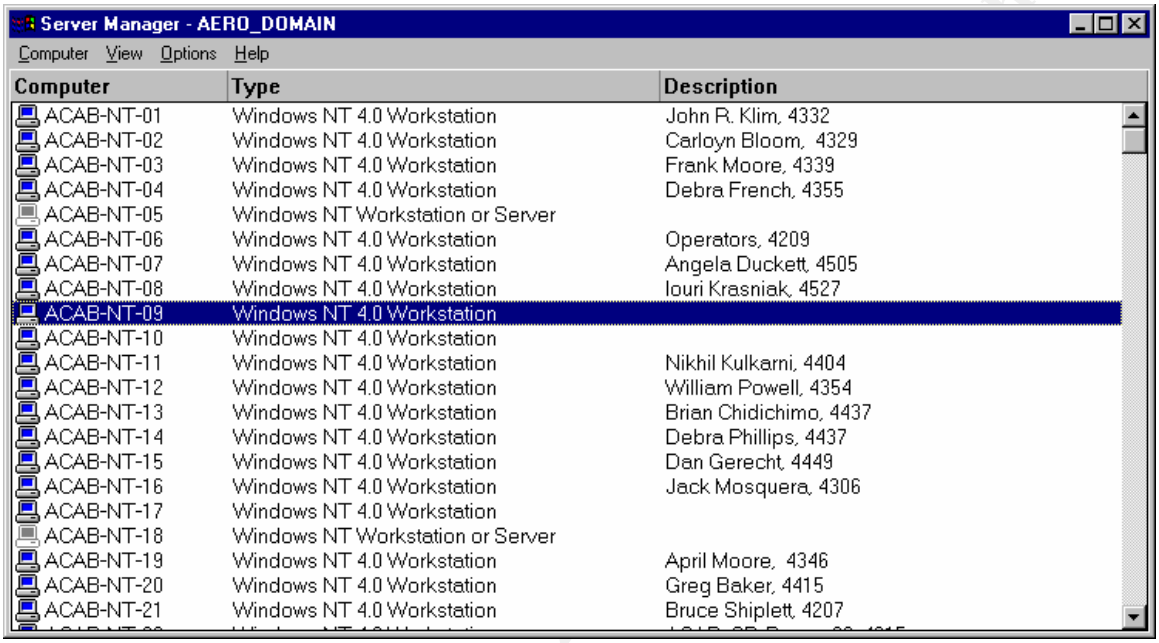


This screen has areas where the path to the service can be entered, the start type, error level, the account name and password settings. As well as a Dependencies tab. Which shows the following screen capture.

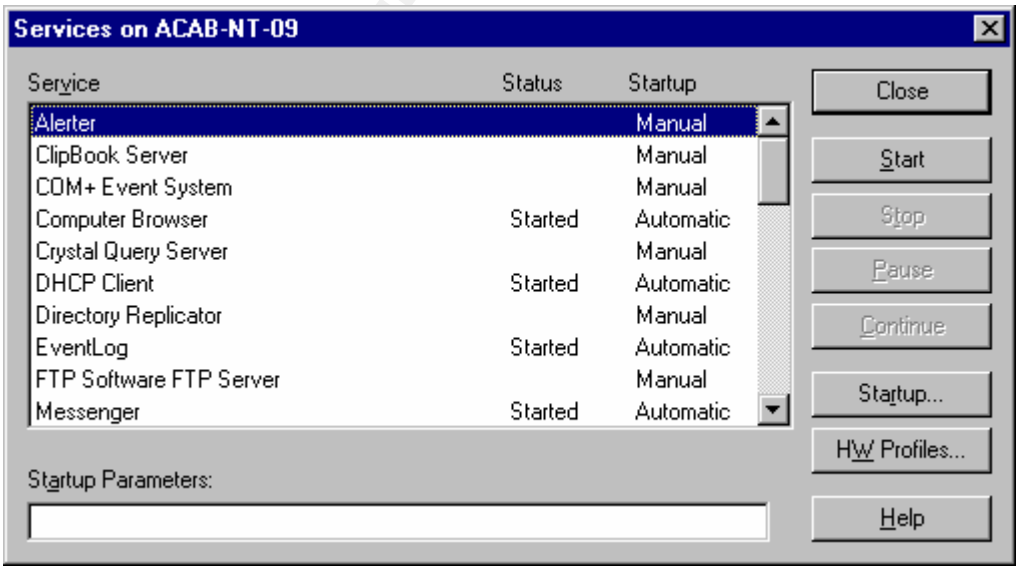


This indicates that the service selected is dependent on the Remote Procedure Call (RPC) Service to run properly. A recommendation, and something that I have done, is that I have tested all of these scripts, batch files and programs on test workstations. This has allowed me to familiarize myself with any problems, messages, and log files, before actually applying the changes. Another recommendation is to consider using the Service Manager NT program to make all of the service changes to your servers by hand. That way you can be certain that they will reboot successfully, providing you with minimal down time.

If you don't want to use the above utility to change service information/accounts, you can always use Server Manager. This is a program in the Administrative Tools. If you are on a Server click the START button on the toolbar, then the Administrative Tools, then click on Server Manager. This will give you the following screen.

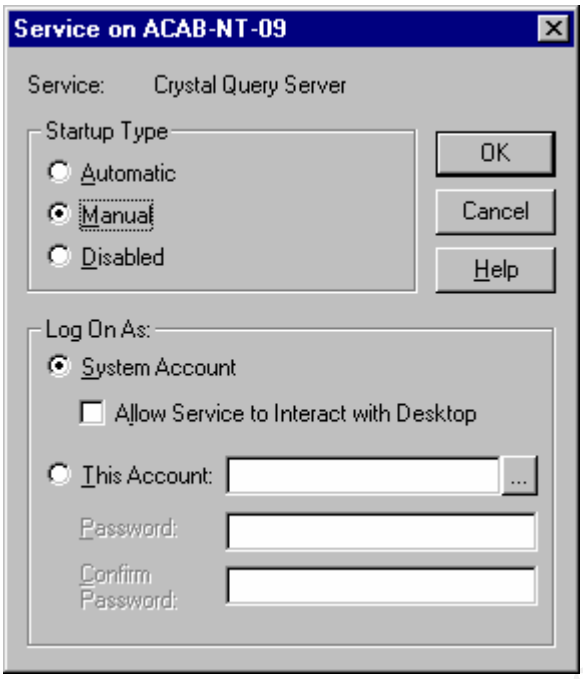


If all of the systems on your Domain are not listed click on View, and select ALL. This will display all of the systems on your network. To edit the services you would next click on a system then click on the Computer pull down menu. Select Services. This will look like the following screen capture



From here you can double click on any service and edit any of the properties

displayed.



This process works just as well as the Service Manager NT program but it is much more limited in its abilities.