How to set up IIS to use a domain user for the anonymous web user

By Colin Young

When creating a complex ASP application it is often necessary to communicate with other servers on your network for services such as file storage or databases. This leads to 2 major sources of initial errors, both of which may be attributed to permission problems.

The first type of error manifests itself when you attempt to access files in a shared directory on another machine. Fortunately this error is easy to spot since it actually reports itself as permission denied. The other type of error occurs when you attempt to connect to a database on another machine. This problem will become apparent when you first attempt to connect to your database from an ASP page and, after waiting an inordinately long time for any sort of response, you will be given the rather helpful default ODBC error that some CreateFile function failed.

Luckily for us the solution is simple. Before proceeding to the solution, however, it is helpful to understand what is happening in the background.

The default installation for IIS creates a local user account to be used as the security context for the web server. This user is local to the machine that is running the web server software, and will not be recognized on the network. The obvious solution is to make the machines you are attempting to communicate with recognize the web server's user. By default, this user is called IUSR_MACHINENAME (where MACHINENAME is replaced with the actual name of the machine the server is running on as it is referred to on the network).

During setup, a random password is created for this user. One solution is to recreate the user on all the machines that the web server will need to communicate with. This approach requires you to change the default password in two places (the web server and in the User Manager for Domains utility for the local "ghost" domain). You will then need to add the user to the other servers (again in the User Manager for Domains on each machine, only in the local domain). This method is the most secure but requires the most administration if you need to change passwords.

An easier method is to simply create a domain user and tell the web server to act as that user, therefore taking advantage of the integrated domain-based security in NT. There are a couple of things to make sure of though. So, here's how to set up IIS to use a domain user for the anonymous web user.

- Add IUSR_MACHINE (replace MACHINE with the name of the web machine) to the domain.
- Grant log on locally to IUSR_MACHINE (not done automatically)
- Add DOMAIN\IUSR_MACHINE (replace DOMAIN with the NT domain the user belongs to, e.g. CEOGROUP.COM) to the anonymous user in Internet Service Manager. Put in the password you assigned to the user.

- Turn off NT challenge/response. That will enable us to detect potential problems by not having our local domain users automatically authenticated via the NT methods.
- Grant read privileges to IUSR_MACHINE on the root web directory and all subdirectories (and any virtual roots on virtual servers if they are not under the main root).
- Test.

When choosing the anonymous user, use a name that is not likely to be guessed, and a password that will be difficult to guess. If you follow standard security measures for passwords and login names you should be safe. Also, restricting the anonymous web server to allow access to only what is absolutely necessary is a very good idea.

There is one more warning - if you use FrontPage to manage your webs, do not attempt to adjust permissions or virtual directories manually using IIS. Microsoft’s position is that you should use either FrontPage or IIS to manage your virtual directories. Using both will lead to bizarre behavior that can be very difficult to track down, but that’s another story...

About Colin Young

Colin studied Mechanical Engineering and actually got his degree! Now he is putting it to good use writing database programs for the internet. Started in unix Oracle, switched to NT and SQL Server and never looked back. Currently working for The CEO Group Inc. No personal web page yet. Maybe someday if he ever gets time or find something that needs to be shared with the world. Hobbies include turning his office into a jungle (the real type with plants, he's not referring to the mess of papers covering his desk).