



F1 Solutions September 2005



::REM

Hello All,



I've always liked September. The air seems cleaner and I always feel a little more energized. I also always like going back to school. Even though I haven't been in any real school for longer than I'll admit to, I still enjoy learning new things. Even better, I enjoy teaching new things. That's one of the reasons I find this newsletter rewarding, and some of you do as well. Check out some Reader Feedback on the next page. I'm finishing up work for the Techmentor conference in San Jose next month. I think there is still time to register at <http://www.techmentorevents.com>. If you missed the August webcast on scripting Exchange 2003, you can view it online at <https://msevents.microsoft.com/CUI/Register.aspx?culture=en-US&EventID=1032276551&CountryCode=US>

We received some excellent feedback and comments. If you attended, I hope you found it worth your time.

The new scripting book is also coming along nicely. I think we're still on track to finish the manuscript this fall. I expect the Microsoft Press will get the book out early next year. I'll keep you posted.

My mailing address has changed so if you keep track of that sort of thing, check the last page for the updated address. I'll also get it updated on the web site.

As always, I appreciate your continued support and welcome all comments, suggestions and feedback at jhicks@jdhitsolutions.com.

~Jeff

Groove Virtual Office

I've been using Groove Virtual Office 3.1 for the last few months. They offer a 60 day trial and since some of my work seems to require it, I decided to spring for a Groove Professional license. Don Jones and I have been using Groove to collaborate on the scripting book as well as the Techmentor sessions.

Groove is ideal for virtual offices or teams. Since Don is on PST and I'm on EST, being able to work asynchronously has been very helpful. The center of Groove is a shared workspace. This can be a standalone workspace with documents, a shared calendar, discussions and more. Or you can share a directory on your computer and Groove will synchronize it with all members of the virtual team.

Synchronization is essentially peer to peer but is change based. Uploads and downloads never seem to take much time and you can work offline if you choose.

Volume 2, Issue 9

September 2005

Special points of interest:

- Reader Feedback
- RodentNet
- WMI Events
- WMI Domain

Inside this issue:

Web Crawling	2
Feedback	2
Tech Tutor	3
10 Minute Scripts	4



Groove 3.1- cont'd.

Groove offers it's own chat and mail service as well. In addition, the workspace provides presence information. If I'm in a workspace, I get a small notification when Don "enters". We can quickly establish a secure chat. Or if one of us is offline, we can leave a mail message. The benefit as I see it is that all work related mail and documentation stays in one location.

For the Techmentor sessions I built a workspace, there are several templates to choose from, and started adding

Powerpoint presentations. I was able to edit the file directly from the workspace. When finished, Groove prompts you to save the changes back to the workspace. This workspace and all the files were then synchronized with Don. I like that this functions as a poor man's disaster recovery tool.

There's much to Groove that I haven't tried yet such as creating forms, document reviews, shared pictures, shared whiteboard and more.

Of course, now that Microsoft owns Groove, it will be interesting to see how it integrates the product into its suite of collaboration tools such as Sharepoint, Exchange and Live Communication Server.

But for now, for distributed teams, ad hoc projects, or just organizing your own work, Groove has a lot to offer. You can try it for free for 60 days yourself.

See more at <http://www.groove.net>.

"September: it was the most beautiful of words, he'd always felt, evoking orange-flowers, swallows, and regret"

—Alexander Theroux

Web Crawling—RodentNet

There are many web sites with free IP tools like DNS Report (<http://www.dnsreport.com>) and DNS Stuff (<http://www.dnsstuff.com>). I came across another one recently with a very intriguing name, Rodentnet. Although I'm not sure what the connection is with rodents, the site offers a number of very interesting and useful IP related tools. Lookup tools are always nice (and this site has many), but I also like testing tools that run checks. For example, on the site I can test if I have an SMTP open relay or if a server has been blacklisted. This is very handy when troubleshooting a client's mail problem.

Many of these tools are actually run from other sites, but it's nice to have them all in one place and to be able to pass values right from the page. It doesn't look like the page has been updated in a while and not all tools seem to work all the time, but you still might find something useful.

You can visit Rodentnet at <http://tatumweb.com/iptools.htm>

Reader Feedback

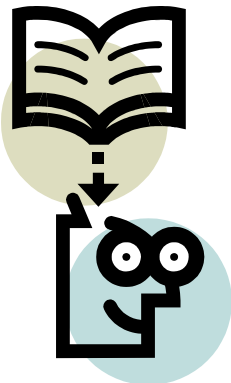
I've been amazed at the growing number of people who find my newsletter interesting enough to subscribe to. If you find it of value, I hope you'll pass it on to your friends and colleagues and invite them to subscribe as well.

I thought I'd share some recent reader feedback.

"You newsletters are great. I've already printed, hole punched, added ALL of them to my "Secrets of the Universe" (Windows AD/Exchange stuff) notebook."

-M.S.

That's a pretty high bar to meet but I'll continue to do my best.



Tech Tutor — WMI Events

I've been working a bit with WMI events in preparing for the Techmentor conference and in the new book. I thought I'd add a tutorial or two here as well. We can use WMI events to monitor systems and take action when certain things happen.

A WMI Event is a special type of WMI object that is created when certain Windows events fire. This is a system object so it is prefixed with a `__` like this `__Event`. The `__Event` class is abstract, meaning it isn't tied to anything specific. There are different types of `__Event` classes, but the one that we will use the most is the `__InstanceOperationEvent` which has child classes of

```
__InstanceCreationEvent
__InstanceModificationEvent
__InstanceDeletionEvent
```

The default query method is `semisynchronously` which uses the standard return flags of `wbem-FlagForwardOnly` and `wbemFlagReturnImmediately`. However, we can also query for events asynchronously. Using the latter method our script can continue to execute code until the event fires, at which point the event triggers another portion of the script to run. We'll get into that in more detail at a later time.

The query is similar to a data query, but in this case we want event information. So instead of a query like "Select * from Win32_logicaldisk where DeviceID='C:'", we query for an event, "Select * from __InstanceCreationEvent where TargetInstance ISA win32_ntlogevent". You'll notice some differences between the two. First, the class is the system class of `__InstanceCreationEvent`. This refers to anything that is created in the CIM repository or on the system such as a process starting, a file being created or an event log being written. Because this class can return more information than we could possibly process or find of interest, we restrict the query using a WHERE clause. In a data query, we use WHERE clauses to limit the data returned based on the values of one or more attributes, such as DeviceID in our first example. With event queries, we use `TargetInstance`. The second difference you'll notice is in the operator. We don't use = because `TargetInstance` isn't like an attribute that has an exact value. Instead we use ISA, which works just like it looks in plain English. Our event query is asking, "Tell me everything you know when a creation event occurs and the type of creation is an NT Log event."

One way we can execute this query is to use the `ExecNotificationQuery` method. When this method is executed, an event object is returned. Let's run this through `Wbemtest` to see how this works.

Open `WbemTest` and select the `Enable All Privileges` checkbox. (Because an event log might be security related we need to explicitly enable the `SeSecurityPrivilege`). Click `Connect` and change the namespace to `root\cimv2`. Click `Connect`. Next, click the `Notification Query` button. Enter `select * from __InstanceCreationEvent where targetinstance ISA 'win32_NTLogevent'` for the query string and click `Apply`. `Wbemtest` is now waiting for an event to happen.

Open a command prompt and stop a service (ie net stop spooler). You should get a couple of entries in the `Query Result` window. Double-click on one of them to view the properties of the instance. As you can see, there is not much information here that is of use, other than perhaps the `Time_Created` property. But notice the `TargetInstance` property? You should see that it is listed as an embedded object. This is the object we want to work with. Double-click on `targetinstance` which should bring up the `Property Editor` window. Click `View Embedded`. Now we can see all sorts of properties that we might find useful such as `Message`, `Event Code` and `Source Name`. These are the types of properties you would expect to see with an event log. You can cancel and close out the windows to stop the query.

This type of query sends a notification when the event happens and returns the embedded object we just saw. Next time I'll show you how to work with notification queries in a VBScript.



"It is only the ignorant who despise education."

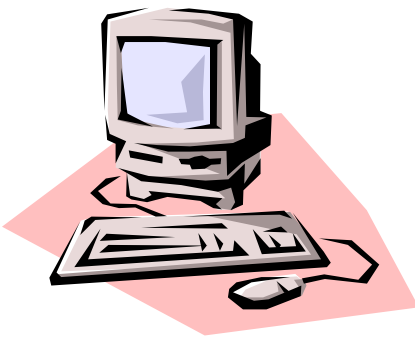
— Publius
Syrus (42 B.C.)

JDH Information Technology Solutions

6349 Tulipwood Lane
Jamesville, NY 13078

Phone: (315) 256-7023
Fax: (315) 295-2534
E-mail: jhicks@jdhitsolutions.com

WE'RE ON THE WEB AT
HTTP://
WWW.JDHITSOLUTIONS.COM



If you wish to no longer receive this newsletter, please send an email to:

newsletters@jdhitsolutions.com

Use a subject line of Unsubscribe.

This newsletter was created with
Microsoft Publisher 2003

Copyright 2005 All Rights Reserved
JDH Information Technology Solutions, Inc.

All trademark names are property of their
respective owners

Disclaimer:

All code and script samples are provided
'as is' with no warranty, either expressed
or implied.

Use at your own risk and test thoroughly in
a non-production environment.

Mission Statement

Our mission is to provide outstanding information technology consulting services and solutions to our clients utilizing a value-oriented approach. We recognize that most information technology projects are goal not hour driven. Our aim is to leverage technology to solve our clients' business challenges in the most cost-effective manner possible. We succeed when they succeed.

10 Minute Scripts

Windows XP and Windows 2003 include a new WMI class, Win32_NTDomain. This class can provide some interesting information about your active domain. Here is a sample script showing some of the information. Not every attribute may be populated. You can run this script connecting to a Windows 2003 domain controller or an XP desktop that is a domain member.

```
strComputer="."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" & strComputer & _
    "\root\cimv2")

Set colItems = objWMIService.ExecQuery("Select * from Win32_NTDomain")

For Each objItem in colItems
    Wscript.Echo "Client Site Name: " & objItem.ClientSiteName
    Wscript.Echo "DC Site Name: " & objItem.DcSiteName
    Wscript.Echo "Description: " & objItem.Description
    Wscript.Echo "DNS Forest Name: " & objItem.DnsForestName
    Wscript.Echo "Domain Controller Address: " & _
        objItem.DomainControllerAddress
    Wscript.Echo "Domain Controller Address Type: " & _
        objItem.DomainControllerAddressType
    Wscript.Echo "Domain Controller Name: " & _
        objItem.DomainControllerName
    Wscript.Echo "Domain GUID: " & objItem.DomainGuid
    Wscript.Echo "Domain Name: " & objItem.DomainName
    Wscript.Echo "DS Directory Service Flag: " & _
        objItem.DSDirectoryServiceFlag
    Wscript.Echo "DS DNS Controller Flag: " & _
        objItem.DSDnsControllerFlag
    Wscript.Echo "DS DNS Domain Flag: " & _
        objItem.DSDnsDomainFlag
    Wscript.Echo "DS DNS Forest Flag: " & _
        objItem.DSDnsForestFlag
    Wscript.Echo "DS Global Catalog Flag: " & _
        objItem.DSGlobalCatalogFlag
    Wscript.Echo "DS Kerberos Distribution Center Flag: " & _
        objItem.DSKerberosDistributionCenterFlag
    Wscript.Echo "DS Primary Domain Controller Flag: " & _
        objItem.DSPrimaryDomainControllerFlag
    Wscript.Echo "DS Time Service Flag: " & _
        objItem.DSTimeServiceFlag
    Wscript.Echo "DS Writable Flag: " & objItem.DSWritableFlag
    Wscript.Echo "Name: " & objItem.Name
    Wscript.Echo "Primary Owner Contact: " & _
        objItem.PrimaryOwnerContact
Next
'EOF
```