

Balance downloading Web-Proxy Client with ISA Server 2004 Standard Edition (Part 2)

We got used to balancing the Web-Proxy Client with ISA Server 2004 Standard Edition in part one of this series. Also in part one, we went into the depth of understanding proxies with automatic configuration files. For many people, this procedure significantly reduces costs

Review part I

We got used to balancing the Web-Proxy Client with ISA Server 2004 Standard Edition in part one of this series. Also in part one, we went into the depth of understanding proxies with automatic configuration files. For many people, this procedure significantly reduces the extra costs incurred when investing the Enterprise version for businesses. In Part 2, we will continue to explore some of the extensive load balancing capabilities.

Introduce

In part one we exported the "wpad.dat" file with a server of the ISA Server Standard Edition server pair and slightly modified some of the lines in the file. Start as follows:

```
cNodes = 1;
function MakeProxies () {
this [0] = new Node ("10.245.10.254", 0.1.000000);
}
?ã thay ??i thành thành:
cNodes = 2;
function MakeProxies () {
this [0] = new Node ("10.245.10.253", 2032180928,1.000000);
this [1] = new Node ("10.245.10.254", 2843172549,1.000000);
}
```

By creating an aggregate file through a website to browsers like Internet Explorer, this change allows some procedures to be hidden inside the file. As a result, two servers running Server Standard Edition become load balancing and error tolerant for Web proxy services.

However, this simple operation also means that the configuration made for ISA Server is not applied to our orphaned file: some "more manual" edits will have to be done so that it becomes appropriate. and useful.

In part one, you are also shown how to configure Internet Explorer "manually" to select a new configuration file. This is not a practical solution for most of us. We should first use the Internet Explorer Maintenance add-on

component in Group Policy.

Group Policy and Internet Explorer Maintenance

Before going into Group Policy, we should also mention the built-in ISA Server mechanism for managing IE in Firewall Client. There are several reasons why we ignore this mechanism. First, too many ISA Servers are just Web proxies and Firewall Client not deployed; second, we will refer to Group Policy; and third, we have seen the method of using Firewall Client in many other articles. Now, go back to the Group Policy issue.

Internet Explorer Maintenance in Group Policy is not my favorite component. It is not the same as the rest of the settings in Group Policy and some settings appear double in the 'Administrative Templates' section. Internet Explorer Maintenance does not have the same functionality as IEAK. In Group Policy, it is actually IEAK components for the client, used for settings.

In order for these components to work, we need to meet some requirements.

Configure browser automatically

First, select Group Policy to manipulate. You will not want to corrupt the Default Domain Policy, so you should have a policy with your own settings.

Open this policy, locate **Internet Explorer Maintenance** from **User Configuration** , on **Windows Settings** . Right-click it to see the drop-down menu.

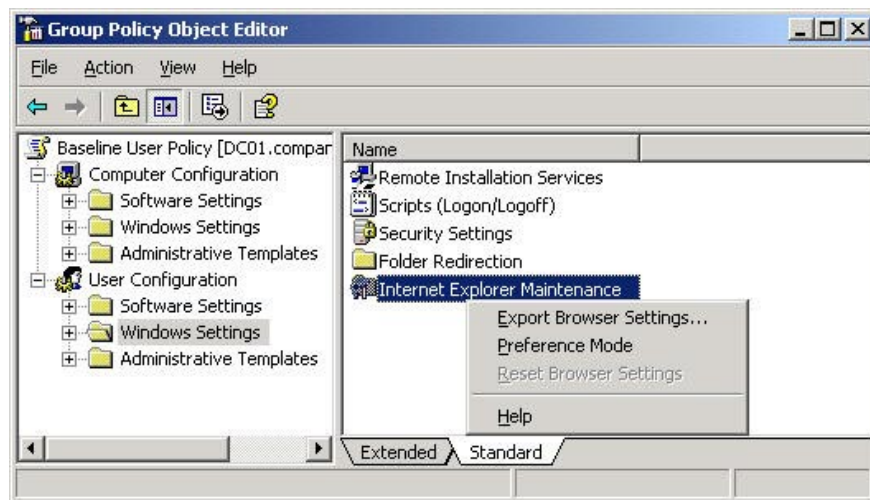


Figure 1

We need **Policy Mode** , not **Preference Mode** . So don't click on it and make sure you don't tick it again. After editing in Internet Explorer, you cannot delete these changes from Group Policy. To do that, you need the **Reset Browser Settings** option. You will see this option is grayed out because no settings have been made yet. Double click on IE Maintenance model to expand.

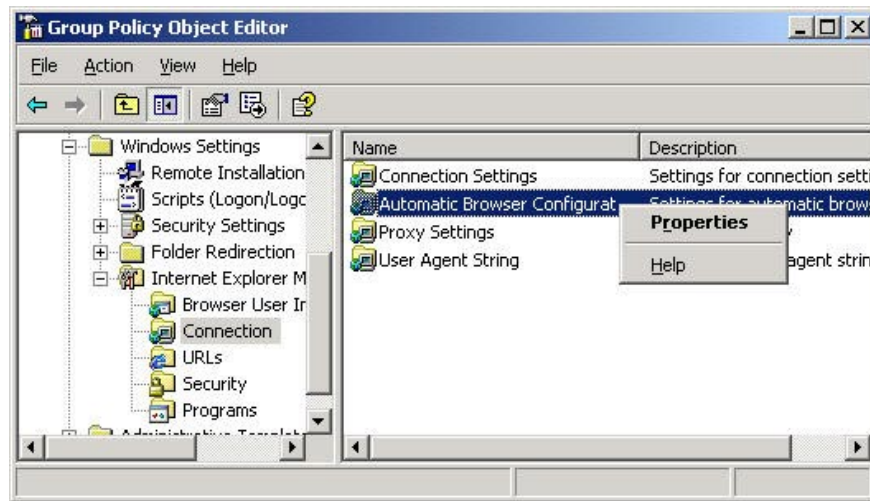


Figure 2

Under the **Connection** tab, you will see **Automatic Browser Configuration** . Right-click it and select **Properties** .

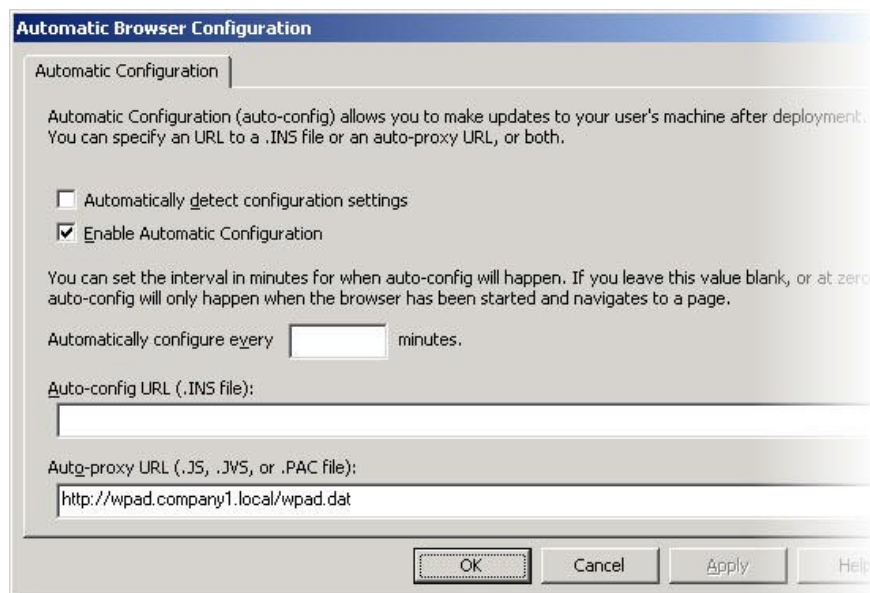


Figure 3

Check the **Enable Automatic Configuration** box and enter your **Auto-proxy URL** path. Note, the program will require JS, JVS or PAC files, but the example used here is the .DAT file. Your browser won't notice.

Click **OK** , the program is done: At least you will be forgiven when thinking that the program is being implemented. That's not how the IE Maintenance add-on component works. If you go to Internet Explorer and perform settings on the LAN (on the Tools tab, Internet Options, Connections), you will really see that Group Policy has added some new settings (if you wait for the policy to apply or run GPUPDATE.EXE), while you may still not mark the setting. That's what you don't want users to encounter.

Things get worse: you don't check the settings. Now wait for Group Policy to apply again (or go to GPUPDATE), but setting it back up is useless. IE Maintenance will not reuse the setting unless something in the policy is changed. This activity can be very messy. Microsoft obviously has something else in the 'Policy Mode' model.

Policy enforcement

In order for the policy settings to be properly applied, we take a closer look at the 'User Configuration' settings of Group Policy in **Windows Components** , at **Administrative Templates** .



Figure 4

Under **Internet Explorer** , you will see that there are two settings: **Disable changing proxy settings** (do not use **changing proxy settings**) and **Disable changing Automatic Configuration settings** (do not use **change configuration settings**). Mark the check box to allow both of these options to work (or at least let them work later).

You can go to **Internet Control Panel** , allow the option to **Disable the Connections page** (do not use the connection page) to make the entire tab disappear. This setting is also set in 'Computer Configuration' with priority.

But after the changes are working, your settings are still not safe when someone else's intervention, like the registry editor. And remember that your policy will not be applied again until it is changed.

Really enforce policy!

To do this, you first need to change the 'Computer Configuration' settings of Group Policy. Go to **Administrative Templates** , **System and Group Policy** to find **Internet Explorer Maintenance policy processing** .

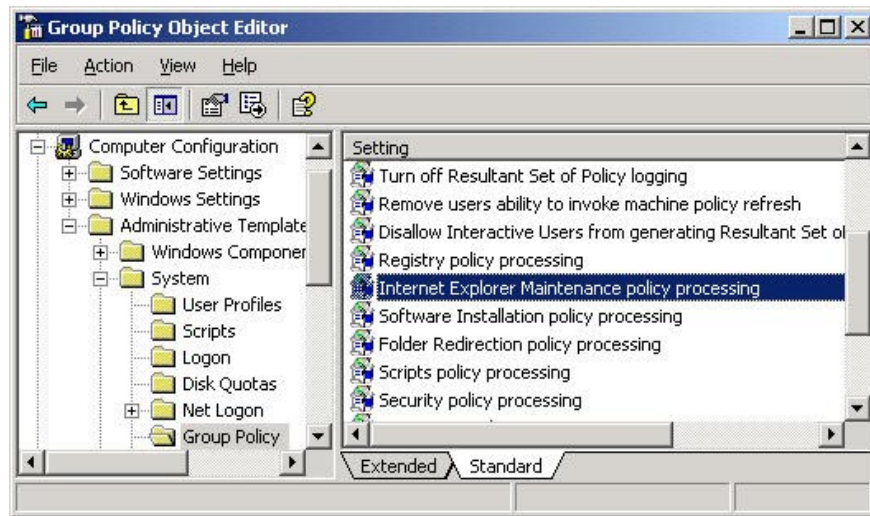


Figure 5

Double click to open it.

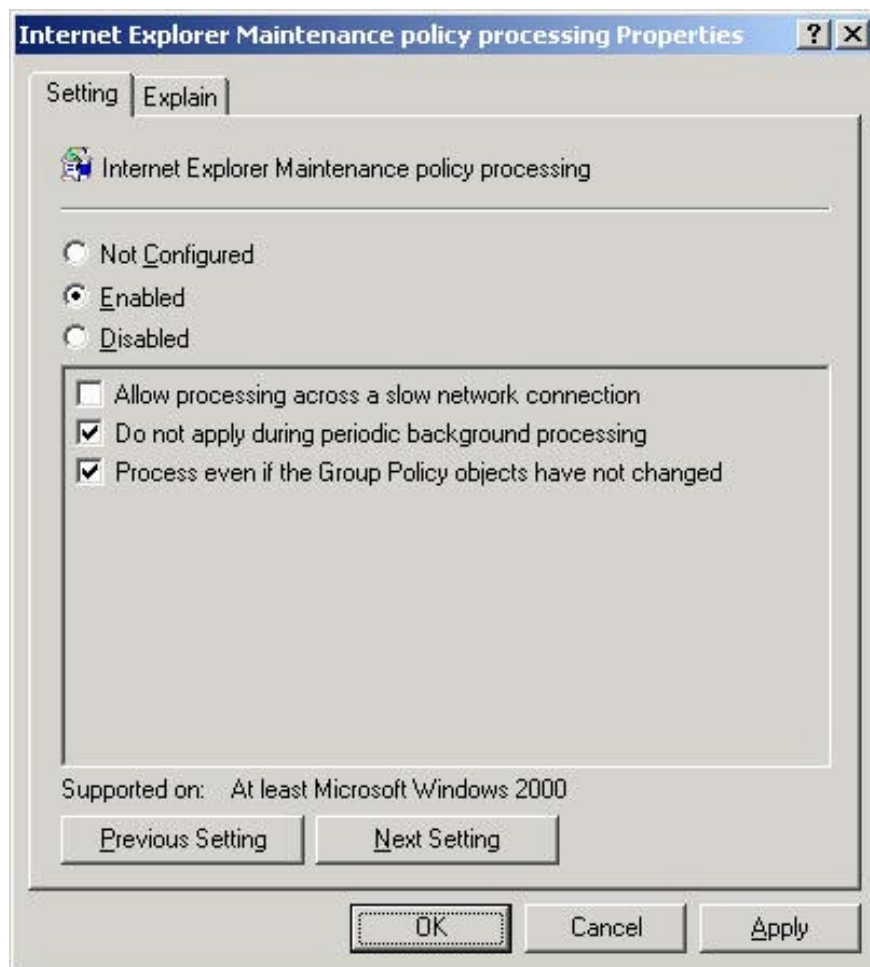


Figure 6

At least you need to select **Process even if the Group Policy objects have not changed** or **Do not apply during periodic background processing** .

The reason why this activity does not become the default: if you use IE Maintenance for some types of extensions, you just want the changes to appear once, or worse, every 90 minutes with the rest of the Group Policy. So think carefully about how to use IE Maintenance before proceeding to the next step.

Optional Automatically detect settings

Notice that you will find the **Automatically detect settings** option along with the **Automatic automatic configuration script** (using automatic bridge scripting) is used throughout this article. You can use them alternately if you want, but there are some dangers in doing so.

If you have already shown the instructions in Part 1, you should have created a website with the same name "wpad.company1.tld" used in this example. The important point is that the website is called "WPAD" corresponding to port 80, and the file is called "wpad.dat" (as mentioned in part 1). Once there, select **Automatically detect settings** , everything will be done; Your browser will start searching **http://wpad/wpad.dat** .

Another way to use **Automatically detect settings** is to have an entry point in DHCP. This entry in "Option 252" is of a format like **http://wpad.company1.tld: 80 / wpad.dat** . The point here is that you can call the file (and lead to it) whenever you like and use any TCP port for the website you want. But there are also some limitations:

The browser will create DHCP requests for this value. But before Windows XP SP2 and 2003 SP1, only the administrator was allowed to do so, and the clients (clients) did not.

And, if your browser is allowed to locate DHCP entries; Did I successfully download the script? Perhaps Microsoft needs a point or two to fix the hotfix here.

To get a deeper understanding of the **Automatically detect** settings option, you should consult Stefaan Pouseele's next article (with links to updates and hotfixes).

For now, you should absolutely use the **Use automatic configuration script option** .

Exception

ISA Server does a good job of bringing back Web content from extended networks. But the last thing that most of us want is that the browser sends requests to the proxy for the site on the internal Intranet server. Then the browser will go directly to the website.

ISA Server allows you to configure these "exceptions" and rights of some entry points, placing them in the automatic configuration file (PAC) it creates. That is also the file we have reviewed. When downloading the "wpad.dat" file, you will see some exceptions. In the following example you will see in the first line of the PAC file, these exceptions have not been configured:

```
// Copyright (c) 1997-2004 Microsoft Corporation
BackupRoute = "DIRECT";
UseDirectForLocal = true;
function MakeIPs () {
}
DirectIPs = new MakeIPs ();
cDirectIPs = 0;
function MakeNames () {
}
DirectNames = new MakeNames ();
cDirectNames = 0;
```

Our PAC files are now "orphaned" from ISA Server and must be edited "manually". Exceptions can be provided with only a few edit lines.

BackupRoute

This is not really an exception, just "what to do if it all fails". If the firewall (or possibly ISA Server) still allows direct access to the Internet to search Web content or to quickly reconfigure when an emergency occurs, "DIRECT" is the best option here. .

You can choose other Web proxy configurations that can be loaded in an emergency. Its format is as follows:

```
BackupRoute = 'PROXY W3PROXY.COMPANY1.LOCAL: 8080';
```

Of course you need to change the name here with your own name (or IP address) along with the port used. Because the point of the article is to pair ISA Servers to provide "fault-tolerance", we hope this backup routing will never be needed.

UseDirectForLocal

Surely you want to use this option and it may be all the "exceptions" you need. This means that any URL with a fully qualified name, or host name, without dots will go directly to the destination address, not through ISA Server, for example:

http://www.isaserver.org/pages/newsletters.asp goes through ISA server, but **http://myserver/intranet/index.html** will come directly.

DirectIPs

If you use an IP address to point to an Intranet, or have links in Intranet pages that refer to an IP address, you'll probably want to have a little tweaking here. For example, it could be:

```
function MakeIPs () {
this [0] = "172.16.0.0";
this [1] = "255.240.0.0";
}
```

```
DirectIPs = new MakeIPs ();  
cDirectIPs = 2;
```

An important point to note is that entry points come in pairs: a subnet and a mask (subnet and mask). The value of "cDirectIPs" reflects both entry points. Here is 2, which means that this adjustment provides only one subnet. You can add more pairs, just keep the numbers of the "this [n]" lines and the value "cDirectIPs".

This is a pretty bad piece of code, but you won't have to edit it much later and don't need to tweak or clean the code to make it easier to read.

DirectNames

This option works similarly to "DirectIP". Here, you will list all host names that you do not want to go through ISA Server.

```
function MakeNames () {  
this [0] = "intranet.company1.com ";  
this [1] = '*. local';  
this [2] = '*. develservers.tld';  
}  
DirectNames = new MakeNames ();  
cDirectNames = 3;
```

Note that you can describe wildcards for an entire domain, but only use the wildcard at the beginning of the name. For example 'www.company1. *' Will not work.

CARP exceptions

Because the browser uses PAC files for all URL requests, it will use more than one proxy for different sites on the same website. Some websites will get confused when they get requests from the same client, but on two different IP addresses.

This is not a problem if your ISA Server is behind a "NATing" device, but will become a serious problem if the ISA Server Web-proxy is also the firewall with IP interface. general.

To avoid problems with these websites, the browser must order all requests to specific hosts through the same proxy. In ISA Server Enterprise Edition, it is described as "CARP exceptions". PAC files will also have the same impact, requiring additional code.

The first step is to add some lines near the top of the file with the value "cDirectNames":

```
cDirectNames = 0;  
function MakeCARPEXceptions () {  
}  
CARPEXceptions = new MakeCARPEXceptions ();  
cCARPEXceptions = 0;
```

The next step is to replace the FindProxyForURL function with the following lines (changes are red):

```
FindProxyForURL function (url, host) {
var urlhash, urllower, ibest, bestscore, list, i, j, port = HttpPort , hostonly = false ;
urllower = url.toLowerCase ();
if ((urllower.substring (0.5) == "rtsp:") ||
(urllower.substring (0.6) == "rtspt:") ||
(urllower.substring (0.6) == "rtspu:") ||
(urllower.substring (0.4) == "mms:") ||
(urllower.substring (0.5) == "mmst:") ||
(urllower.substring (0.5) == "mmsu:"))
return "DIRECT";
if (UseDirectForLocal && isPlainHostName (host))
return "DIRECT";
if (cDirectNames> 0)
for (i = 0; i
if (shExpMatch (host, DirectNames [i]))
return "DIRECT";
if (cDirectIPs> 0)
for (i = 0; i
if (isInNet (host, DirectIPs [i], DirectIPs [i + 1]))
return "DIRECT";
    if (cCARPEExceptions> 0)
        for (i = 0; i
            if (shExpMatch (host, CARPEExceptions [i])) {
                hostonly = true;
                break;
            }
urlhash = HashString (url , hostonly );
for (i = 0; i
Proxies [i] .score = Proxies [i] .load * Scramble (MakeInt (urlhash ^ Proxies [i] .hash));
list = "";
for (j = 0; j
for (bestscore = -1, i = 0; i
if (Proxies [i] .score> bestscore) {
bestscore = Proxies [i] .score;
ibest = i;
}
}
Proxies [ibest] .score = -1;
list = list + "PROXY" + Proxies [ibest] .name + ":" + port + ",";
}
list = list + BackupRoute;
return list;
}
```

Finally, replace the entire function:

```

HashString function (url , hostonly ) {
var h = 0;
var slashes = 0;
for (var i = 0; i
var c = url.charAt (i);
if (c == '/')
slashes ++;
if (slashes 3) {
c = c.toLowerCase ();
    } else if (hostonly) {
        i = url.length;
    }
h += (((h & 0x1fff) 19) | ((h >> 13) & 0x7fff)) + CharToAscii (c);
h = MakeInt (h);
}
return h;
}

```

Activate the code in a similar way to "MakeNames", but give a list of all host names you want to go through the same ISA Server:

```

function MakeCARPEExceptions () {
this [0] = "crabby.website.tld";
this [1] = "gripping.tld";
}
CARPEExceptions = new MakeCARPEExceptions ();
cCARPEExceptions = 2;

```

These changes are made to the PAC file procedures in ISA Server Enterprise Edition. It has the same function but not the source code. The first reason is the copyright issue, and the second is not to include too many additional lines in the Enterprise Edition version.

Variations (only for those who want to test)

There are other options for the above CARP exception changes: just replace HashString with:

```

function HashString (url) {
var h = 0;
var slashes = 0;
for (var i = 0; (i 3) ; i ++ ) {
var c = url.charAt (i);
if (c == '/')
slashes ++;
h += (((h & 0x1fff) 19) | ((h >> 13) & 0x7fff)) + CharToAscii (c);
h = MakeInt (h);
}
}

```

```
return h;  
}
```

Change the line calling this function in FindProxyForURL to:

```
urlhash = HashString ( lower url);
```

In this case, all requests for a Web page on a specific hostname will go through the same proxy (for example, all requests are "CARP Exceptions"). We do not know how the effect of this method on load-balancing, but you can try to save the browser some process.

There are a number of ways to handle PAC file ISA Server, but in the framework of this article we cannot fully introduce it.

What is Client-side CARP?

It's a bit uncomfortable here with the term "client-side CARP". The "P" stands for "Protocol". So when you create the Proxy Automatic Configuration file, does this become a protocol? So far, this is still an accepted term. Hope you won't be confused.

Conclude

ISA Server 2004 Enterprise Edition is usually the choice for load-balancing Web proxies using ISA Server. But this article also shows that, if you accept some of the unimportant inconveniences of PAC files on ISA Server, the performance of load balancing and error tolerance (load-balancing and fault-tolerance) on ISA 2004 Standard Edition is undeniable.

You finished reading the article "**Balance downloading Web-Proxy Client with ISA Server 2004 Standard Edition (Part 2)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.