

Google No SSL Search DNS Modifications

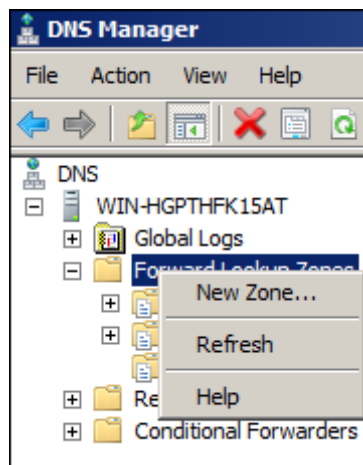
When students search using <https://encrypted.google.com>, NetSpective will not be able to see their searches or Google's response. NetSpective does not decrypt HTTPS traffic and will not be able to see inside the SSL tunnel. However, you can block <https://encrypted.google.com> using a workaround provided by Google.

There are several steps we will need to take in order to transparently direct users to the non-encrypted Google search. First we will need to create a new DNS zone on the domain controller. Then, we will need to create and schedule a PowerShell script to automatically update the IPs in the new DNS zone in the event that Google changes the IP address of their search engine.

Note: These steps are based on Windows Server 2008 R2 and Active Directory at a 2008 R2 functional level.

Creating a new DNS Zone

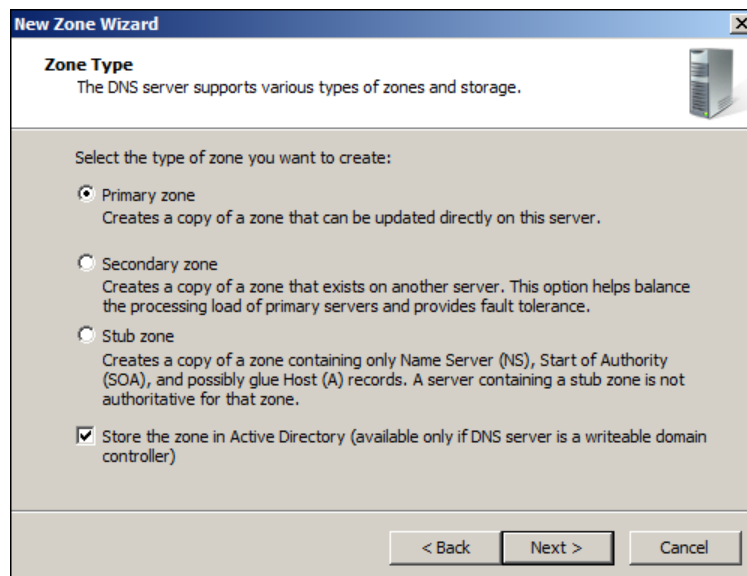
1. Go to Start > Administrative Tools > DNS
2. Expand the DNS Server and the Forward Lookup Zones.
3. Right Click on Forward Lookup Zones and Choose New Zone.



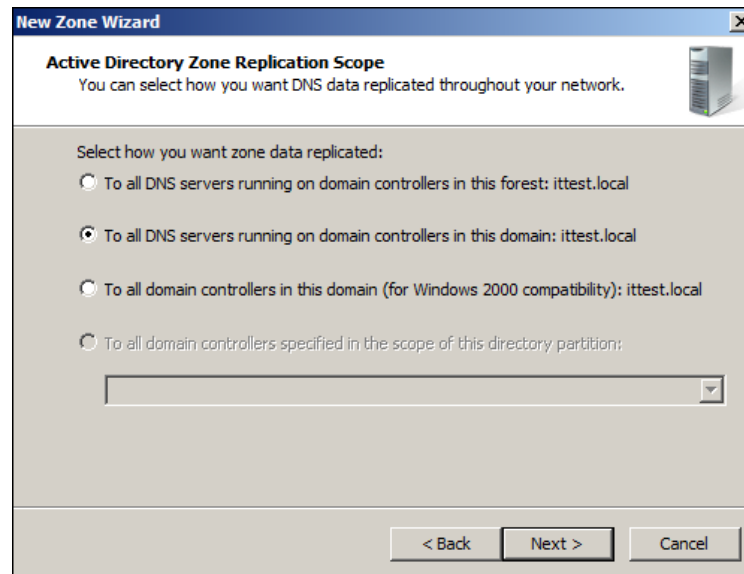
4. This will open the New Zone Wizard. Click Next.



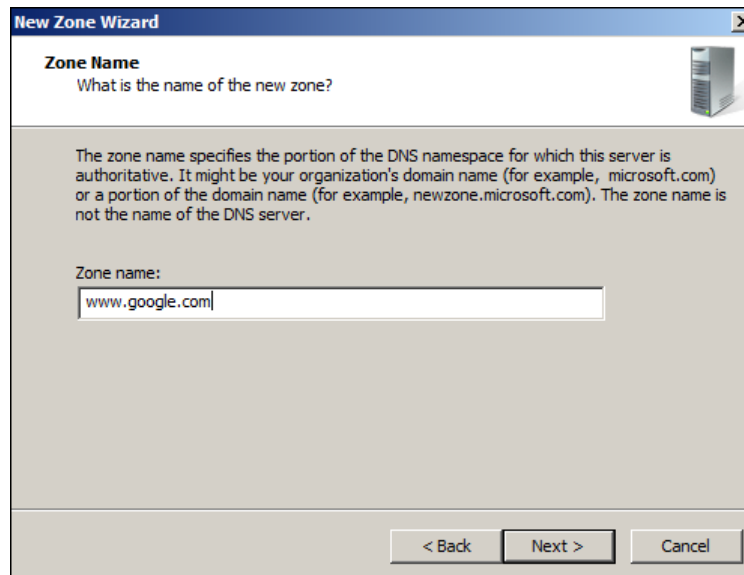
5. Select Primary zone and then click Next.



6. Select how you want to replicate the new zone to other DNS servers in the domain or domain forest and then click Next.



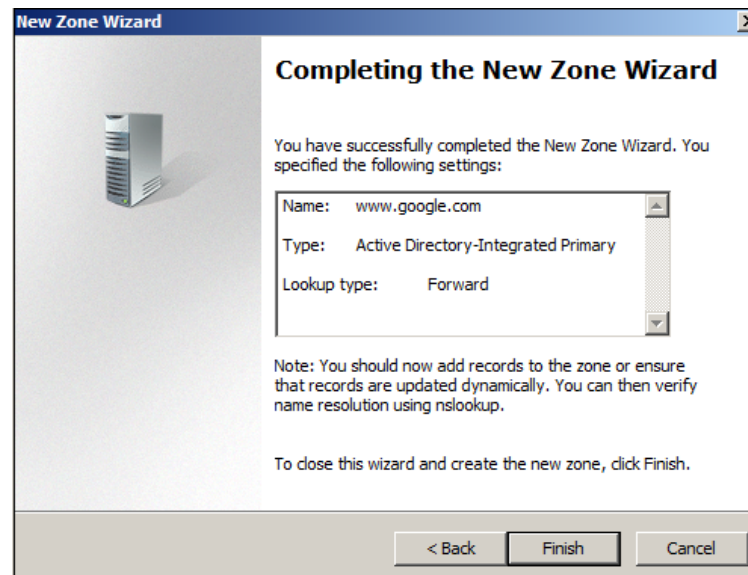
7. Enter www.google.com for the Zone Name and then click next.



8. Select what types of updates you would like to allow in the new zone and then click Next.



9. Click Finish to create the new DNS zone.



10. Open a command prompt and do type “nslookup nossl.google.com” without the quotes and make note of the IP Address or addresses that are returned.

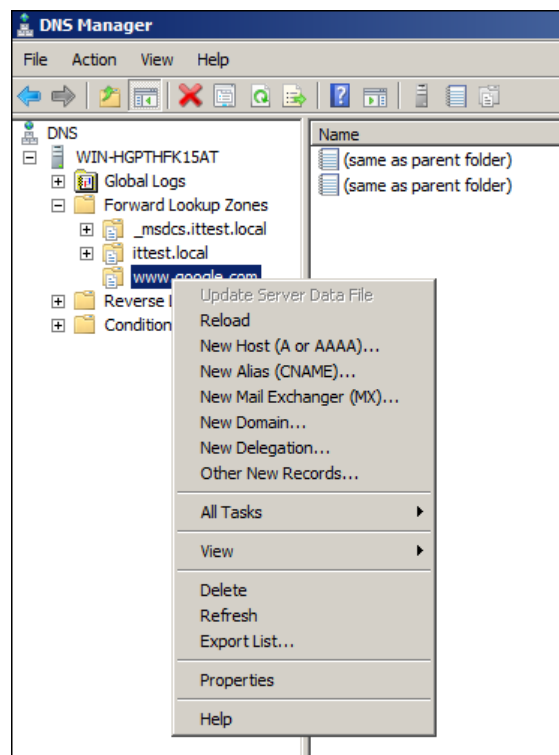
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup nossl.google.com
Server:    Unknown
Address:    ::1

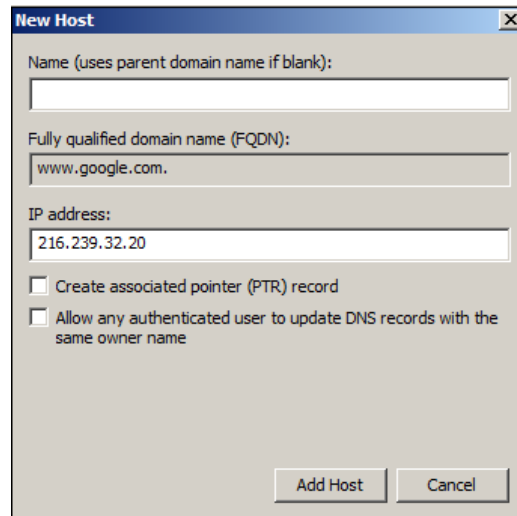
Non-authoritative answer:
Name:      nossl.google.com
Address:    216.239.32.20

C:\Users\Administrator>_
```

11. In DNS Manager right click on the www.google.com zone and select “New Host (A or AAAA)...”



12. In the New Host window, leave the Name field blank and enter the IP address from the previous nslookup (Step 10) in the IP Address field. Finally click Add Host.



New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

☐ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

Creating and Scheduling a PowerShell Script to update the DNS zone

1. Go to Start -> All Programs -> Accessories -> Notepad

2. Enter the following into Notepad

```
# Environment Setup
$DNSServer = "."
$DNSZone = "www.google.com"

# DNS lookup
$result = Invoke-Expression "nslookup nossl.google.com 8.8.8.8"
if($result[4] -match "Address(es)?: *(.*)") {
    dnscmd . /RecordDelete $DNSZone "@" A /f
    dnscmd . /RecordDelete $DNSZone "@" AAAA /f
    $address = $matches[2]
    $extra = $matches[1] -eq $null
    $next = 5
    While ($address -ne $null -and $address.length -gt 0) {
        $type = "A"
        if($address -match ":") {$type = "AAAA"}
        dnscmd . /RecordAdd $DNSZone "@" $type $address.Trim()
        $address = $result[$next]
        $next = $next + 1
    }
}
```

3. Save the file with a .ps1 file extension

PowerShell's default execution policy does not allow the running of scripts. Perform the following steps to change the execution policy to allow running locally created scripts and remote signed scripts.

- a. Open PowerShell
- b. Type:

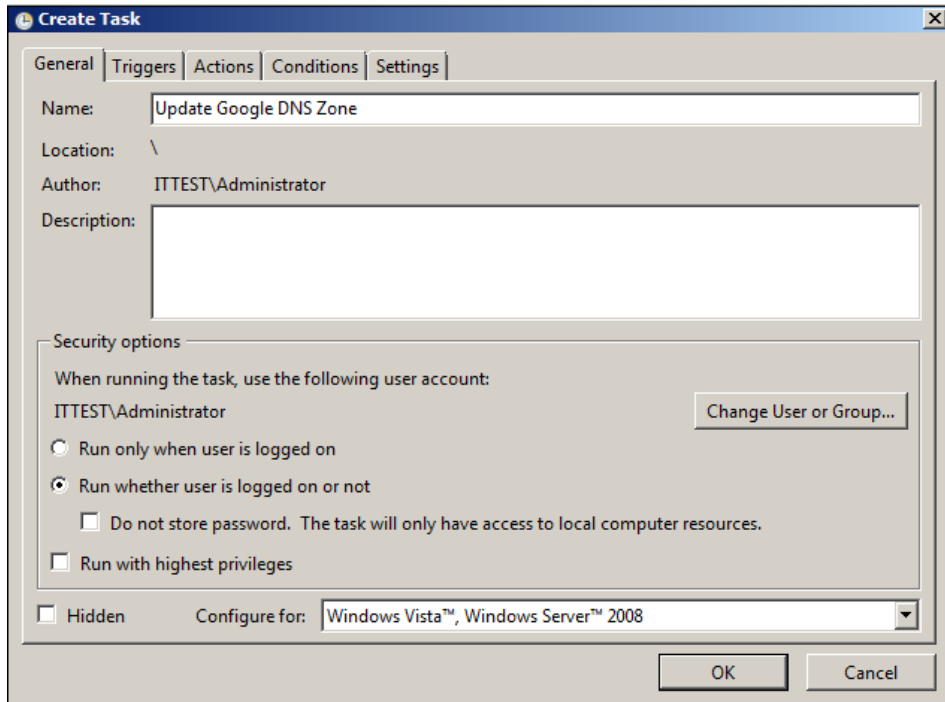
```
Set-ExecutionPolicy RemoteSigned
```

- c. Then press enter. Next answer Yes (Y)

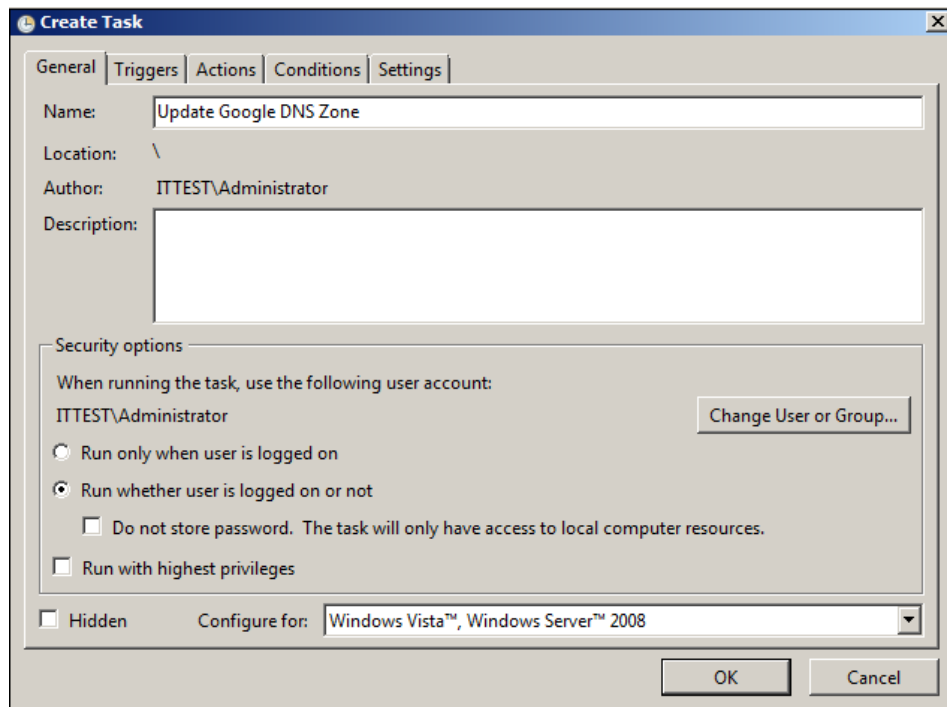
4. Finally we need to create a scheduled task to run the PowerShell script on a periodic basis to make sure we have up to date IP Address(es) for nossl.google.com

- a. Go to Start -> Administrative Tools -> Task Scheduler
- b. In the Actions panel click Create Task

- c. On the General Tab, enter a Name for the task. Change the user account used to a domain admin account or other account that has the right to update DNS entries. Change the radio button to the “Run whether user is logged on or not” option.

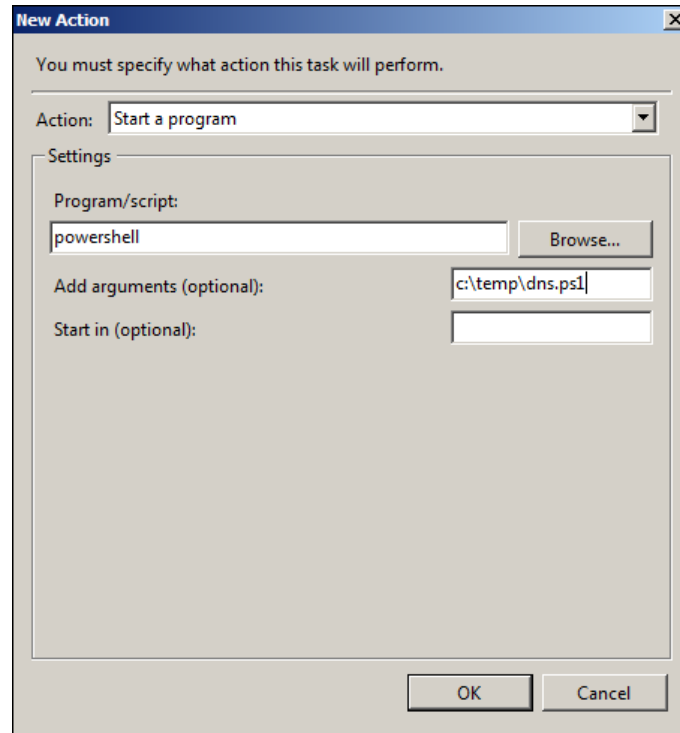


- d. On the Triggers tab, click the New button
- e. Select the “Repeat task every” option and select the how often you would like to run the task from the drop down and change the “for a duration of” drop down to Indefinitely. Finally click OK



- f. On the Actions tab, click the New button.

- g. On the New Action window select “Start a program” from the Action drop down. Then in the Program/script field, enter “powershell” without quotes, in the Add arguments field enter the script you created in Step 3 including the full path to it. Then click OK.



- h. On the Create Task window Click OK

Now when students search using <http://www.google.com> , NetSpective will continue to filter objectionable content without the student accessing Google securely. You will still be able to log into your Google account and use “Google Apps for Education”, as well as other authenticated Google services. These services are currently hosted at <https://www.google.com> and will not be affected. As long as you allow access to <https://www.google.com> , your organization should still be able to access all of Google’s other services.