<u>Home</u> > <u>Network and technology service docs</u> > <u>Janet CSIRT</u> > <u>Technical advice</u> > How to block or sinkhole domains in Windows Server 2008

How to block or sinkhole domains in Windows Server 2008

How to block or sinkhole domains on Windows server 2008 DNS.

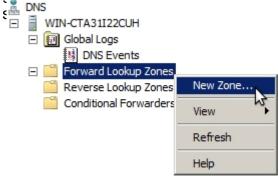
There may come a time when you may require to sinkhole or block a large number of domains.

One of the easiest way of doing this is within your BIND DNS infrastructure by making your DNS Resolvers authoritative for the domains that you wish to block.

However if you do not have a BIND DNS server then this guide will allow you to sinkhole domains within a windows server 2008 environment.

Microsoft's implementation of DNS is heavily centered around a GUI interface and is not natively designed to work with text files for mass import of domains, however there are some tweaks that we can make in order to do so.

The first thing that we can do is create the default zone that all of our blocked domains are going to use. Within the MS DNS Manager utility right click Forward Lookup Zones and the DNS



When confronted with the New Zone Wizard select Next ? Select Primary zone ? Next

ew Zone Wizard		×
Zone Name What is the name of the new zone?		
The zone name specifies the portion of the authoritative. It might be your organization or a portion of the domain name (for exam not the name of the DNS server.	n's domain name (for example, microsoft	
Zone name:		
blocked_domains		
	< Back Next > Ca	ancel
		ancer

Now enter the name that you want to give this zone. And then accept the default filename of the specified Zone name.dns in this example it is blocked_domains.dns.

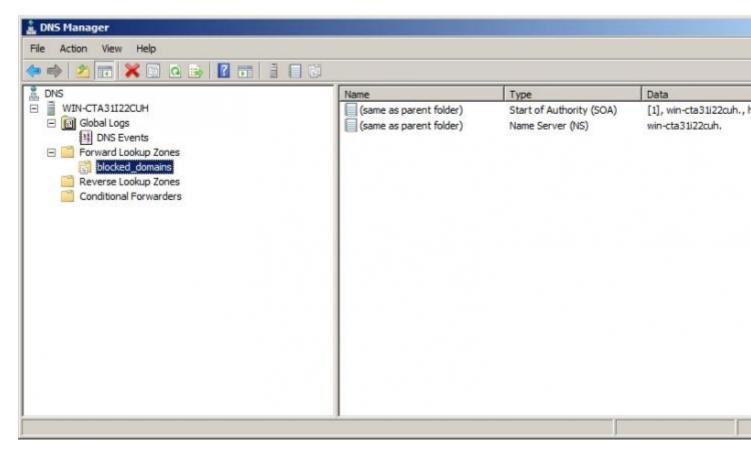
The next page in the wizard talks about dynamic updates.

New Zone Wizard
Dynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
 Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.
 Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be accepted from untrusted sources.
O not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back Next > Cancel

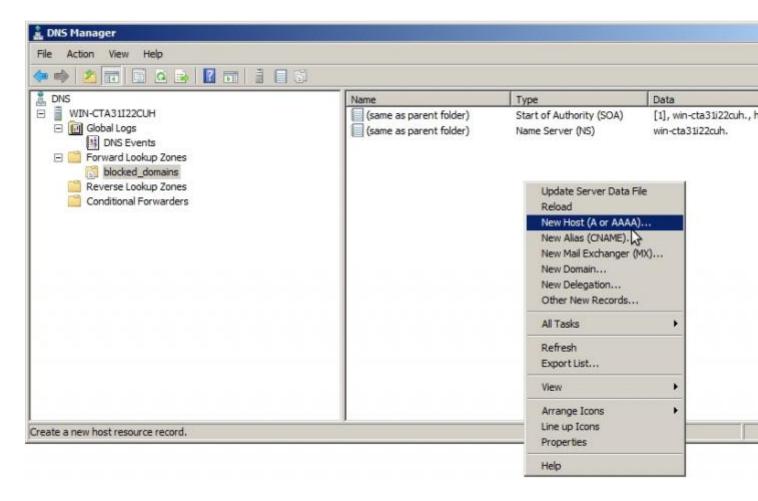
We do not want these being updated dynamically from clients in this case we use **Do not allow dynamic updates**, now just finish through the wizard.

You will now see the newly created zone of blocked_domains listed in your Forward Lookup

Zones within the MS DNS Manager utility along with some initial configuration for the zone.



We now need to add the appropriate entries to this zone for the blacklisting of the domain and sub-domains of the blacklisted domain. As such we now add the wildcard A and AAAA records. Right click in the right pane under the blocked_domains container and select " *New Host (A or AAAA)...*"



Now fill out the required information that is needed, in the example below we created both A and AAAA records. The A records are pointing to a sinkhole and the AAAA are pointing to local host.

DNS WIN-CTA31122CUH Global Logs DNS Events Forward Lookup Zones Slocked_domains Reverse Lookup Zones Conditional Forwarders	Name (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) * (same as parent folder) *	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) IPv6 Host (AAAA) IPv6 Host (AAAA)	Data [1], win-cta31i22cuh., hostmaster. win-cta31i22cuh. 192.168.56.200 192.168.56.200 0000:0000:0000:0000:0000:0000:000 0000:0000:0000:0000:0000:0000:000	

Now that this has now been defined we can now specify that the DNS server loads its zone data from a file rather than from the registry on first load, this will enable us to operate bulk updates.

We now need to right click the DNS server and then select Properties and select the

Advanced tab on the DNS server Properties Window.

DNS UNI-CTA3- Condition DN UNI-CTA3- Condition DN UNI-CTA3- Condition DN UNI-CTA3- Condition DN	Configure a DNS Server New Zone Set Aging/Scavenging for All Zones Scavenge Stale Resource Records Update Server Data Files Clear Cache Launch nslookup
	All Tasks
	Delete Refresh
)pens the propertie	Properties
	Help

We now choose to Load zone data on startup: from file and then select apply.

WIN-CTA31122CUH	Properties			<u>?</u> ×	
Debug Logging Interfaces	Event Logging Forwarders	Trust Adva	Anchors	Monitoring Root Hints	
Server version nu 6.1 7601 (0x1db					
■BIND secondar Fail on load if b Enable round ro Enable netmas	Server options: Disable recursion (also disables forwarders) BIND secondaries Fail on load if bad zone data Penable round robin Enable netmask ordering Secure cache against pollution				
Name checking:	Name checking: Multibyte (UTF8)				
Load zone data on startup: From registry					
Enable automatic scavenging Scavenging period; From registry From file From Active Directory a registry days					
			Reset	to Default	
(DK Can	cel	Apply	Help	

Now if we check in %SystemRoot%\System32\DNS (normally C:\Windows\System32\dns) we will see a few files blocked_domains.dns and boot.

Blocked_domains.dns contains the configuration for the zone we recently configured, and as you can see looks very similar to a BIND zone file if you are familiar with them.

; Database file blocked_domains.dns for blocked_domains zone. Zone version: 5 ; ; IN SOA win-cta31i22cuh. hostmaster. (@ 5 ; serial number 900 ; refresh 600 ; retry 86400 ; expire 3600) ; default TTL ; ; Zone NS records ï NS win-cta31i22cuh. @ ï ; Zone records ï A 192.168.56.200 @ AAAA ::1 @ * A 192.168.56.200 AAAA ::1

The other file, boot is used to define the separate zones or domains. Here we can specify what domains we want to block, by stating the domain type, the domain and the appropriate zone file.

```
;
; Boot information written back by DNS server.
;
cache . cache.dns
primary blocked_domains blocked_domains.dns
```

Once we have added a few domains that we wish to block the boot file will look as follows.

```
ï
   Boot information written back by DNS server.
;
;
                                       cache.dns
cache
             blocked domains
primary
                                       blocked domains.dns
             blockeddomain.com
                                       blocked_domains.dns
primary
                                       blocked_domains.dns
             buymalwarehere.ru
primary
             s23a93884skf.net
                                       blocked_domains.dns
primary
             almost-somedodgeybank.com blocked_domains.dns
primary
primary
             google.co.uk
                                       blocked_domains.dns
```

You can now save the the file. However as the file is only read on the startup of the DNS service you will need to **restart the DNS Server service** within the server manager. Once this

has been restarted the added domains will now be within the MS DNS manager as shown below.

Image: Second state Image: Second state	BNS Manager File Action View Help			_ 🗆 ×
	 DNS WIN-CTA31I22CUH Global Logs Forward Lookup Zones almost-somedodgeybank.com blocked_domains blockeddomain.com 	Name almost-somedodgeybank.com blocked_domains blockeddomain.com buymalwarehere.ru google.co.uk	Standard Pri Standard Pri Standard Pri Standard Pri Standard Pri	Running Running Running Running Running

From the queries below the DNS server is now acting as primary for these domains meaning that any queries it receives for these domains instead of looking them up it will respond with it's configuration.

```
😣 🖨 🗊 : ~
:~$ dig @192.168.56.101 almost-somedodgeybank.com
; <<>> DiG 9.8.1-P1 <<>> @192.168.56.101 almost-somedodgeybank.com
; (1 server found)
;; global options: +cmd
; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 907
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;almost-somedodgeybank.com.
                               IN
                                       А
;; ANSWER SECTION:
almost-somedodgeybank.com. 3600 IN
                                       A
                                              192.168.56.200
;; Query time: 5 msec
;; SERVER: 192.168.56.101#53(192.168.56.101)
; WHEN: Tue May 27 12:34:02 2014
  MSG SIZE rcvd: 59
```

```
>= 🗈 : ~
:~$ dig AAAA @192.168.56.101 almost-somedodgeybank.com
 <<>> DiG 9.8.1-P1 <<>> AAAA @192.168.56.101 almost-somedodgeybank.com
 (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37125
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;almost-somedodgeybank.com.
                                        AAAA
                                IN
;; ANSWER SECTION:
almost-somedodgeybank.com. 3600 IN
                                        AAAA
                                                 ::1
;; Query time: 0 msec
; SERVER: 192.168.56.101#53(192.168.56.101)
;; WHEN: Tue May 27 12:38:28 2014
; MSG SIZE rcvd: 71
```

Caveats to blocking domains

There are some easy ways that clients may be able to mitigate these DNS configurations. By modifying their hosts file on their systems to point at the correct IP addresses for the domains or by using a public resolver however both of these methods will require local administrator access.

You should only do this on your internal resolvers, if you take these actions on your public facing authoritative servers then you will be responding to domains which are not your responsibility.

Taking these actions on domains which are secured with DNSSEC will also break the security on them. If validation is turned on then the resolution will fail and the sinkhole will not get contacted.

This guide has been conducted on a system that is not running active directory DNS and there could be some issues experienced within such an environment.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/how-block-or-sinkhole-domains-windows-server-2008