**--- CHANGE DETAILS ---**

All of the COMPANY domains have been migrated into the COMPANY domain and all COMPANY DNS zones that are still active are hosted on the COMPANY domain controllers.

To remove old records DNS scavenging needs to be enabled on only XX01ADC1a.   
Static records will need to be cleaned up manually.

**--- IMPLEMENTATION DATE ---**

**--- IMPLEMENTATION STEPS ---**

Scavenging is set in three places on a Windows Server:

* On the individual resource record to be scavenged
* On a zone to be scavenged
* At one or more servers performing scavenging

It must be set in all three places or nothing happens

**---1---**

To enable scavenging for all zones in the COMPANY domain we need to:

* Take a full backup of all zones using DPM
* Take a manual export of all zones for reference (from a 2008 or earlier DC)
* Browse to C:\Windows\System32\dns
* Create a folder called export
* Open a command prompt
* Browse to C:\Temp
* Run the following commands:
* dnscmd /enumzones > AllZones.txt
* for /f %a in (AllZones.txt) do dnscmd /ZoneExport %a export\%a.txt

**---2---**

* Turn off scavenging on all SERVERS (currently enabled on DC1 and DC2)

<http://blogs.msdn.com/b/muaddib/archive/2013/08/03/how-to-determine-which-dns-server-s-have-scavenging-enabled.aspx>

**---3---**

* Ensure secure dynamic updates are allowed on all zones  
  “dnscmd <ServerName> /Config {..AllZones} /AllowUpdate 2”

\*Dynamic updates are not currently enabled on the following zones and will need to be enabled:

\*NB: Secure dynamic update is supported only for AD DS-integrated zones. For the following zones, dynamic updates cannot be enabled

zonename IsDsIntegrated

-------- --------------

0.in-addr.arpa False

127.in-addr.arpa False

255.in-addr.arpa False

**---4---**

* Turn on scavenging on all ZONES   
  “Get-dnsserver”  
    
  NB: All zones have scavenging enabled, see output at  
   \dnssettings.txt

**---5---**

* Wait 2 weeks, confirm that records are updating and that replication is working properly
* Confirm that ipconfig /register DNS is working
* Look at the stale records and check that they are healthy/ don’t have permissions issues
* Any stale records that aren’t fixed up will be deleted in step 6  
    
  $ServerName = "XX01ADC1a.catholic.net.au"

$ContainerName = "catholic.net.au"

Get-WmiObject -Computer $ServerName -Namespace "root\MicrosoftDNS" -Class "MicrosoftDNS\_Zone" `

# -Filter "ContainerName='$ContainerName'" |

Select-Object NoRefreshInterval, RefreshInterval,

@{n='AvailForScavengeTime';e={ (Get  
Date("01/01/1601")).AddHours($\_.AvailForScavengeTime) }}

**---6---**

* Enable scavenging on XX01ADC1a only

**--- TEST PLAN ---**

* Ceate a new test record and enable it for scavenging.
* Map out the point in time when this record will disappear:
  + Start with the timestamp on the record
  + Add the refresh interval
  + Add the no refresh interval
  + The result will be your "eligible to scavenge" time. The record will not disappear at this time though. It's just eligible.
  + Check your DNS event logs for 2501 and 2502 events to find what hour the DNS server is doing a scavenging run.
  + Take your "eligible to scavenge" time, find the most recent 2501/2502 event and add the server's Scavenging Period (from server properties | advanced tab) to it. This is the point in time when the test record you just created will disappear.

Look up COMPANY.net.au records and ensure they can be resolved

Test mail flow for COMPANY.net.au addresses

Test Lync for COMPANY.net.au users

Test Lync edge access for COMPANY.net.au users

Look up catholic.net.au records and ensure they can be resolved

Test mail flow for catholic.net.au addresses

Test Lync for catholic.net.au users

Test Lync edge access for catholic.net.au users

Check DC event logs for errors

**--- ROLLBACK PLAN ---**

If there are a small number of erroneous deletions refer to DNS Zone Backup" and re-create them

If there are a large number of erroneous deletions, turn of scavenging and restore the zone from a backup

**--- COMMUNICATION ---**

Email the ICT team with details and possible issues

**--- RISK ---**

High- changes to DNS may cause outages to all services including email, domain authentication, RDS and Lync.

Objects with static records are the most vulnerable to erroneous deletion.

**--- REF ---**

Don't be afraid of DNS Scavenging: <http://blogs.technet.com/b/networking/archive/2008/03/19/don-t-be-afraid-of-dns-scavenging-just-be-patient.aspx>

Understanding Aging and Scavenging:   
<http://technet.microsoft.com/en-us/library/cc771677%28v=WS.10%29.aspx>

how-to-determine-which-dns-server-s-have-scavenging-enabled:   
<http://blogs.msdn.com/b/muaddib/archive/2013/08/03/how-to-determine-which-dns-server-s-have-scavenging-enabled.aspx>

Microsoft DNS & stale records: <http://www.indented.co.uk/2008/10/10/microsoft-dns-stale-records/>

Enable scavenging on all dns zones using Powershell: <http://virot.eu/enable-scavenging-on-all-dns-zones-using-powershell/>

Allowing secure dynamic updates: <http://technet.microsoft.com/en-us/library/cc753751.aspx>