# DNS in a workgroup

Posted on June 12, 2013

Ace Fekay, MCT, MVP, MCSE 2012\Cloud, MCITP EA, MCTS Windows 2008\R2, Exchange 2007 & 2010, Exchange 2010 Enterprise Administrator, MCSE 2003\2000, MCSA Messaging 2003
Microsoft Certified Trainer
Microsoft MVP: Directory Services
Active Directory, Exchange and Windows Infrastructure Engineer and Janitor
www.delcocomputerconsulting.com

## DNS Dynamic Updates in a Workgroup

### Prelude

So the machines and devices you want to register into DNS are not in an Active Directory. Therefore, that means none of your Windows computers have been configured with a Primary DNS Suffix. When you join a computer to a domain, one of the many things that occur on the computer is that the Primary DNS Suffix is automatically configured, which matches the name of the AD DNS domain name, which should also be identical to the DNS zone name.

And further, as we already know, that's what a computer needs to register into a zone with the same name. If you weren't aware of this basic requirement, you can catch up on how Dynamic DNS registration works by reading my other blog:

AD & Dynamic DNS Updates Registration Rules of engagement
https:\blogs.msmvps.com\acefekay\2012\11\19\ad-dynamic-dns-updates-registration-rules-of-engagement

### Primary DNS Suffix

However, workgroup computers normally do not have a Primary DNS Suffix, unless you've already manually configured all of them. Neither do other devices, such as mobile phones, tablets and other non-Microsoft products.

No fret. We can make this work without a Primary DNS Suffix. After all, non-Windows devices, such as phones and tables, do not have such a setting to configure.

There are actually a number of ways to get this to work. One way is to force the Primary DNS Suffix on your Windows workgroup computers by using a registry script (outlined later below). However, that will only be good for your Windows computers. What about those non-Windows devices?

To register your Windows computers and non-Windows devices, an easier way to go about it is to use Windows Server DHCP to register all leases into the DNS zone. We can do this by using the DHCP service on a non-AD joined Windows Server configured with DHCP credentials, DHCP Option 015, and configured to force all leases to register into the zone whether the device has the ability to register on its own or not.

The credentials allows DHCP to own the record, so in case the device leaves and returns at a later date and gets a new IP, the DHCP service can update the old host record in DNS with the new IP. Without credentials, the

device will update, but it may not be able to update its old record, which then you may wind up with duplicate host entries in the zone. Of course, we wouldn't want that.

## Use Windows DHCP to Force Register All Leases

The first thing we need is a Windows Server with the DHCP and DNS services installed and running. To provide a 30,000' view of what's involved, we start by creating a regular, non-Administrator, local user account on the server that will be used to configure the DHCP scope to use as credentials for registration. And to stress what I just said, it does NOT have to, nor should it be, an Administrator account. It should just be a plain-Jane user account, but give it a really strong password. In an AD domain environment, the credentials would be a plain-old AD Domain User account. But in this case, it's a local User account. Then configure DHCP to force update all records, whether the entity can register or not.

## Zone's NS & SOA Entries

For the DNS service to properly work, the DNS server itself must have its own host (A) record reregistered into the zone, as well as registered its record as an NS record in the zone's properties. This means that the Windows server DNS is installed on, must be configured with a Primary DNS Suffix matching one of the zones that DNS will be authoritative for (meaning that DNS is hosting the zone). We usually pick the main zone for the company environment. Once configured, then this part will automatically occur. If it doesn't have a Primary DNS Suffix, then this automatic part will not happen.

You can easily tell if any Windows computer has a Primary DNS Suffix by a simple ipconfig \all, however I'm sure you already know if your server has one configured one or not, since this must be manually done on a workgroup computer. As stated, an AD joined computer (server or workstations) will automatically configure itself with a Primary DNS Suffix that matches the AD DNS domain name,

## Detailed Steps:

1. First, assuming you haven't already installed DNS and created a zone in DNS, let's go ahead and install and create your zone.
2. You can install the DNS service Role (yes, it's a Role, not a Feature), using Server Manager in Windows Server 2008, 2008 R2, 2012, and newer.
   Install a DNS Server
   http:\technet.microsoft.com\en-us\library\cc725925.aspx
3. Once installed, create your zone, such as adatum.com. Also in the zone properties, make sure you allow Updates. And note, with DNS on a non-DC, the only option you have is either "None," or "Nonsecure and secure." You have no choice other than "Nonsecure and secure." (Click image to see a larger version of the image in a new window)
   **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
   Obviously it's important that the DNS & DHCP server is set to a static IP configuration. Pick an IP, and stick to it. Then make sure that the server itself is ONLY using its own IP for DNS entry in its NIC. No others must be in here, otherwise you'll get unexpected and possibly undesired results.
   (Click image to see a larger version of the image in a new window)
   **⚠ You have pasted a link referring an attachment that could not be found in the storage location of**

**this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**

4. I need to stress that this is extremely important.
5. If you have any computers in the environment that have a static IP address configured (not getting an IP from DHCP), you must also make sure they are configured with only your own Windows DNS server's IP.
6. If you've configured it with your ISP's DNS, because you thought that's what you need for internet resolution, then that's wrong, and more importantly, that computer will not register nor be able to resolve internal hosts.
7. Same thing using your router (either ISP provided, or something you bought from a retail store such as a Linksys, Dlink, etc). Do not use your router as a DNS address. They are not DNS servers, and they only proxy to an external DNS, which is useless if you are running DNS internally.
8. And no, you CAN'T mix internal and external DNS entries. It doesn't work that way. It's not a DNS server thing, rather it's based on a DNS client, specifically it's based on how the client side resolver algorithm works. For a technical explanation for the technically curious, please read my blog explaining it: http:\msmvps.com\blogs\acefekay\archive\2009\11\29\dns-wins-netbios-amp-the-client-side-resolver-browser-service-disabling-netbios-direct-hosted-smb-directsmb-if-one-dc-is-down-does-a-client-logon-to-another-dc-and-dns-forwarders-algorithm.aspx
9. The DNS server can use Root Hints to resolve internet names. Or you can configure a Forwarder: Configure a DNS Server to Use Forwarders – Windows 2008 and 2008 R2 (Includes info on how to create a forwarder) http:\technet.microsoft.com\en-us\library\cc754941.aspx
   (Click image to see a larger version of the image in a new window)
   **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
10. Configure a Primary DNS Suffix on your Windows Servers that's hosting DNS. To do that:
    Go to Start
    Right-click Computer, properties
    In the computer name tab click change settings
    Then click change
    Then click More
    Type your domain name here.
    Click Ok a few of times, and restart the server.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
11. After the restart, make sure it registered into the your zone, for example, contoso.com. You can simple check by running an ipconfig \all. Look for the Primary DNS Suffix name.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
    For more information on all the info that an ipconfig \all provides, please read the following:
    Why do we ask for an ipconfig \all, when we try to help diagnose AD issues and other issues?

https:\blogs.msmvps.com\acefekay\2013\03\02\why-do-we-ask-for-an-ipconfig-all-when-we-try-to-help-diagnose-ad-issues\

12. In the contoso.com zone properties, Nameserver tab. Make sure it registered itself. If not, manually add it by clicking Add, then type in the server's FQDN, and click Resolve. If all things are configured correctly, then it should resolve it. Click OK.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
13. On the "Start of Authority (SOA)" tab click "Browse…" next to the Primary server field and browse for the server's A record in the contoso.com zone. Click OK.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
14. Repeat step 4 for the reverse zone, and any other zones you've created in DNS.
15. DHCP Options
    1. DHCP Option 015 must be set to your zone, such as adatum.com. This provides a way to work for the interface to use that zone for registration, as well as for the DHCP server to use it to register into the zone.
    2. DHCP Option 006 must be set to only your internal DNS servers. Do not use your router as a DNS address (it's really not a DNS server anyway), or your ISP's DNS servers.
       (Click image to see a larger version of the image in a new window)
       **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
16. Configure scavenging. The scavenging NoRefresh and Refresh values combined should add up to or greater than the lease length. For example, if the DHCP lease length is 8 days, then the NoRefresh value should be 4, and the Refresh value should be 4.
    More info:
    Good article by Sean Ivey, MSFT:
    How DNS Scavenging and the DHCP Lease Duration Relate
    (Make the NoRefresh and Refresh each half the lease, so combined, they are equal or greater than the lease).
    http:\blogs.technet.com\b\askpfe\archive\2011\06\03\how-dns-scavenging-and-the-dhcp-lease-duration-relate.aspx
17. In DHCP properties, DNS tab (note -this tab is actually DHCP Option 081, even though it doesn't say it), choose to force DHCP to update all records whether a DHCP client asks or not. And configure it to register records for machines that can't.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**
18. Configure a user account to be used for DHCP Credentials (as I said above), then go into DHCP, IPv4, properties, Advanced, Credentials, and enter the credentials.
    (Click image to see a larger version of the image in a new window)
    **⚠ You have pasted a link referring an attachment that could not be found in the storage location of**

**this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**

19. Restart the DHCP service.
20. It should now work.

## Example of what you should see after it's configured and working:

(Click image to see a larger version of the image in a new window)
**⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**

**⚠ You have pasted a link referring an attachment that could not be found in the storage location of this note. Pasting links referring attachments is only supported if the source and destination location is the same storage. Please Drag&Drop the attachment instead! ⚠**

## Other notes and references:

There are a number of ways to get this to work. Read the following discussion for more info:

Technet thread: "Server 2008 R2: DNS records not dynamically registering in workgroup situation" 12\31\2010
http:\social.technet.microsoft.com\Forums\en-US\winserverNIS\thread\2380872f-2e71-49eb-8fbb-87f980920fc7\

## Registry summarized:

Not that this will work for your non-Windows devices, but I'm providing this information if you want to only configure your Windows computers.

You can create and remotely run a registry script for the interface on the workgroup machines using a tool called PSEXEC (free download from Microsoft). Of course you must have the local admin account credentials on all your computers to run this remotely, and the remote Registry service started, and possibly antivirus software and Windows firewall configured to allow this.

You'll want to target and populate the following two registry entries with your zone name, such as adatum.com:

- HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\domain
- HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\NV domain

Using the above two keys, try this VB script:
SET WSHShell = CreateObject("WScript.Shell")
WSHShell.RegWrite "HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\NV domain", "adatum.com", "REG_SZ"
WSHShell.RegWrite "HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\domain", "adatum.com", "REG_SZ"

## If you are in an AD Environment

Oh, and if you're curious how DHCP should be configured in an AD environment to force updates, etc, read my blog on it, please:

DHCP Service Configuration, Dynamic DNS Updates, Scavenging, Static Entries, Timestamps, DnsUpdateProxy Group, DHCP Credentials, prevent duplicate DNS records, DHCP has a "pen" icon, and more…
Published by Ace Fekay, MCT, MVP DS on Aug 20, 2009 at 10:36 AM 3758 2
http:\msmvps.com\blogs\acefekay\archive\2009\08\20\dhcp-dynamic-dns-updates-scavenging-static-entries-amp-timestamps-and-the-dnsproxyupdate-group.aspx

## Good summary:

How Dynamic DNS behaves with multiple DHCP servers on the same Domain?
http:\social.technet.microsoft.com\Forums\en-US\winserverNIS\thread\e9d13327-ee75-4622-a3c7-459554319a27
Summary

I hope you've found this helpful. Any suggestions, errors, comments, etc., are all welcomed!

# AD & Dynamic DNS Updates Registration Rules of engagement

Keep in mind, for the most part it automatically works "out of the box" without much administrative overhead.

Original Compilation: 11\19\2012
Updated: 9\5\2013

## Prologue

What I've tried to do is accumulate all pertinent information about configuring dynamic DNS registration in an AD environment. I hope I haven't missed anything, and that I've explained each numbered bullet point well enough and removed all ambiguity, to fully understand each point.

And yes, this blog is regarding an AD environment. If you have a non-AD environment with a Windows DNS server that you want your computers to register, please read the following blog:

DNS Dynamic Updates in a Workgroup
https:\blogs.msmvps.com\acefekay\2013\06\12\dns-dynamic-updates-in-a-workgroup\

## Summary

1. The machine's DNS entries in the NIC, must be ONLY configured to use the internal DNS servers that host the zone. No others.
   a. DHCP Option 006 MUST only be the internal DNS server(s) you want to use, otherwise if using an ISP's DNS or your router, expect undesired results.
2. The Primary DNS Suffix on the machine MUST match the zone name in DNS.
   1. For joined machines, this is default.
   2. For non-joined machines, the Primary DNS Suffix must be manually configured or scripted.
3. If using DHCP Option 015 (Connection Specific Suffix), it must match the zone name and have "Use This Connection's DNS Suffix in DNS Registration" along with "Register This Connection's Addresses in DNS"

checked in the NIC's IPv4, Advanced, DNS tab.

    1. For additional information on how to configure updates in a workgroup:
       DNS Dynamic Updates in a Workgroup
       https:\blogs.msmvps.com\acefekay\2013\06\12\dns-dynamic-updates-in-a-workgroup\

4. The Zone must be configured to allow updates.
5. For AD Integrated Zones where you have it configured for "Secure and Unsecure Updates:
    1. If the machine's network card DNS address entries have been statically configured:
        1. They must only point to the internal DNS servers that host the AD zone or to servers that have a reference to the zone (such as stubs, secondary zones, conditional forwarders, or forwarders)
        2. It must be joined to the domain in order to authenticate using Kerberos to update.
    2. If statically configured and not joined to the domain, the client can't update its record if the zone is set to Secure Only.
    3. For non-joined domain DHCP clients, you can configure DHCP to update in lieu of the client updating into a Secure Only zone.
6. For any non-Windows statically configured machine, it must support the DNS Dynamic Updates feature and the zone configured to allow Secure and Unsecure updates.
7. If the DNS server is multihomed and not configured properly to work with multihoming, it may cause problems with Dynamic Updates.
    1. Read the following for more info:
       Multihomed DCs (with more than one unteamed NIC or multiple IPs) with DNS, RRAS, iSCSI, Clustering interfaces, management interfaces, backup interfaces, and\or PPPoE adapters – A multihomed DC is not a recommended configuration, however there are ways to configure a DC with registry mods:
       http:\msmvps.com\blogs\acefekay\archive\2009\08\17\multihomed-dcs-with-dns-rras-and-or-pppoe-adapters.aspx
8. If the zone is single label name, such as 'domain' instead of the proper minimal format of 'domain.com,' 'domain.net,' etc., it will NOT update.
9. The client will "look" for the SOA of the zone when it attempts registration. If the SOA is not available or resolvable, it won't register. Keep in mind with AD integrated zones the SOA rotates among the DCs because of the multimaster feature. This is default and expected behavior, but if there are any DCs that have any problems, and the client resolved the SOA to that DC, it may not accept the update.
10. The zone in DNS must NOT be a single lable name, such as "DOMAIN" instead of the required minimum of two hierarchal levels such as domain.com, domain.local, domain.me, domain.you, etc. Single label name zones are problematic, do not conform to the DNS RFC, and causes excessive internet traffic to the Root Servers when DNS tries to resolve a single label name query, such as querying for computername.domain – in such a query, the domain name is actually treated as a TLD. ISC has made a note of the excessive traffic generated by Microsoft DNS servers configured with a single label name in 2004 with Microsoft, which in turn disabled the ability for Microsoft DNS in Windows 2000 SP4 and newer to resolve single label names without a registry band aid. More info on this:
    1. Active Directory DNS Domain Name Single Label Names – Problematic
       Published by Ace Fekay, MCT, MVP DS on Nov 12, 2009 at 6:25 PM 641 0
       http:\msmvps.com\blogs\acefekay\archive\2009\11\12\active-directory-dns-domain-name-single-label-names.aspx
11. 
```
For Windows 2008 and all newer operating systems, IPv6 must not be disabled. If disab
```

The Cable Guy – Support for IPv6 in Windows Server 2008 R2 and Windows 7, by Joseph Davies, Microsoft, Inc.
Quoted by Joseph Davies, MSFT:
"IPv6 is a mandatory part of the Windows operating system and it is enabled and included in standard Windows service and application testing during the operating system development process. Because Windows was designed specifically with IPv6 present, Microsoft does not perform any testing to determine the effects of disabling IPv6. If IPv6 is disabled on Windows Vista, Windows Server 2008, or later versions, some components will not function. "Moreover, applications that you might not think are using IPv6—such as Remote Assistance, HomeGroup, DirectAccess, and Windows Mail—could be."
http:\technet.microsoft.com\en-us\magazine\2009.07.cableguy.aspx

1. Arguments against disabling IPv6
   Demoire, [MSFT], 24 Nov 2010 12:37 AM
   http:\blogs.technet.com\b\netro\archive\2010\11\24\arguments-against-disabling-ipv6.aspx

12. IPv6 for Microsoft Windows: Frequently Asked Questions
    (Basically Microsoft is saying in this KB article to not disable IPv6)
    http:\technet.microsoft.com\en-us\network\cc987595.aspx

## Full explanation:

1. Active Directory's DNS Domain Name is NOT a single label name ("DOMAIN" vs. the minimal requirement of "domain.com." "domain.local," etc).
2. The Primary DNS Suffix MUST matches the zone name that is allowing updates. Otherwise the client doesn't know what zone name to register in. You can also have a different Connection Specific Suffix in addition to the Primary DNS Suffix to register into that zone as well.
3. AD\DNS zone MUST be configured to allow dynamic updates, whether Secure or Secure and Non-Secure. For client machines, if a client is not joined to the domain, and the zone is set to Secure, it will not register either.
4. You must ONLY use the DNS servers that host a copy of the AD zone name or have a reference to get to them.
   1. Do not use your ISP's, an external DNS address, your router as a DNS address
   2. Do not use any DNS that does not have a copy of the AD zone.
   3. Internet resolution for your machines will be accomplished by the Root servers (Root Hints), however it's recommended to configure a forwarder for efficient Internet resolution.
5. The domain controller is multihomed (which means it has more than one unteamed, active NIC, more than one IP address, and\or RRAS is installed on the DC).
6. The DNS addresses configured in the client's IP properties must ONLY reference the DNS server(s) hosting the AD zone you want to update in.
   1. This means that you must NOT use an external DNS in any machine's IP property in an AD environment.
   2. You can't mix internal and external DNS server. This is because of the way the DNS Client side resolver service works. Even if you mix up internal DNS and ISP's DNS addresses, the resolver algorithm may still pick the incorrect DNS to query. Based on how the algorithm works, it will ask the first one first. If it doesn't get a response, it removes the first one from the eligible resolvers list and goes to the next in the list. It will not go back to the first one unless you restart the machine, restart the DNS Client service, or set a registry entry to cut the query TTL to 0. The rule is to ONLY use your internal DNS server(s) and configure a forwarder to your ISP's DNS for efficient Internet resolution.

3. There is a registry entry to cut the query to 0 TTL (normally this is not necessary, but I'm posting it as a reference).
    1. The DNS Client service does not revert to using the first server …The Windows 2000 Domain Name System (DNS) Client service (Dnscache) follows a certain algorithm when it decides the order in which to use the DNS servers …
    http:\support.microsoft.com\kb\286834
4. The DNS Client Service Does Not Revert to Using the First Server in the List in Windows XP (applies to all Operating Systems, too)
    http:\support.microsoft.com\kb\320760
5. For more info, please read the following on the client side resolver service:
    DNS, WINS NetBIOS & the Client Side Resolver, Browser Service, Disabling NetBIOS, Direct Hosted SMB (DirectSMB), If One DC is Down Does a Client logon to Another DC, and DNS Forwarders Algorithm if you have multiple forwarders.
    http:\msmvps.com\blogs\acefekay\archive\2009\11\29\dns-wins-netbios-amp-the-client-side-resolver-browser-service-disabling-netbios-direct-hosted-smb-directsmb-if-one-dc-is-down-does-a-client-logon-to-another-dc-and-dns-forwarders-algorithm.aspx

7. For DHCP clients, DHCP Option 006 for the clients are set to the same DNS server.
8. If using DHCP, DHCP server must only be referencing the same exact DNS server(s) in it's own IP properties in order for it to 'force' (if you set that setting) registration into DNS. Otherwise, how would it know which DNS to send the DNS registration request data to?
9. If the AD DNS Domain name is a single label name, such as "EXAMPLE", and not the proper format of "example.com" and\or any child of that format, such as "child1.example.com", then we have a real big problem. DNS will not allow registration into a single label domain name.
    This is for two reasons:
    1. It's not the proper hierarchal format. DNS is hierarchal, but a single label name has no hierarchy. It's just a single name
    2. Registration attempts causes major Internet queries to the Root servers. Why? Because it thinks the single label name, such as "EXAMPLE", is a TLD (Top Level Domain), such as "com", "net", etc. It will now try to find what Root name server out there handles that TLD. In the end it comes back to itself and then attempts to register. Unfortunately it doe NOT ask itself first for the mere reason it thinks it's a TLD.
    3. Quoted from Alan Woods, Microsoft, 2004:
    "Due to this excessive Root query traffic, which ISC found from a study that discovered Microsoft DNS servers are causing excessive traffic because of single label names, Microsoft, being an internet friendly neighbor and wanting to stop this problem for their neighbors, stopped the ability to register into DNS with Windows 2000 SP4, XP SP1, (especially XP,which cause lookup problems too), and Windows 2003. After all, DNS is hierarchal, so therefore why even allow single label DNS domain names?"
    4. The above also *especially* applies to Windows Vista, Windows 7, &, 2008, 2008 R2, Windows 2012, and newer.
10. 'Register this connection's address" on the client is not enabled under the NIC's IP properties, DNS tab.
11. Maybe there's a GPO set to force Secure updates and the machine isn't a joined member of the domain.

12. With Windows 2000, 2003 and XP, the “DHCP client” Service is not running. In Windows 2008, Windows Vista and all newer operating systems, it’s now the DNS Client Service.
    1. This is a requirement for DNS registration and DNS resolution even if the client is not actually using DHCP.
    2. Dynamic DNS Updates Do Not Work if the DHCP Client Service Stops (2000\2003\XP only) http:\support.microsoft.com?id=264539
13. You can also configure DHCP to force register clients for you, as well as keep the DNS zone clean of old or duplicate entries. The following has more information on how to do that:
    1. DHCP, Dynamic DNS Updates, Scavenging, static entries & timestamps, and the DnsProxyUpdate Group (How to remove and prevent future duplicate DNS host records)
       Published by acefekay on Aug 20, 2009 at 10:36 AM 3758 2
       http:\msmvps.com\blogs\acefekay\archive\2009\08\20\dhcp-dynamic-dns-updates-scavenging-static-entries-amp-timestamps-and-the-dnsproxyupdate-group.aspx

## What will stop AD SRV registration:

1. Any DNS server referenced in TCP\IP properties that does not host the AD zone name, or does not have a reference to the internal AD zones name.
    1. External DNS servers do not host or have a reference, therefore must NOT be used.
    2. AD Domain machines must never be pointed at an external (ISP) DNS server or even use an ISP DNS server as an “Alternate DNS server” because they do not host the internal AD zone, or have a reference to it.
        1. Only use internal DNS servers when part of an Active Directory domain. Active Directory’s Reliance on DNS, and why you should never use an ISP’s DNS address or your router as a DNS address, or any other DNS server that does not host the AD zone name
           http:\msmvps.com\blogs\acefekay\archive\2009\08\17\ad-and-its-reliance-on-dns.aspx
2. Are any services disabled such as the DHCP Client service or the DNS Client Service? They are required services, whether the machine is static or DHCP.
    1. No DNS registration functions if DHCP Client Service Is Not Running (2000\2003\XP only) http:\support.microsoft.com?id=268674
    2. Dynamic DNS Updates Do Not Work if the DHCP Client Service Stops (2000\2003\XP only) http:\support.microsoft.com?id=264539
    3. For all Windows 2008, Windows Vista and all newer operating systems, it’s the DNS Client Service.
3. The AD\DNS zone not configured to allow dynamic updates.
4. Make sure ‘Register this connection’s address” in DNS is enabled under TCP\IP properties.
5. Missing or incorrect “Primary DNS suffix” or “Connection-specific DNS suffix” of the domain to which the machine belongs.
    1. I one of these are incorrect, the client side service cannot find the correct zone to register into. If missing or incorrect, it is called a Disjointed Domain Namespace.
6. Is the firewall service enabled? (disable it).
7. Were the default C: drive permissions altered and was a hotfix installed a recently?
    1. “Systems that have changed the default Access Control List permissions on the %windir%\registration directory may experience various problems after you install the Microsoft Security Bulletin MS05-051 for COM+ and MS DTC”
       http:\support.microsoft.com\kb\909444
    2. For more info about this issue, see:
       http:\blogs.technet.com\steriley\archive\2005\11\08\414002.aspx

8. If the zone is set to Secure Updates Only, the computer may not have authenticated to the domain (which can be due to DNS misconfiguration or DNS server problem), which of course causes more problems than just DNS registration.
9. Is the File and Print services enabled?
    1. It must be enabled
10. Microsoft Client Services enabled?
    1. If not, it must be enabled.
11. Is DNS service listening on the private LAN interface?
    1, Check under the Interfaces tab under DNS server properties in the DNS console.
12. More than one NIC on a client?
    1. The wrong one may be registering.
13. Updates allowed on the zone?
    1. This is an obvious one.
14. Primary DNS suffix matches the zone name in DNS and the AD domain name?
    1. If not, then it won't register into the zone.
15. Was Zone Alarm ever installed on these machines?
    1. If so, ZA leaves SYS files and other remnants that continue to block traffic.
16. Any Event log errors?
17. Was a Registry entry configured to stop registration?
    1. 246804 – How to Enable-Disable Windows 2000 Dynamic DNS Registrations (per NIC too): http:\support.microsoft.com?id=246804
18. Spyware or something else such as DotNetDns installed on it?
    1. Download the free tool at www.malwarebytes.com and run a malware scan.
    2. Download the free Malicious Software Scanner from Microsoft and run a scan
    3. Download TrendMicro HouseCall free scan tool and run it.
19. Single Label Domain Name?
    1. Active Directory DNS Domain Name Single Label Names – Problematic – And this applies to any DNS zone name, not just AD.
       Published by Ace Fekay, MCT, MVP DS on Nov 12, 2009 at 6:25 PM 641 0
       http:\msmvps.com\blogs\acefekay\archive\2009\11\12\active-directory-dns-domain-name-single-label-names.aspx
20. Netlogon and DFS services must be started.
21. Malware or virus altering network services preventing it from registering.
    1. Some sort of firewall in place, whether the Windows firewall disabling File and Print Services, or a 3rd party firewall, which many AV programs now have built in and must be adjusted to allow this sort of traffic and exclude the NTDS and SYSVOL folders.
    2. If Windows Firewall, run the following to see what settings are enabled:

    ```
    netsh firewall show config
    ```

22. Is IPv6 disabled? That will stop registration.
    1. Enable it.
23. Do any duplicate AD integrated zones exist in the AD database?
    1. This will cause major problems. Any duplicates found must be deleted. The cause must also be determined to eliminate it from occurring again.
    2. Using ADSI Edit to Resolve Conflicting or Duplicate AD Integrated DNS zones
       Published by acefekay on Sep 2, 2009 at 2:34 PM 7748 2

http:\msmvps.com\blogs\acefekay\archive\2009\09\02\using-adsi-edit-to-resolve-conflicting-or-duplicate-ad-integrated-dns-zones.aspx

24. Were imaged machines cloned without the image being Sysprepped first?
    1. If not, duplicate SIDs will cause machines to fail authentication to register into the zone.

## Suggestions, Comments, Corrections are welcomed.

Ace Fekay, MCT, MVP, MCSE 2012\Cloud, MCITP EA, MCTS Windows 2008\R2, Exchange 2007 & 2010, Exchange 2010 Enterprise Administrator, MCSE 2003\2000, MCSA Messaging 2003
Microsoft Certified Trainer
Microsoft MVP: Directory Services
Active Directory, Exchange and Windows Infrastructure Engineer and Janitor
www.delcocomputerconsulting.com