


Unexpected DNS record registration behavior when the DHCP server manages dynamic DNS updates - Windows Server

 learn.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-registration-behavior-when-dhcp-server-manages-dynamic-dns-updates

Unexpected DNS record registration behavior if DHCP server uses "Always dynamically update DNS records"

- Article
- 12/26/2023

Applies to: Windows 11, Windows 10, Windows 8.1

Symptoms

You have an infrastructure that uses Windows Dynamic Host Configuration Protocol (DHCP) clients and Microsoft DHCP servers to assign and manage IP addresses. On the DHCP server, you select **Enable DNS dynamic updates according to the settings below** and **Always dynamically update DNS records**. In this configuration, you expect the DHCP server to manage dynamic DNS updates for A records and PTR records. However, you observe that both the client and the server create DNS records. Depending on your configuration, this behavior has the following effects:

- If you configure the DNS zones for **Nonsecure and secure** dynamic updates, you see that the DHCP server creates records, and then the DHCP client deletes and re-creates the same records.
- If you configure the DNS zones for **Secure only** dynamic updates, DNS records might become inconsistent. Both the DHCP server and the DHCP client create records. However, the DHCP server can't update records that the DHCP client creates, and the DHCP client can't update records that the DHCP server creates.

Cause

To obtain an IP address, the DHCP client sends a DHCP Request message to the DHCP server. Typically, this message includes the client's fully qualified domain name (FQDN) and flags that govern dynamic DNS update behavior. This information is collectively named *Option 81* (also known as the *Client FQDN option*).

Note

Some older DHCP clients do not use Option 81. To provide dynamic updates for these clients, configure the DHCP server to enable the **Dynamically update DNS records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)** option.

The DHCP server also stores a set of Option 81 flags that govern dynamic DNS update behavior. Part of the DHCP DORA (Discover/Offer/Request/Acknowledge) process involves a comparison between the client and the server of their values of the Option 81 flags to determine who is responsible for DNS updates. The flags that are involved in the behavior that's described in the Symptoms section are named the **O** (override) and **S** (server) bits. The flags function as follows:

- If **S** = **0**, the client is responsible for updating A records.
- If **S** = **1**, the server is responsible for updating A records.
- If the **S** value that the client sends in its request differs from the server's **S** value, the server sets its **O** value to **1**.

As described in the RFC, the DHCP server's reply to the request message should include its flag values. If **O** is set to **1** in the server's message, the client should understand that the server is overriding the client's **S** value.

In Windows 8.1, a deliberate design change was introduced to the DHCP client's dynamic DNS update behavior. This change supports continued development and enhancements of the TCP/IP (Transmission Control Protocol/Internet Protocol) stack in later versions of Microsoft operating systems. In Windows 8.1 and later versions, the DHCP client doesn't honor the DHCP server's Option 81 **O** and **S** values. If the client is configured to update A records, it continues to do this even if the server is also configured to update A records. That's the case when you select **Always dynamically update DNS records** in the DHCP management console.

If you configure your DNS zones for **Secure only** dynamic updates, then only the entity (the DHCP client, DHCP server, or an account that the DHCP services are configured to use) that created a DNS record can update or delete that record. If the DHCP client and not the DHCP server creates a DNS record, the DHCP server can't modify that record later.

Note

Microsoft's DHCP client doesn't provide a method to directly set the client's **O** and **S** values in the user interface. By default, both values are **0**. You can view the values by recording a netsh trace of a DHCP client request, and by using a tool such as Netmon to view the results.

You can use the Windows PowerShell cmdlet, Get-DhcpServerv4OptionValue, to view the DHCP server's Option 81 value. However, the cmdlet reports this value as a single integer that combines several different settings as bit values. For example, if you select **Always dynamically update DNS records** on the **DNS** tab of a DHCP scope properties window, this sets the **S** value to **1**. But the cmdlet reports one of eight possible values for Option 81. All of these use **S=1**. The specific value depends on the combination of settings that are made on the **DNS** tab.

For more information about how dynamic updates work between the DHCP client, the DHCP server, and the DNS server, see [DNS Processes and Interactions](#)

Resolution

If your architecture requires that you use **Always dynamically update DNS records**, you can create a registry key on the client computer to force the DHCP client to honor the DHCP server override.

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For protection, back up the registry before you modify it so that you can restore it if a problem occurs. For more information about how to back up and restore the registry, see [How to back up and restore the registry in Windows](#).

1. Navigate to the following subkey:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters`

2. Under the subkey, create the following entry:

- Name: **RegistrationOverwrite**
- Type: **REG_DWORD**
- Value: **2**

Note

RegistrationOverwrite has the following possible values:

- **0** - No overwrite.
- **1** - Records that the DNS client creates overwrite records that the DHCP server creates. This is the default value.
- **2** - Records that the DHCP server creates overwrite records that the DNS client creates).

3. Restart the client computer.
4. In the DNS server management console, check the forward and reverse lookup zones. Depending on your specific environment, you might have to manually delete A and PTR records that the DHCP server doesn't have permission to delete or change.