Configure Cache Locking

Applies To: Windows Server 2008 R2/2012

Cache locking is a new security feature available with Windows Server® 2008 R2 that allows you to control whether or not information in the DNS cache can be overwritten. When a recursive DNS server responds to a query, it will cache the results obtained so that it can respond quickly if it receives another query requesting the same information. The period of time the DNS server will keep information in its cache is determined by the Time to Live (TTL) value for a resource record. Until the TTL period expires, information in the cache might be overwritten if updated information about that resource record is received. If an attacker successfully overwrites information in the cache, they might be able to redirect traffic on your network to a malicious site.

Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, then the DNS server will not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This means that cached entries will not be overwritten for the entire duration of the TTL. The cache locking value is stored in the **CacheLockingPercent** registry key. If the registry key is not present, then the DNS server will use the default cache locking value of 100.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (http://go.microsoft.com/fwlink/?LinkId=83477).

Configuring cache locking

Tip

The command line utility **DnsCmd.exe** is the recommended method for configuring cache locking.

- Using a command line
- Using the Windows interface

To configure cache locking using a command line

---

1. Open an elevated command prompt.
2. Type the following command, and then press ENTER:

   Copy

```
dnscmd /Config /CacheLockingPercent
<percent>
```

3. Restart the DNS Server service.

Parameter	Description
dnscmd	The command-line tool for managing DNS servers.
/Config	Required. Allows the user to change a value in the Windows Registry.
/CacheLockingPercent	Required. Specifies the **CacheLockingPercent** registry key.
<percent>	Optional. Specifies the cache locking percent, from 0 to 100 in decimal format. If no value is entered, the cache locking percent is set to 0.

Tip

Use the /Info command to view the current value of a registry key, for example: **Dnscmd /Info /CacheLockingPercent**.

Cache Locking. When cache locking is enabled, the DNS server will not allow cached records to be overwritten for the duration of the time to live (TTL) value on the DNS record. This feature protects the DNS cache records against possible DNS cache poisoning attacks by malicious users on the Internet.

Cache locking is configured as a percent value. Let's say that you set the cache locking value at 75, the DNS server will not overwrite a cached entry for 75% of the duration of the TTL. By default, the cache locking percent value is 100 meaning that cached entries will not be overwritten for the entire duration of the TTL.

You can use the **dnscmd** tool to configure cache locking on a Windows Server 2012 DNS server. See figure below.

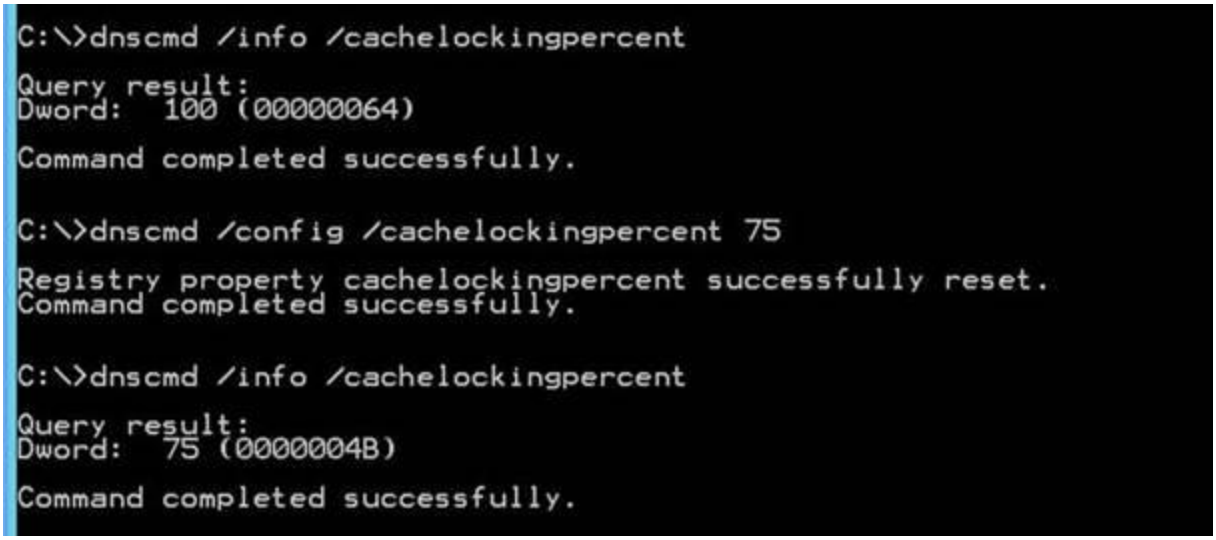

Figure 25

[To configure cache locking using the Windows interface]

---

1. Click **Start**, click **Run**, type **regedit.exe**, and then press ENTER.
2. In Registry Editor, open **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters**.
3. If the **CacheLockingPercent** registry key is not present, right-click **Parameters**, click **New**, click **DWORD (32-bit) Value**, and then type **CacheLockingPercent** for the name of the new registry key.
4. Double-click the **CacheLockingPercent** registry key.
5. Under **Base**, choose **Decimal**, under **Value data** type a value from 0 to 100 for the cache locking percent, and then click **OK**.
6. Close Registry Editor.
7. Restart the DNS Server service.