Knowledge Base

Installing Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) on a Domain Controller

PSS ID Number: 255134

Article Last Modified on 11/4/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server

This article was previously published under Q255134

SUMMARY

When a Windows 2000-based computer Dynamic Host Configuration Protocol (DHCP) Server service is installed on a domain controller, and it is configured to perform Dynamic Domain Name System (DDNS) update of the records on behalf of its clients in the DNS zones that are configured to enable only secure dynamic update, the DHCP Server may overwrite the records for which the DHCP Server did not have write permissions.

MORE INFORMATION

Standard DDNS is prone to name hijacking. To provide protection from name hijacking, you can configure DNS zones hosted on Windows 2000 DNS Servers for Secure Dynamic Updates. Note that this feature is only available on Active Directory-integrated zones.

By default, the Domain Controllers (DCs) group has full control of all DNS zones and records. Because the DHCP Server service runs under the domain controller's computer account, it has full control of all DNS zones and records. Because of this, the DHCP Server service has the authority to update or delete any DNS record that is registered in a secure Active Directory-integrated zone (this includes records that were securely registered by other Windows 2000-based computers, including domain controllers).

To minimize the potential of name hijacking, Microsoft does not recommend that you install the DHCP Server service configured to perform DDNS update on a DC. Instead, install the DHCP Server service on a separate server, and not a domain controller.

Windows 2000 Service Pack 1 Information

To overcome the name hijacking issue that is described in this article, Windows 2000 Service Pack 1 includes the following changes:

You can configure the DHCP Server service to impersonate an account to perform DNS registrations. The Netsh.exe tool can be used to configure the impersonation credentials. You must create a dedicated user account in Active Directory before you use the Netsh.exe tool to configure the DHCP Server service impersonation credentials of this account when DHCP Server service performs secure Dynamic DNS update. For information about how to create a user account in Active Directory, view the **Active Directory user accounts, adding** topic in Windows 2000 Help.

How to Use the Netsh.exe Tool

NOTE: The Netsh.exe tool completes successfully only after you receive a "Command Successfully Completed" message.

- To set the user account that the DHCP Server service uses for DNS registrations, use the following command:
  ```
  netsh dhcp server set dnscredentials user name domain name password
  ```
  Note that if you use an asterisk (*) in place of the *password* variable, you are prompted to type a password.

  NOTE: You must restart the DHCP Server service for these changes to take effect.
- To delete the user account that the DHCP Server service uses for DNS registrations, use the following command:
  ```
  netsh dhcp server delete dnscredentials dhcpfullforce
  ```
  NOTE: You must restart the DHCP Server service for these changes to take effect.
- To show the user account that the DHCP Server service uses for DNS registrations, use the following command:
  ```
  netsh dhcp server show dnscredentials
  ```
  NOTE: User passwords must be periodically updated (the time period is specified by Active Directory domain administrator). DHCP administrators must update this password and configure the DHCP Server service with a new password by using the Netch.exe tool as specified earlier.

How to Configure the DHCP Server Service to Impersonate an Account

- DHCP Server service starts and an impersonation account is configured.
  If impersonation is successful, the impersonation account is used for all further DNS registrations. If impersonation is unsuccessful, the DHCP server logs the following Event ID in the System Event log and does not perform any DNS registrations (ignores DHCP Option 81):
  Event Type: Error
  Event Source: *DHCP server name*
  Event Category: None
  Event ID: 1002
  Date: 5/31/2000
  Time: 3:21:47 PM
  User: N/A
  Computer: *computer name*
  Description: The DHCP service failed to initialize its global parameters.
  The following error occurred: Logon failure: unknown user name or bad password.
  Data: 0000: 2e 05 00 00
- DHCP Server service starts and impersonation account is not configured.

  If the DHCP Server service is not running on a DC, the DHCP Server service uses local computer credentials to perform secure Dynamic DNS update. If the DHCP Server service is running on a DC, the service logs the following Event ID in the System Event log and the DHCP Server Service uses local computer credentials to perform secure DDNS update:
  Event Type: Warning

```
Event Source: DHCP server name
Event Category: None
Event ID: 1002
Date: 5/31/2000
Time: 3:57:13 PM
User: N/A
Computer: computer name
Description: The DHCP service failed to initialize its global parameters. The following error occurred: %%0
Data: 0000: 00 00 00 00
```

REFERENCES

For additional information, see the Windows 2000 DNS white paper at the following Microsoft Web site:

http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadrmgmt/w2kdns.asp

Keywords: kbDNS kbinfo KB255134
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

Send feedback to Microsoft