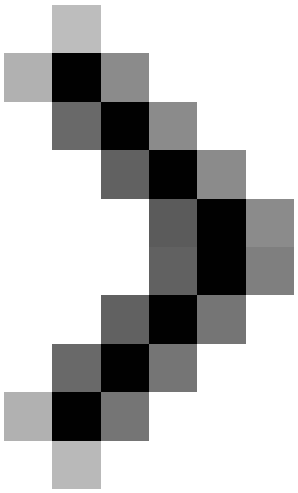
Learn about DHCP Server Security (part 2)

In this part 2, we will continue with the effective methods and tools used to enhance the security of the DHCP server.

***TipsMake.com* - In part 1, we came across some typical situations of DHCP server and some basic methods to prevent** . In Part 2, we will continue with the effective methods and tools used to enhance the security of DHCP servers in Windows 2000 and Windows Server 2003 platforms.



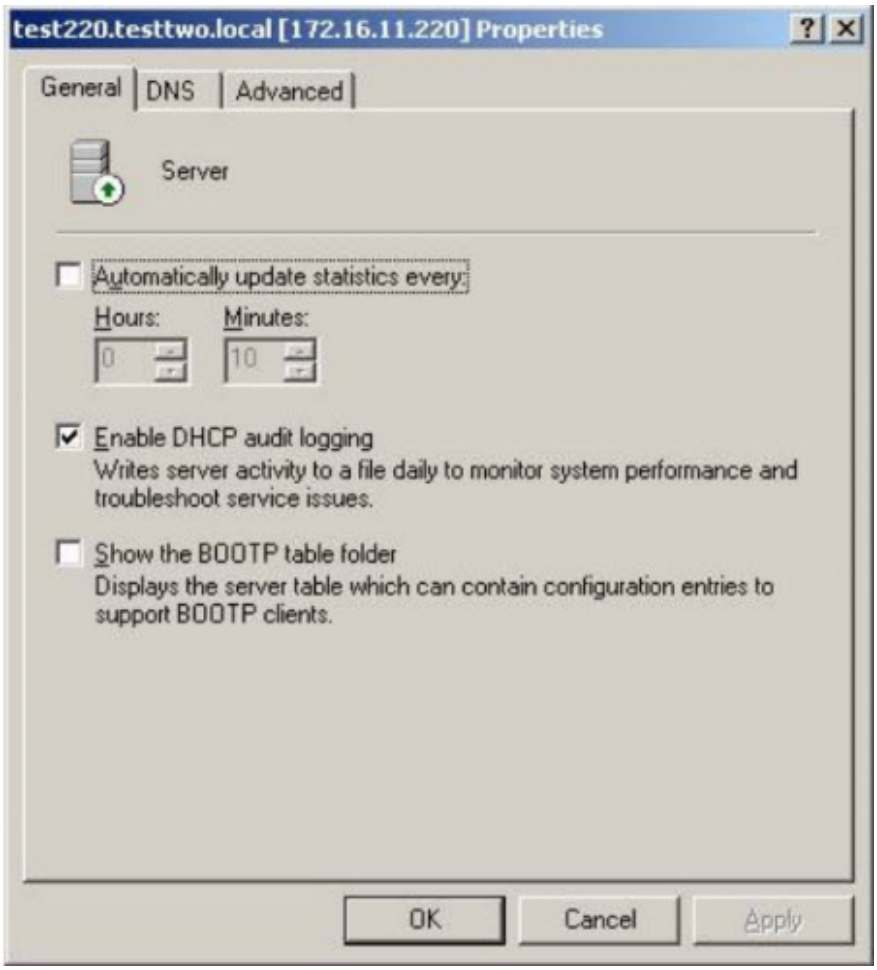
Learn about DHCP Server Security (part 1)

Learn about DHCP Server Auditing

Controlling the DHCP database on a DHCP server will help you determine which DHCP clients are receiving the address directly from the server better. In addition, this process also helps you identify *BAD_ADDRESS* components in the database, and where they are located . these information are really useful, when they can

cause conflicting addresses when The fake DHCP server system performs address assignment while they are still in use.

To enable control over the entire DHCP server system, open the DHCP console panel to connect to the DHCP server on the network. Right-click on the *server node* and select **Properties** , on the *General* tab, check the **Enable DHCP audit logging box** :

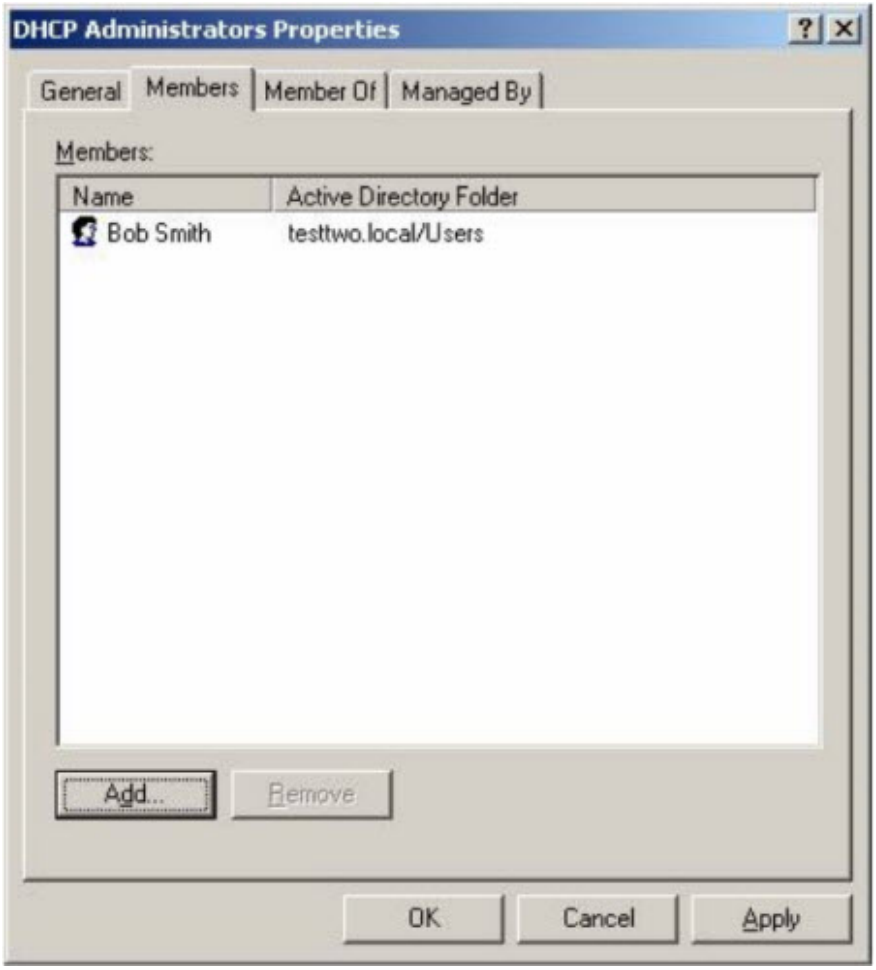


The DHCP control logs are stored by default in the *% windir% system32dhcp directory* , but users can change them via the *Advance* tab. These logs are created or attached to the daily work lists called DhcpSrvLog-Mon.log, DhcpSrvLog-Tue.log . Each of these records will start with the corresponding event ID, and the section First record stores the list of IDs with detailed explanation. In addition, custom operations can also be done via **HKLMSYSTEMCurrentControlSetServicesDHCPServerParameters** key in the Registry:

- **DhcpLogFilesMaxSize** specifies the maximum capacity for all DHCP archive log files (default is 7 MB)
- **DhcpLogDiskSpaceCheckInterval** specifies the checking of DHCP disk usage (default mode is 50 minutes)
- **DhcpLogMinSpaceOnDisk** determines the minimum free space to temporarily lock the login function (default level is 20 MB)

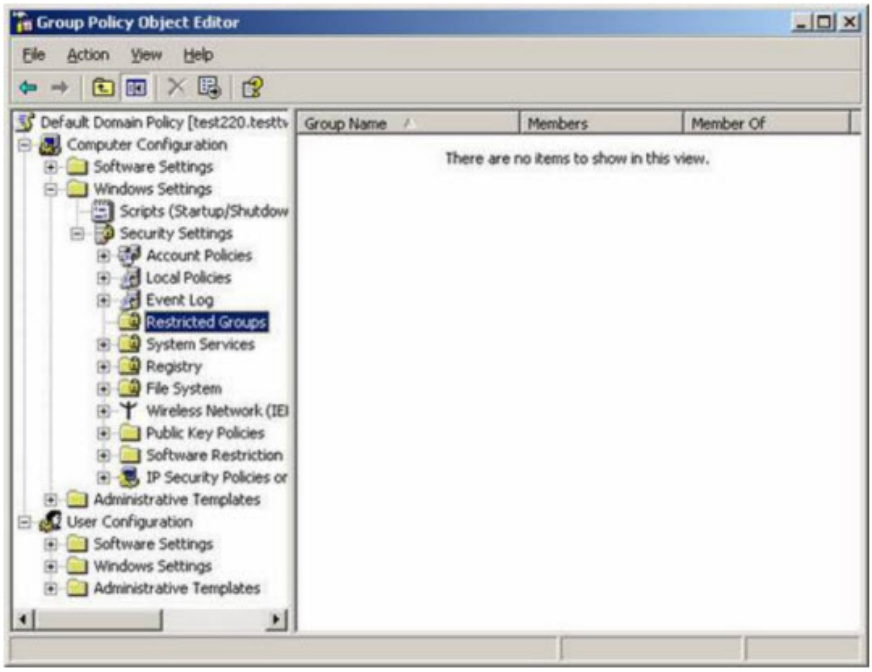
DHCP Administrators Group

In the past, for some systems, members of the Domain Admins group had full authority to set up DHCP on the server, and you could also authorize user accounts with appropriate tasks to manage the system's DHCP. system. To do this, open **Active Directory Users and Computers** and add the user account name to the *DHCP Administrators* group:



This mechanism gives users the ability to directly manage the DHCP server on the system without having to grant, authorize or authenticate to that admin account to perform other tasks. However, a problem arises here is how to manage all members of the DHCP Administrators group to make sure no unauthorized or fake accounts have been added to this group?

Besides, you can track members of important groups like DHCP Administrators using the *Restricted Groups* feature of Group Policy. To do this, use **Active Directory Users and Computers** to open the **Default Domain Policy** and go to **Computer ConfigurationWindows SettingsSecurity SettingsRestricted Groups** :

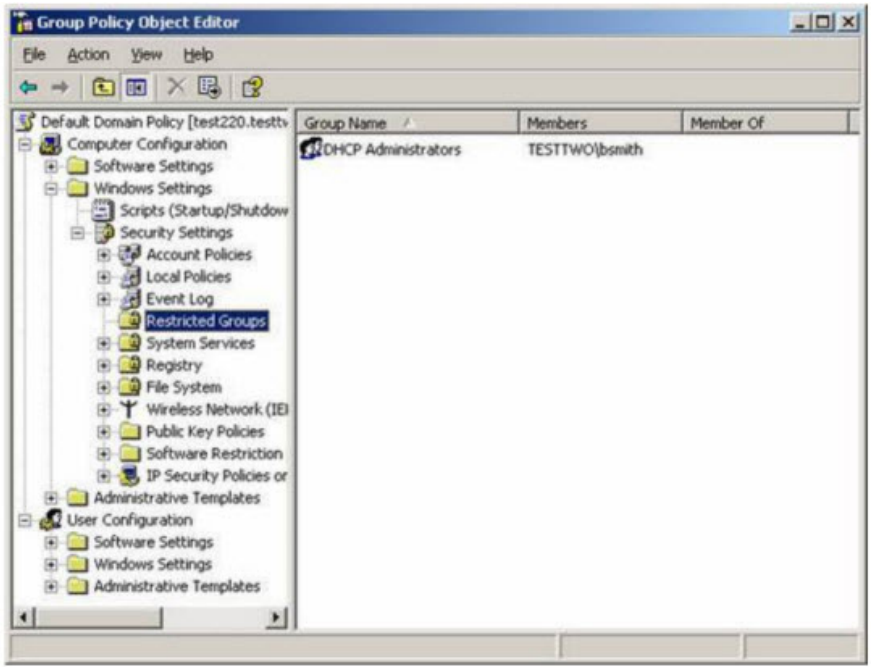


Right-click **Restricted Groups** and select **Add Group** , here we specify DHCP Administrators as the user group to monitor:

Click **OK** , select the **Add** button in the next properties table to specify which accounts are allowed to become members of the group.

Note that, even though the group has a member in it, you still have to take this step and identify each member of that group again:

Click **OK** and the DHCP Administrators group members are limited as desired (in this example, *Bob Smith* account):



What happens when we do the above step, every time Group Policy conducts refreshing of all domain controller members (usually 5 minutes every time) in the DHCP Administrators group checked, or due to a problem (malware) that an account number (here *Mary Smith*) when added to the group, then automatically deleted, event ID 637 will be logged Security log if you have enabled the feature manage and control accounts. And, members of the DHCP Administrators group will be monitored and managed as closely as possible.

Note that Windows 2000 comes with another account group called DHCP Users, which can be used to assign user accounts with read-only properties using a DHCP console, and members of this group. also controlled in the same way as Restricted Groups.

DNSUpdateProxy Group

On Windows networks, DHCP and DNS can work together to simplify the process of setting up and customizing network system operations. Usually, the most common problem is that the DHCP client registers a direct (host) record with the DNS server, while the pointer PTR is registered instead of the client by the DHCP server. This means that attacks on DHCP servers can control through the logs registered with the DNS server system and continue to be used to redirect traffic to bad websites, or cause the current Denial Of Service - DoS. If you 'turn the DHCP server' into a member of the DNSUpdateProxy group, your DHCP server will not lose ownership or data records of the client. These are mostly used when updating or upgrading from Windows NT to ensure that subordinate clients that do not support DNS can lose their ownership when upgrading to Windows 2000 or Windows XP.

The advantage of doing this is that you should only add the computer accounts of the DHCP server to the DNSUpdateProxy group if you intend to upgrade from previous versions of Windows 2000 to Windows 2000 or Windows XP. Another point to note is never add a DHCP server to the DNSUpdateProxy group if the DHCP server system is operating on the domain controller.

Fake DHCP Servers detection signs

Finally, we will show you some useful tools to detect suspicious signs of a fake DHCP server on the system so that it can be easily and easily prevented. Mostly we will use Microsoft 's combined tools and other third - party sources.

Dhcploc.exe

Dhcploc.exe is a tool with the command line interface, which is part of Windows Support Tools located in the *SupportTools folder* on the XP installation disc or here, and is used to display a list of all DHCP servers being activated. on the internal subnet system. Currently, Dhcploc.exe is still in use from Windows NT 4.0, with the mechanism by sending DHCPREQUEST messages, and displaying the DHCP server's IP address responding with DHCPACK. You can find the syntax used in the Help file when installing Support Tools on the system.

dhcp_probe

A research group - Princeton University's Network Systems Group developed a tool called dhcp_probe, capable of detecting DHCP and BOOTP servers via Ethernet. The previous version was built to work on Solaris 8 and SPARC with gcc, and a few patches to work on Linux. Depending on the operating system platform you are using, you can find the right tool on Network Systems Group page or download dhcp_probe directly here.

Good luck!