DNS protection for Windows (Part 1)

DNS is a fairly simple service, but protecting it is a problem that can stop your network infrastructure. Although DNS is a database of names and numbers, an attacker can also take advantage of the information gathered from the attack.

Derek Melber

DNS is a fairly simple service, but protecting it is a problem that can stop your network infrastructure. Although DNS is a database of names and numbers, an attacker can take advantage of the information gathered from attacking the database. Some attacks can get the information in the database and then use that information to destroy you. Some other attacks can fill information into the database, while trying to control DNS servers, some common solutions cannot be implemented. If you haven't been interested in attacking your DNS infrastructure, then this is what you need to know before it's too late.

Basics of DNS

DNS stands for Domain Naming Service, a service used to resolve IP addresses by names. The main purpose here is to understand the names we are talking about. When a name is instructed, DNS stores domain-related information. For example, Active Directory uses DNS to store domain names and computer names of computers on the network. If your domain is named policy.org and the first domain controller in the domain is PDC1 then you will have entries in DNS as shown in Figure 1.

Figure 1 : The first DNS entries for computers in your Active Directory domain

Note in the figure above that there is not only one entry for PDC1 but also an IP address that comes with PDC1 as XXXX The reason here is that there is an IP address that will have a name associated with it and translations Other services on the network will not use this name, rather this IP address. However, in terms of people, we

prefer names rather than their IP addresses. DNS has come up with a name solution for IP addresses. It can be configured with a reverse lookup zone, which will return the name when receiving the IP address.

DNS protection with Active Directory

One of the first decisions you need to make is the type of DNS database you will configure to support Active Directory domains. You can save information in a standard DNS database, which must have a primary DNS server with secondary DNS servers, or you can configure the DNS database as Active Directory integration as if shown in Figure 2.

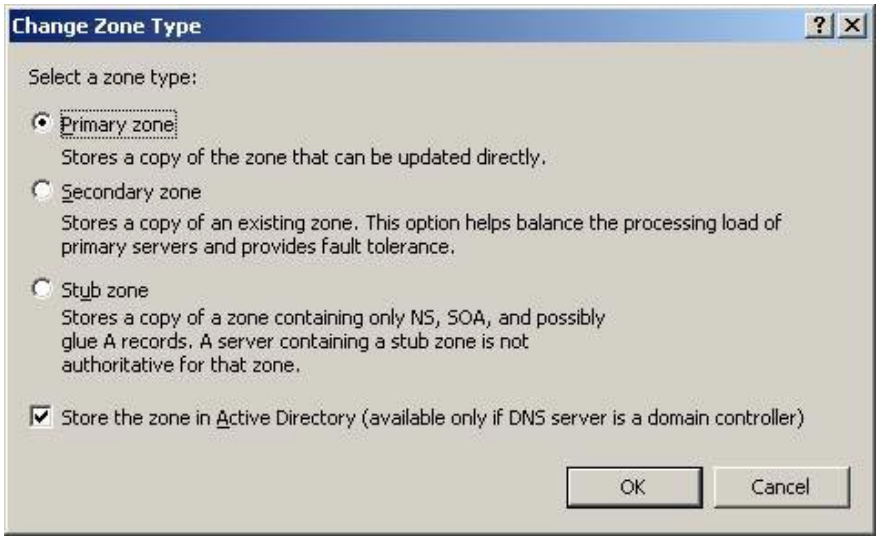


Figure 2 : DNS database can be integrated Active Directory

It is best to configure your DNS servers as Active Directory integrated when they are supporting Windows Active Directory, so you can take advantage of its advantages. You can also get some stability benefits for this type of DNS database, but here we want to focus on security aspects.

The main advantage you get from a DNS-based Active Directory is guaranteed dynamic updates, you can see the configuration in Figure 3. Dynamic updates are the main functions of DNS, functionality This allows domain computers to automatically register their names and IP addresses with DNS servers when they enter the network or change IP addresses through a DHCP server. This upgrade form reduces the difficulty of manually entering the name and IP address into the DNS database, an old method we used. The security aspect will need to be mentioned here is whether an automatic upgrade from a client to a DNS database can open the door for malicious code to enter. However, you can be assured that automatic updates will verify that the computer that is requesting the upgrade to the DNS server also has an entry in the Active Directory database. This means that only computers that are named in the Active Directory domain can update the DNS database automatically.

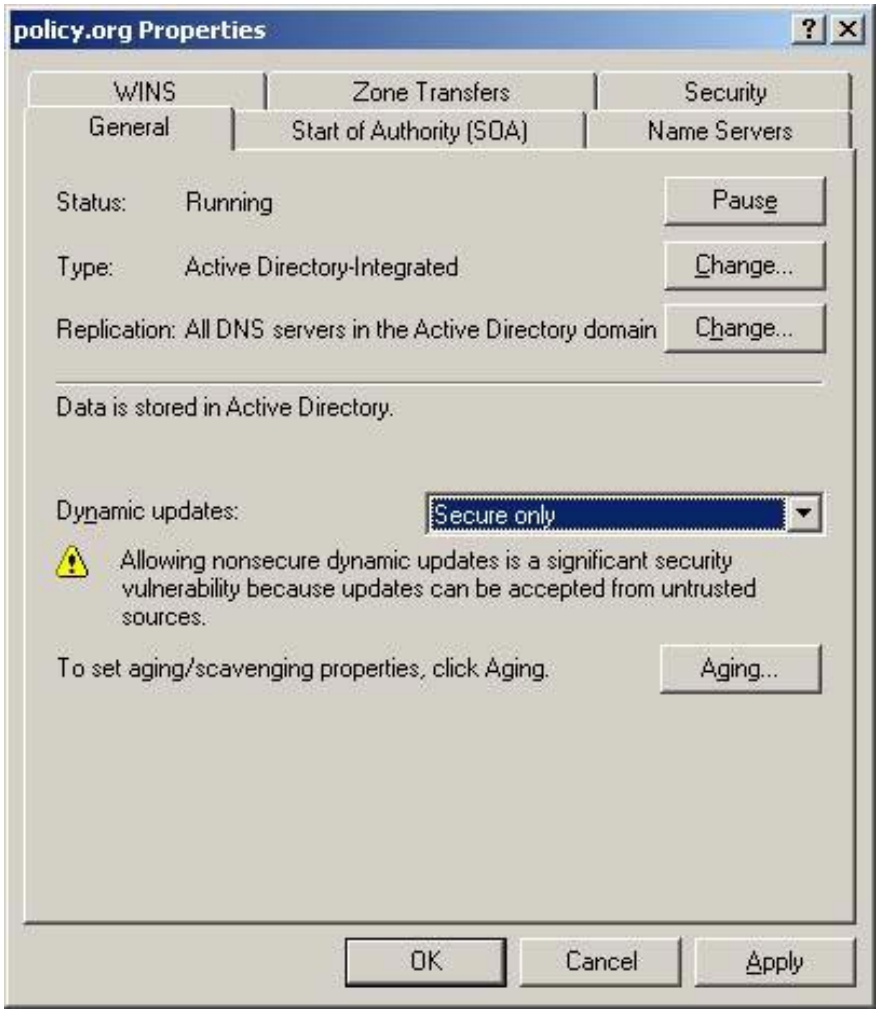


Figure 3: Active Directory integrates DNS database
Can be configured for safe dynamic upgrades

Perform dynamic upgrade with DHCP

One option you have in Windows is to be able to perform dynamic upgrades with DHCP for the client. This is not specified with Windows 2000 / XP / Server 2003 / Vista but it is specified with computers using Windows NT / 9x.

The DHCP server is the input controller, preventing other DHCP servers or clients to upgrade records in the future. To resolve this, add DHCP server accounts to the DNSUpdateProxy group, which will result in DNS for clients to have a secure Access Control Lists (ACLs) control list. The new ACL includes authenticated users who are able to update the DNS input for the client. This problem is designed for either another DHCP server or even the client can update future entries into DNS for the client.

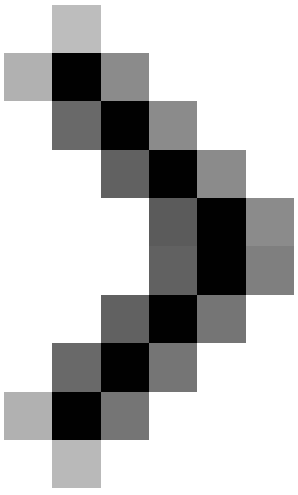
The security issue here is that the authenticated user has the ability to update the client, but there is another problem that may arise. If you install DHCP on a domain controller and then add this computer to the group, the result will be that all entries created by the domain controller have the same secure ACL. Entries of existing domain controllers are very sensitive to the security and stability of Active Directory, getting such entries is not interesting in security. with your organization. The entries will be exposed to all SRV (Service Resource

Records) to control the client and server to find Active Directory related services within the network. These services can be Kerberos, site, TCP, IP, and SRV records.

Therefore, the solution to this problem is not to install DHCP on domain controllers. If you have DHCP installed on domain controllers, it is best not to use a DHCP server to perform dynamic updates for the client. On the other hand, you edit the insecure settings within each referral given to domain controllers in DNS.

Conclude

As you can see, DNS is really simple, not a complex service. With the task of resolving names for IP addresses or vice versa, people will think that it is easy to configure and secure. However, there are some settings that will allow for more security and a more stable DNS environment. The first is the ability to create an integrated DNS database Active Directory that provides ongoing compatibility with Active Directory, as well as the ability to protect dynamic updates. These secure dynamic updates will help us combat the malicious code that infiltrates the DNS database because computers are not in the same domain. With these dynamic updates, you can have clients perform them on their own, or have DHCP perform them. If you choose to use DHCP and the DNSUpdateProxy group, you will need to make sure that this configuration is not exposed to domain controller inputs in DNS. The easiest solution to this is to prevent domain controllers from performing DHCP. In the next section of this article, we will introduce detailed settings that you can perform in DNS to protect DNS databases and services for your network.



DNS protection for Windows (Part 2)

tips and guides. Thank you for reading and for following us regularly.