Checklist: Secure Your DNS Server

Applies To: Windows Server 2008, Windows Server 2008 R2

Especially in the case of Internet-facing Domain Name System (DNS) servers, it is important to ensure that your DNS infrastructure is protected from attack from outside—or even inside—your organization. You can configure your DNS server, when it is integrated with Active Directory Domain Services (AD DS), to use secure dynamic updates to prevent unauthorized modifications to DNS data. You can take additional steps to reduce the chances of an attacker being able to compromise the integrity of your DNS infrastructure.

|  |  |
| --- | --- |
| **Task** | **Reference** |
| Determine which DNS security threats are most significant to your environment, and determine the level of security that is required. | [Security Information for DNS](https://technet.microsoft.com/en-us/library/cc755131(v=ws.11).aspx) |
| To help prevent anyone outside your company from obtaining internal network information, use separate DNS servers for internal and Internet name resolution. Your internal DNS namespace should be hosted on DNS servers behind the firewall for your network. Your external, Internet DNS presence should be managed by a DNS server in a perimeter network. To provide Internet name resolution for internal hosts, you can have your internal DNS servers us a forwarder to send external queries to your external DNS server. Configure your external router and firewall to allow DNS traffic between your internal and external DNS servers only. | [Understanding Forwarders](https://technet.microsoft.com/en-us/library/cc730756(v=ws.11).aspx);  [Using Forwarders](https://technet.microsoft.com/en-us/library/cc754931(v=ws.11).aspx) |
| For the DNS servers in your network that are exposed to the Internet, if zone transfer must be enabled, restrict DNS zone transfers to either DNS servers identified in the zone by name server (NS) resource records or to specific DNS servers in your network. | [Modify Zone Transfer Settings](https://technet.microsoft.com/en-us/library/cc771652(v=ws.11).aspx) |
| If the server running the DNS Server service is a multihomed computer, restrict the DNS Server service to listen only on the interface IP address that is used by its DNS clients and internal servers. For example, a server acting as proxy server may have two network adapters, one for the intranet and one for the Internet. If that server is also running the DNS Server service, you can configure the service to listen for DNS traffic only on the IP address that the intranet network adapter uses. | [Configuring Multihomed Servers](https://technet.microsoft.com/en-us/library/cc772564(v=ws.11).aspx);  [Restrict a DNS server to listen only on selected addresses](https://technet.microsoft.com/en-us/library/cc755068(v=ws.11).aspx) |
| Ensure that default server options that secure the caches of all DNS servers against names pollution—have not changed. Names pollution occurs when DNS query responses contain nonauthoritative or malicious data. | [Secure the Server Cache Against Names Pollution](https://technet.microsoft.com/en-us/library/cc772349(v=ws.11).aspx) |
| Allow only secure dynamic updates for all DNS zones. This ensures that only authenticated users can submit DNS updates using a secure method, which helps prevent the IP addresses of trusted hosts from being hijacked by an attacker. | [Understanding Dynamic Update](https://technet.microsoft.com/en-us/library/cc771255(v=ws.11).aspx);  [Allow Only Secure Dynamic Updates](https://technet.microsoft.com/en-us/library/cc753751(v=ws.11).aspx) |
| Disable recursion on DNS servers that do not respond to DNS clients directly and that are not configured with forwarders. A DNS server requires recursion only if it responds to recursive queries from DNS clients or if it is configured with a forwarder. DNS servers use iterative queries to communicate with each other. | [Disable Recursion on the DNS Server](https://technet.microsoft.com/en-us/library/cc771738(v=ws.11).aspx) |
| If you have a private, internal DNS namespace, configure the root hints on your internal DNS servers to point only to the DNS servers that host your internal root domain and not the DNS servers that host the Internet root domain. | [Updating Root Hints](https://technet.microsoft.com/en-us/library/cc754568(v=ws.11).aspx);  [Update Root Hints on the DNS Server](https://technet.microsoft.com/en-us/library/cc730735(v=ws.11).aspx) |
| If the server running the DNS Server service is a domain controller, use Active Directory access control lists (ACLs) to secure access control of the DNS Server service. | [Modify Security for the DNS Server Service on a Domain Controller](https://technet.microsoft.com/en-us/library/cc771921(v=ws.11).aspx) |
| Use only AD DS-integrated DNS zones. DNS zones that are stored in AD DS can take advantage of Active Directory security features, such as secure dynamic update and the ability to apply AD DS security settings to DNS servers, zones, and resource records.  If a DNS zone is not stored in AD DS, secure the DNS zone file by modifying permissions on the DNS zone file or on the folder where the zone files are stored. The zone file or folder permissions should be configured to allow Full Control only to the System group. By default, zone files are stored in the %systemroot%\System32\Dns folder. | [Understanding Active Directory Domain Services Integration](https://technet.microsoft.com/en-us/library/cc726034(v=ws.11).aspx);  [Configure a DNS Server for Use with Active Directory Domain Services](https://technet.microsoft.com/en-us/library/cc732284(v=ws.11).aspx) |