Best Practices for Administering DNS Server

Updated: May 9, 2008

Applies To: Windows Server 2008

The following best practices ensure trouble-free operations when you use them to administer Domain Name System (DNS):

* **Configure the DNS server to use a static IP address**   
    
  If you configure the DNS server to use dynamic addresses that are assigned by Dynamic Host Configuration Protocol (DHCP), when the DHCP server assigns a new IP address to the DNS server, the DNS clients that are configured to use that DNS server's previous IP address will not be able to resolve the previous IP address and locate the DNS server.
* **Be conservative in adding alias records to zones.**   
    
  Avoid using alias (CNAME) resource records where they are not needed to map a host name that is used in a host (A) resource record. Also, ensure that any alias names that you use are not used in other resource records.  
    
  For more information, see [Managing Resource Records](https://technet.microsoft.com/en-us/library/cc794723(v=ws.10).aspx).
* **When you design your DNS network, use standard guidelines and, wherever possible, follow preferred practices for managing your DNS infrastructure.**   
    
  DNS was designed to provide a level of fault tolerance for resolving names. If possible, you should have at least two DNS servers hosting each zone.
* **If you are using Active Directory® Domain Services (AD DS), use directory-integrated storage for your DNS zones for increased security, fault tolerance, and simplified deployment and management.**   
    
  By integrating DNS zones with AD DS, you can simplify network planning. For example, when you use Active Directory-integrated DNS, domain controllers for each of your Active Directory domains correspond in a direct one-to-one mapping to DNS servers. This can simplify the planning and troubleshooting for DNS and Active Directory replication problems because the same server computers are used in both topologies.  
    
  If you are using directory-integrated storage for your zones, you can select from the different replication scopes that replicate your DNS zone data throughout the directory. You can select replication scopes that replicate your DNS zone data to all DNS servers in the Active Directory forest, all DNS servers in a specified Active Directory domain, or all domain controllers that are specified in a custom replication scope.  
    
  For more information about directory-integrated DNS zone storage and replication options, see [Managing Server Integration with AD DS](https://technet.microsoft.com/en-us/library/cc816658(v=ws.10).aspx).  
    
  Any DNS server that hosts a directory-integrated zone is a primary DNS server for that zone. This enables a multimaster model in which multiple DNS servers may update the same zone data. A multimaster model eliminates a single point of failure that might be associated with a conventional, single-master DNS topology, in which only a single DNS server may update the data for a given zone.  
    
  One of the important benefits of directory integration is the support for secure dynamic update of the names within a zone. For more information, see. [Managing Dynamic Update for a Zone](https://technet.microsoft.com/en-us/library/cc794806(v=ws.10).aspx).
* **Enter the correct e-mail address of the person who is responsible for each zone that you add to or manage on a DNS server.**   
    
  Applications use this field in the start of authority (SOA) resource record to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. While most Internet e-mail addresses contain the “at” symbol (@) in e-mail applications, this symbol must be replaced with a period (.) when an e-mail address is entered for this field. For example, instead of "administrator@microsoft.com", use "administrator.microsoft.com".  
    
  For more information about configuring the identity of a person who is responsible for a zone, see [Modify the Start of Authority (SOA) Resource Record for a Zone](https://technet.microsoft.com/en-us/library/cc816941(v=ws.10).aspx).