DNS Requirements for Complex AD DS Environments

AD DS requires DNS to function correctly, and implementing DNS in a multidomain or multiforest environment requires an extra level of planning.

When deploying a DNS structure to support a complex AD DS environment, you will need to address several important configuration areas:

- Verify the DNS client configuration. Configure all computers in the AD DS domain with at least two addresses of functional DNS servers. All computers must have good network connectivity with DNS servers.
- Verify and monitor DNS name resolution. Verify that all of your computers, including domain controllers, are able to perform successful DNS lookups for all domain controllers in the forest. Domain controllers need to be able connect to other domain controllers to successfully replicate changes to AD DS. Client computers need to be able to locate domain controllers by using service (SRV) resource records, and need to be able the resolve the domain controller names to IP addresses. In a multidomain or multiforest environment, client computers may need to locate domain computers in any domain to validate trusts when accessing resources in another domain.
- Optimize DNS name resolution between multiple namespaces. When organizations deploy multiple trees in an AD DS forest, or when they deploy multiple forests, name resolution is more complicated because you need to manage multiple domain namespaces. Use DNS features such as conditional forwarding, stub zones, and delegation to optimize the process of resolving computer names across the namespaces.
- Use AD DS integrated DNS zones. When you configure a DNS zone as AD DS integrated, the DNS information is stored in AD DS and replicated through the normal AD DS replication process. This optimizes the process of replicating changes throughout the forest. You can also configure the scope of replication for the DNS zones. By default, domain-specific DNS records will be replicated to other domain controllers that are also DNS servers in the domain. DNS records that enable cross-

domain lookups are stored in the _msdcs.forestrootdomainname zone and are replicated to domain controllers that are also DNS servers in the entire forest. This default configuration should not be changed.