微软学习：关于DNS的不完全总结 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/140/2021_2022__E5_BE_AE_E8_BD_AF_E5_AD_A6_E4_c100_140112.htm 几年前第一次接触到活动目录的时候，正是领导要求部署活动目录的时候。虽然当时手头上有几本书，但是时间紧迫没有来得及仔细研究。边看着帮助边运行dcpromo就开始活动目录的部署了，相信不少人和我当年差不多，稀里糊涂的就开始当起了活动目录的管理员。对于DNS，因为安装会提示自动部署，相信很多人都不会在这方面下很多功夫（包括我原来也是）。我为此付出了不少代价——因为不懂DNS所以遇到DNS的问题不知如何解决。我通过对论坛上的帖子和参考书的阅读，加上自己经验的总结得出一些操作方面的结论和总结。希望对大家能有所帮助。 有过DNS域部署经验的朋友都能感觉到，活动目录的DNS、DHCP和WINS（用的不多了）和NetBios是息息相关的。也是很容易混淆的。所以很麻烦，通常我们开始部署AD的时候是在一个小公司里，大约有几十台电脑的局域网。人员流动不是很频繁，所以的电脑也差不多的天天都开。很少有电脑会换地方，我们全都使用DNS的默认配置就可以很少会出问题。但这样的地方我们不能待一辈子，我们来到一个相对复杂的网络环境时，意识到自己缺乏对DNS的起码常识，怎么办？ 为了在遇到难题时能正确表述自己的问题（否则别人想帮你都没办法，除了UP我们更重要的是说清楚自己的问题和听明白高手的意思）那么和我一样从基础开始吧。 什么样的DNS系统是一个比较完美的系统呢？DNS服务器的连续性能提供出色的性能，减少WAN的通信，安全性

也必须得到保障。我们先从概念开始。 1．DNS和活动目录关系 DNS定义“ 命名空间 ”（名字空间）－－－微软把例如“ contoso.com ”的东东叫命名空间，这个空间内的主机储存在一个“ 区域文件 ”（zone file）里－－－主要是一种映射的关系（中学数学就有映射的概念） 活动目录的域（domain）“ 存储域和域中的对象 ”，把用户、租计算机帐户记录组注册表的SAM里。－－－当然域不止这些内容。 DNS和域的结合－－完全合格域名（FQDN）：例如srv1.contoso.com－－说明了srv1主机位于contoso.com这个域里面。 注意： DNS的结构中，顶级域com.的末尾是有一个句点.的。DNS解析器是从左到右解析FDQN（看看上面FDQN的例子）的，最后到“ . ”结束。因为windows的DNS会自动在末尾添加“ . ”所以我们很容易忘了它的存在，在我们检测DNS（尤其是命令行方式）最好加上末尾的这个.正因为根域上有这个点，所以我们在林根的DNS上设置转发的时候会发现那个转发器的选现是灰的，不让你设置，因为.认为自己是根了，没必要转发。所以解决的方法是删掉这个点，才能转发（删掉后就不会灰色可以选择转发了）。 如果没有行政方面的要求你完全可以在域里使用例如devil.coco的域名称，不一定非要.net或者.com.即使父域叫contoso.com，子域也可以叫devil.coco。 当一个企业在做DNS规划时要注意。当企业外部服务（例如网站）需要在internet上注册名称（例如，公司.com）。如果企业内部使用活动目录，那么要使内外部使用不同的名字或者内部的活动目录使用外部名称的一个子域。例如：“ contoso.com ”，作为企业在internet上的网站，使用www.contoso.com域名。内部的域可以使用contoso.net或

者corp.contoso.com作为DNS名。如果不这么做将有可能使内部和外部名称空间出现重叠。客户端登陆域或访问internet都将可能产生问题。尤其当涉及网络地址转换 (NAT) 并且外部 IP 地址处于内部客户端够不到的范围中时就会有麻烦了(了解NAT 的 人应该知道,如果客户端不配置可以正确解析外部地址的DNS是无法访问相关网站的.)。 DNS和活动目录使用各自不同的数据库解析名字。关于这一点我觉得对于实际操作意义不大所以不说了有兴趣的看看上面提到的那个帖子。2．hosts文件 很多帖子里都有人回复说，看看那个hosts文件有没有问题，或者说修改那个hosts文件里的什么地方（例如屏蔽QQ）。这是为什么？ hosts存在的目的：减少DNS服务器的工作量，如果客户端查找的一个主机名在hosts文件里有记录（说明不久前访问过），那么客户端就不必找DNS服务器了直接就知道了该主机的IP。我们可以用记事本打开hosts文件。找不到？一般在这里C:\WINDOWS\system32\drivers\etc这里除了hosts还有好几个文件，也能用记事本打开。都是和TCP/IP相关的，详细我就不说了跟DNS关系不大。 TTL（生存时间），DNS记录必须有TTL，Hosts中得缓存超过了ttl就将被删除，否则DNS得改变将无法在hosts文件中体现。 我们需要一个具体的例子： 有天，客户发现srv1.contoso.com主机无法访问了，我们查看DNS表，发现确实没有相关A记录了。我们手动添加了记录，但是客户还是抱怨无法访问该主机——因为客户端的缓存里里，还是认为该主机无法访问。这时我们就必须在客户的电脑上运行ipconfig/ flushdns 来清除缓存信息。是的，服务器也有缓存。服务器清理缓存的命令是dnscmd /clearcache 3．主DNS服务器和辅助名称服务器 这个

概念在论坛上也无数次的被提起，我觉得还是有必要说明一下的。照例我不会用很专业的词汇，需要考MCSE的朋友最好不要看我写的东西。 我是这样认为的，DNS服务器把所有资源记录到一个文件中（zone file）。只有“ 主DNS服务器 ”能对该文件进行写操作（能修改DNS记录），辅助DNS服务器从主DNS服务器（或者其他辅助DNS服务器）那里获得该文件的拷贝（默认24小时得不到拷贝的话，辅助DNS服务器就将失效）。 除此之外还有一种“ 仅缓存名称服务器 ”（caching－only name server），它上面仅保存缓存的查询结果（从辅助DNS服务器那里获得），以便使客户端尽快获得查询信息。 这种机制让人想起NT时代的主域控制器和备份域控制器——当然这是一种脆弱的机制。微软为了能多凑合一些时间，允许任何运行DNS的DC都能被设置为它所在域的主DNS服务器。 