简单谈谈windowsServer2008的NAP到底是什么Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/581/2021_2022__E7_AE_80_E5_8D_95_E8_B0_88_E8_c100_581202.htm 什么是NAP？ NAP-Network Access Protection，网络访问保护。我觉得其实还不完整，我认为完整的应该叫做网络策略访问保护。他的作用是用策略来保护客户端对网络的访问，确保整个网络的访问过程是达到一定安全级别的。07年初前我开始做08的时候，当时的第一反应就是防火墙。觉得是不是就是跟防火墙类似的一个东西。后来发现不是的，而且完全不一样。防火墙是通过网络的通讯接口，比如IP、端口号之类的来控制访问连接的通或者断。简单理解防火墙是控制网络行为的，而NAP是通过安全策略来控制网络中所有客户端的状态。可能这么说，还是不够清楚。我觉得这个东西应该分开来看，就是网络-策略-访问-保护。 下面先来看看网络。对于NAP的网络我们理解，可以大致分为三类：一个外网，也就是没有受NAP管理的网络。这个网络可能是互联网，也可能是某个个刚刚通过无线网络想想接入到网络中的某个计算机，这是因为他还在处于一个请求IP或者请求接入的阶段，所以它应该算外部网络；第二个是内网，也就是受NAP管理的网络。这个网络指的就是我们已经接入进来的这些内部计算机，比如刚才那个计算机如果已经接入进来了以后，那它现在就处于一个内部网络当中；最后一个是一个比较特殊的网络，有点防火墙术语当中的DMZ，但还是有区别。它是一个更偏向内网的网络，但又不全是。当然你可以去定义它，如果有客户端被NAP放到了这个网络，那它也许只能访问部分网络资

源，也许什么资源都不能访问。后面我们再来详细描述这个网络，暂时我们就先理解为一个受限制网络吧。 网络分析完了，在来讲讲策略。NAP中的策略叫做安全策略，可能有人会跟防火墙中的策略去做对比。那么防火墙中的策略准确说应该叫规则策略，比如如果是某个人，在某台机器上，通过某个应用程序进行访问，那么我们可以决定是否允许通过。这个规则策略可能是允许用户A通过，B不能通过，或者允许A程序能够通过而B程序不能通过。但NAP中的安全策略是用于验证客户端是否达到某个在安全方面的特性的要求。比如在NAP中，有的策略是要求客户端是否打开安全更新设置，有的是要求防火墙是否处于启用状态，有的是要求系统补丁是否打到某个级别或者某个时间点之后，有的是要求防病毒软件的病毒库是否达到某个特定版本或者某个最新的时间点，等等。可以看出来实际上策略就是一把尺，在防火墙中它是通过规则来定义这把尺，在NAP中它是通过跟安全相关的状态或者叫属性来定义这把尺。有了这把尺，我们才能在后面的过程中去衡量一个客户端或者网络中的某个因素是否达到我们所期望的要求。这就是策略的作用。 好，有了一把尺，如果我们不用它，也是白费，下面就来说说访问的问题。我的理解应该叫访问监控或者访问验证。这里的意思是用刚才的那个些安全策略，去监控所有网络中的客户端，去跟客户端当前的状态进行对比。比如一个策略是要求病毒库的版本必须要达到2.0版本，结果发现有一台计算机的病毒库版本还是1.8，那这个时候NAP服务器就会将这台计算机标记为“ 不符合 ”。也就是说，访问验证的过程就是用策略去对比客户端的状态信息是否符合我们所定义的策略。强调一下，

这个验证过程是实时存在的，也就是说，一旦你修改了某些安全设置，与NAP中的策略是相矛盾的，那么会立即将你标记成“ 不符合 ”。反过来，如果当你更新了某些配置，比如病毒库版本时，NAP会立即将你从“ 不符合 ”标记成“ 符合 ”。这种实时保护，就是为了防止恶意连接在开始进入网络时通过伪装蒙混过关，进入以后再开始进行破坏。据我所知，像VPN的很多应用就是这样，它只在网络连接开始的时候进行验证，一旦通过验证，以后的任何操作将不再受到限制。 所有的计算机都有了一个“ 符合 ”或者“ 不符合 ”的标记，最后我们就能够简单的对其进行控制了。实际上这个过程很简单，就是定义一个规则，如果是“ 符合 ”的，我们允许它连入到哪个网，不允许他连入到哪个网。如果是“ 不符合 ”的，我们又允许它连入到哪个网，不允许他连入到哪个网。 案例展示 最后我们举个例子来看看整个NAP的工作流程是怎样完成的。就拿刚才那个病毒库为1.8版本的计算机为例。首先，他会通过有线或者无线网络接入进来，在没有连入进来之前，它对于NAP来说应该是一个外网，而他现在请求进入NAP的内网，NAP就开始工作了。 NAP中定义了一条病毒方面的安全策略，要求“ 病毒库版本必须达到2.0 ”。这时NAP的策略服务器将会对这个客户端进行验证，结果发现其版本为1.8，所以最后给这台计算机标记了一个“ 不符合 ”。 NAP这时启动保护规则，其中定义了一条规则是“ 不符合病毒策略的计算机，将被指派到一个只允许访问病毒更新服务器的受限制网络中 ”。这时，这个客户端会发现，他能够访问的只有这台病毒服务器。言下之意，就是说，如果你的病毒不符合现在的策略要求，我就只允许你连接到病毒服务

器，将病毒库更新到所要求的版本。 最后，客户端通过连接病毒服务器，将病毒库版本更新至2.0。我们刚才说过，NAP是实时监控的，所以这个时候，这台机器的“ 不符合 ”标记，会立即改为“ 符合 ”。 这个时候NAP的保护规则定义了“ 符合 ”的客户端允许访问内部网络中的所有的服务器或数据资源。也就是说，直到这个时候，这个客户端才能真正的进入到企业网络中去访问资源。 再次强调，这个时候不能叫做NAP完成了验证过程，因为它是实时监控的。如果你这个时候将病毒软件卸载了，那你同样会被立即断开网络。至于对于一个没有安装某个防病毒软件的客户端，该如何处置，那就取决于你的安全策略和访问规则怎么设置了。 特殊功能：强制保护 说到这里，我想大家应该对NAP是怎么回事。另外，我在提一个NAP里面的一个特殊的功能，叫做强制保护。说它特殊，是因为目前并不是所有的安全策略或访问规则都支持这个功能的。目前微软自己的安全设置肯定是支持强制保护的，比如防火墙设置，自动更新设置等等。但一些其他厂商的应用，比如某个厂商的防火墙、防病毒软件，由于现在2008中的NAP才刚刚起步，可能目前的版本还不能够支持这个强制保护的功能。那强制保护到底怎么回事呢，下面还是举例来说明吧。 拿刚才那个举例来说，他现在可以正常连接到内部网络当中。而NAP中有另外一条跟防火墙有关的策略，这个安全策略定义的是“ 必须开启防火墙 ”。而这时这个客户端的用户发现防火墙把某些端口给阻断了，他希望能够使用一些特殊的软件，比如BT之类的。可能他的权限足够，所以自己就把防火墙给关闭了。 这个时候，按照我们刚才所说的，这个客户端会立即打上一个“ 不符合 ”的标记并

且被断网，或者分配到某个受限制网络中。但是这里如果启用了强制保护的话，我们会发现网络并没有发生变化，用户再次打开防火墙设置的时候会发现，明明刚才把防火墙关掉了，怎么现在还是开的。并且多次尝试，都是这种现象。其实，这就是强制保护，或者叫强制符合策略。如果支持这个功能的安全组件，会自动的将客户端的安全配置修改成安全策略所要求的那样。正是因为需要自动执行，所以目前并不是所有的安全组件都能支持的，比如第三方防病毒软件这种，就需要第三方厂商跟微软来合作才可能实现。 好了，说到这里，相信大家应该对NAP有一个比较清晰的认识了，至少知道NAP是怎么一回事，以及它怎么工作的。如果有兴趣继续深入研究的话，可以去微软网站查阅相关的信息。 