11.5.2 主机基线

使用主机基线并不意味着你必须要在网络上测试每台主机。主机基线只需要在高流量或关键任务服务器上执行。基本上，一旦某台服务器运行缓慢，便会招来管理层愤怒的电话，你应当在那台主机上建立基线。

主机基线包含以下几个组件。

1．使用的协议

当捕获这台主机的流量时，这个基线提供了使用协议分层统计窗口的好机会。然后，你可以对照看一看是否缺少本应出现的协议，或者主机上是否出现了新的协议。你也可以在协议的基础上，用它来发现高于正常数量的特定类型的流量。

2．空闲/繁忙流量

这个基线只是简单包含了高峰和非高峰时段正常操作流量的总体捕获记录。了解到一天之中不同时段的连接数量及其占用的带宽大小，有助于你确定缓慢是用户负载还是其他原因造成的。

3．启动/关闭

为了获取这个基线，你需要在主机启动和关闭时创建一个流量捕获记录。一旦计算机不能启动、不能关闭，或这两个过程异常缓慢，你就可以使用它确认问题是否跟网络有关。

4．身份验证序列

这个基线要求在主机上捕获所有服务的身份验证过程的流量。身份验证通常是服务运行缓慢的一个方面。通过基线你可以确认身份验证是否是通信缓慢的原因。

5．关联/依赖

这个基线需要持续更长时间的捕获，以确定这台主机依赖于哪些主机（以及哪些主机依赖于这台主机）。你可以通过会话窗口（**Statistics->Conversations**）查看这些关联和依赖。Web 服务器依赖于 SQL 服务器便是这样的例子。有时我们会意识不到主机间的一些潜在依赖关系，这时主机基线便能派上用场。通过这个，你可以确定主机不能正常运转，是因为配置错误还是因为所依赖主机的高延迟。