11.5 网络基线

当所有的努力都失败时，网络基线将成为检修网络缓慢故障最关键的数据之一。对我们的目的而言，网络基线包含来自网络不同端点的流量样本，包括大量我们认可的「正常」网络流量。网络基线的作用是在网络或设备工作不正常时作为比较的基准。

例如，考虑一个场景，网络上几个客户反映登录某个本地 Web 应用服务器时反应迟钝。如果你捕获这些流量并与网络基线对照，就会发现 Web 服务器一切正常，但嵌入到 Web 应用中的外部内容引发了额外的外部 DNS 请求，而这些请求比正常速度慢两倍。

也许不靠网络基线的帮助，你也能注意到异常的外部 DNS 服务器，但当你处理微妙的变化时，就不一定了。10 个 DNS 请求都比正常情况多耗费 0.1s，这跟一个 DNS 请求比正常多耗费 1s 一样糟糕，但没有网络基线的话，检测前者要难得多。

由于网络各不相同，因此网络基线的组件将有很大差异。接下来的几节提供了网络基线组件的几个例子。你也许会发现所有这些条目都能应用到你的网络基础设施，或只是很少一部分能适用。不管怎样，你应该把你的基线中的每一个组件置入这 3 个基本基线目录中：站点、主机和应用程序。