

WSA积极监控性能使用SNMP

目录

[简介](#)

[哪些值可以通过SNMP监控工具观察为了主动地监控思科WSA的性能？在阈值警报应该配置什么级别？](#)

简介

本文描述积极监控性能思科Web安全工具(WSA)有简单网络管理协议(SNMP)的。

哪些值可以通过SNMP监控工具观察为了主动地监控思科WSA的性能？在阈值警报应该配置什么级别？

当您监控思科WSA时，SNMP轮询的最重要的项目如下：

- 客户端的要求/第二
cacheThruputNow (.1.3.6.1.4.1.15497.1.2.3.7.1.1)在最后一刻的请求吞吐量
- 响应时间
cacheTotalRespTimeNow (.1.3.6.1.4.1.15497.1.2.3.7.9.1)在最后一刻的缓存总响应时间
- CPU 使用情况
cacheBusyCpuUsage (.1.3.6.1.4.1.15497.1.2.3.1.5)CPU的百分比忙时

注意： WSA的SNMP管理信息库(MIB)文件可以在[思科Web安全产品支持页面](#)找到。

因为每用户环境变化，推荐搜集基准生产统计资料在集合时期为了发现在基准期限，是否有任何外围之物。在此基准期间，注意期限，当客户端的要求/第二时其中最大化。如果有在响应时间和可能性CPU使用情况的一对应的猛烈增加，这可能代表在此特定环境的峰值性能。应该执行进一步测试和监听为了确认此最高标准。

在基准以后期限流逝了，并且特定最大峰值在客户端的要求/second未被观察，是推荐人工地设置阈值为10%到25%最高的被观察的客户端的要求/警告的目的秒钟。

除监听性能和警告在特定被超出的阈值外，思科WSA可能也配置发送在这些硬件情况的SNMP陷阱：

默认情况下启用

- RAID状态变化
- 风扇故障
- 高温
- 关键有效期
- link down
- 链路开启
- 电源状态崔凡吉莱
- 更新失败

- 上行代理失败

默认情况下禁用

- 连通性故障
- 超出的CPU利用率
- 超出的存储器利用率

如果需要检查特定代理CPU使用情况，[使用SNMP](#)，请查看[在WSA的计算的代理CPU利用率](#)。