

WSA积极监控性能使用SNMP

Contents

[Introduction](#)

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

Introduction

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

哪些值可以通过SNMP监控工具观察为了主动地监控Cisco WSA的性能？在阈值戒备应该配置什么级别？

当您监控Cisco 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)在最后一刻的高速缓冲存储器总响应时间
- 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

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

因为每个用户环境变化，推荐搜集基准生产统计资料在集时期为了发现在基准周期，是否有任何外围之物。在此基准期间，请注释周期，当客户端的要求/秒钟时其中最大化。如果有一个对应的猛烈增量及时响应时间和潜在的CPU使用情况，这在此特定环境里可能表示峰值性能。应该进行进一步测试和监控为了确认此最高标准。

在基准以后周期流逝了，并且没有特定最大峰值在客户端的要求/second被观察了，是推荐人工地设置门限值为10%到25%最高的被观察的客户端的要求/警告的目的秒钟。

除监控性能和警告在特定被超出的阈值外，可能也配置Cisco WSA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
- 关键到期
- 下来链路
- 链路
- 电源状态变化

- 更新故障
- 上行代理故障

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](#)。