

# 使用SNMP主動監控WSA的效能

## 目錄

### [簡介](#)

[為了主動監控Cisco WSA的效能，可以通過SNMP監控工具觀察哪些值？應在什麼級別配置閾值警報？](#)

## 簡介

本檔案介紹使用簡易網路管理通訊協定(SNMP)主動監控思科網路安全裝置(WSA)的效能。

## 為了主動監控Cisco WSA的效能，可以通過SNMP監控工具觀察哪些值？應在什麼級別配置閾值警報？

監控Cisco WSA時，SNMP輪詢最重要的專案如下：

- 每秒客戶端請求數  
cacheThruputNow(.1.3.6.1.4.1.15497.1.2.3.7.1.1)最後一分鐘的請求吞吐量
- 響應時間  
cacheTotalRespTimeNow(.1.3.6.1.4.1.15497.1.2.3.7.9.1)快取上一分鐘的總響應時間
- CPU使用率  
cacheBusyCpu使用率(.1.3.6.1.4.1.15497.1.2.3.1.5)CPU的忙碌時間百分比

附註：WSA的SNMP管理信息庫(MIB)檔案可在[Cisco Web Security產品支援頁面上找到](#)。

由於每個客戶環境都各不相同，因此建議收集一段時間內的基線生產統計資訊，以便檢視基線期間是否有任何異常值。在此基線期間，請注意客戶端每秒請求的最大化時段。如果響應時間和潛在CPU使用率出現相應的急劇增加，則可能代表此特定環境中的峰值效能。應執行進一步的測試和監控以確認該最高水準。

在基線時段過去之後，並且在客戶端請求中並未觀察到特定的最大峰值/秒，建議為警報目的人為設定最高觀察到的客戶端請求的10%到25%的閾值。

除了監控效能和發出特定超出閾值的警報外，還可以將Cisco WSA配置為在以下硬體條件下傳送SNMP陷阱：

### 預設啟用

- RAID狀態更改
- 風扇故障
- 高溫
- 金鑰過期
- 連結關閉
- 連結啟動
- 電源狀態更改
- 更新失敗

- 上游代理失敗

預設情況下禁用

- 連線故障
- 超出CPU使用率
- 超出記憶體使用率

如果需要檢查特定代理CPU使用情況，請檢視[使用SNMP計算WSA上的代理CPU利用率](#)。