

Proaktive Überwachung der WSA-Leistung mithilfe von SNMP

Inhalt

[Einführung](#)

[Welche Werte können über ein SNMP-Überwachungstool beobachtet werden, um die Leistung der Cisco WSA proaktiv zu überwachen? Auf welcher Ebene sollten Schwellenwertwarnungen konfiguriert werden?](#)

Einführung

In diesem Dokument wird die proaktive Überwachung der Leistung der Cisco Web Security Appliance (WSA) mit Simple Network Management Protocol (SNMP) beschrieben.

Welche Werte können über ein SNMP-Überwachungstool beobachtet werden, um die Leistung der Cisco WSA proaktiv zu überwachen? Auf welcher Ebene sollten Schwellenwertwarnungen konfiguriert werden?

Wenn Sie die Cisco WSA überwachen, sind die wichtigsten Elemente für das SNMP Polling:

- Client-Anfragen/Sekunde
cacheThruputNow (.1.3.6.1.4.1.15497.1.2.3.7.1.1)Anforderungsdurchsatz in letzter Minute
- Reaktionszeit
cacheTotalRespTimeNow (.1.3.6.1.4.1.15497.1.2.3.7.9.1)Gesamtantwortzeit des Cache in letzter Minute
- CPU-Auslastung
cacheBusyCPUUsage (.1.3.6.1.4.1.15497.1.2.3.1.5)Prozentsatz der Arbeitszeit der CPU

Hinweis: SNMP Management Information Base (MIB)-Dateien für WSA finden Sie auf der [Support-Seite für Cisco Web Security-Produkte](#).

Da jede Kundenumgebung variiert, wird empfohlen, über einen bestimmten Zeitraum hinweg grundlegende Produktionsstatistiken zu erfassen, um festzustellen, ob es während des Ausgangszeitraums zu Ausreißern kommt. Beachten Sie während dieser Baseline Zeiträume, in denen Kundenanfragen/Sekunden maximiert werden. Wenn die Reaktionszeit und die potenzielle CPU-Auslastung entsprechend drastisch erhöht wurden, kann dies die Spitzenleistung in dieser spezifischen Umgebung darstellen. Zur Bestätigung dieses Höchstgehalts sollten weitere Tests und Kontrollen durchgeführt werden.

Nach Ablauf des Basiszeitraums und ohne spezifische Höchstwerte bei Client-Anfragen /second wird empfohlen, für Warnzwecke künstlich einen Schwellenwert von 10 % bis 25 % der höchsten beobachteten Client-Anfragen/Sekunde festzulegen.

Neben der Überwachung der Leistung und der Warnung bei bestimmten Überschreitungsschwellen kann die Cisco WSA auch so konfiguriert werden, dass SNMP-Traps unter folgenden Hardwarebedingungen gesendet werden:

Standardmäßig aktiviert

- RAID-Statusänderung
- Lüfterfehler
- Hohe Temperatur
- Tastenablauf
- Link-Down
- Link-Up
- Änderung des Netzteilstatus
- Update-Fehler
- Upstream-Proxy-Fehler

Standardmäßig deaktiviert

- Verbindungsfehler
- CPU-Auslastung überschritten
- Speichernutzung überschritten

Wenn Sie die CPU-Nutzung eines bestimmten Proxys überprüfen müssen, überprüfen Sie die [Berechnung der Proxy-CPU-Auslastung auf der WSA mithilfe von SNMP](#).