

Proactivement surveillance de la représentation de WSA utilisant le SNMP

Contenu

[Introduction](#)

[Quelles valeurs peuvent être observées par un outil de surveillance SNMP surveillent proactivement la représentation de Cisco WSA ? À quel niveau les alertes de seuil devraient-elles être configurées ?](#)

Introduction

Ce document décrit surveiller proactivement la représentation de l'appliance de sécurité Web de Cisco (WSA) avec le Protocole SNMP (Simple Network Management Protocol).

Quelles valeurs peuvent être observées par un outil de surveillance SNMP surveillent proactivement la représentation de Cisco WSA ? À quel niveau les alertes de seuil devraient-elles être configurées ?

Quand vous surveillez Cisco WSA, les éléments les plus importants pour l'interrogation SNMP sont comme suit :

- Demandes de client/en second lieu
cacheThruputNow (.1.3.6.1.4.1.15497.1.2.3.7.1.1) Débit de demande dans le de dernière minute
- Temps de réponse
cacheTotalRespTimeNow (.1.3.6.1.4.1.15497.1.2.3.7.9.1) Temps de réponse total de cache dans le de dernière minute
- Utilisation du CPU
cacheBusyCpuUsage (.1.3.6.1.4.1.15497.1.2.3.1.5) Temps occupé de pourcentage de la CPU

Remarque: Des fichiers de la base d'informations de gestion SNMP (MIB) pour WSA peuvent être trouvés sur la [page de support produit de sécurité Web de Cisco](#).

Puisque chaque environnement de client varie, il est recommandé de recueillir des statistiques de production de spécification de base sur une période de positionnement afin de voir s'il y a des annexes au cours de la période de spécification de base. Pendant cette spécification de base, périodes de note où demandes de client/en second lieu où maximisé. S'il y avait une augmentation radicale correspondante de l'utilisation du CPU de temps de réponse et de potentiel, ceci pourrait représenter la performance maximale dans cet environnement spécifique. Davantage de test et de surveillance devraient être exécutés afin de confirmer ce taux maximum.

Après spécification de base la période s'est écoulée, et aucune crête maximum spécifique n'a été observée dans des demandes /second de client, il est recommande de placer artificiellement une

valeur seuil de 10% à 25% des demandes de client observées les plus élevées/en second lieu d'alerter des buts.

Hormis la représentation de surveillance et l'alerte sur les seuils dépassés par particularité, Cisco WSA peut également être configuré pour envoyer des déroutements SNMP sur ces états de matériel :

Activé par défaut

- Changement d'état RAID
- Panne de ventilation
- À hautes températures
- Expiration principale
- Lien vers le bas
- Relier
- Changement d'état de bloc d'alimentation
- Panne de mise à jour
- Panne en amont de proxy

Désactivé par défaut

- Panne de Connectivité
- Utilisation du processeur dépassée
- Utilisation de mémoire dépassée

Si vous devez vérifier l'utilisation du CPU spécifique de proxy, passez en revue l'[utilisation du processeur calculatrice de proxy sur le WSA utilisant le SNMP](#).