

Fehlerbehebung bei hoher CPU-Auslastung aufgrund des SNMP-Prozesses

Inhalt

[Einleitung](#)

[Verwendete Komponenten](#)

[Protokollsammlung](#)

[Protokollanalyse](#)

[Konfiguration der SNMP-Ansicht](#)

[FehlerbehebungTipp](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird ein strukturierter Ansatz zur Fehlerbehebung und Behebung einer hohen CPU-Auslastung beim SNMP-Prozess auf einem Wireless LAN-Controller der Serie 9800 beschrieben.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless-Controller: C9800-80-K9 mit 17.09.03

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Protokollsammlung

Identifizieren von CPU-Auslastungsmustern Nach Erhalt eines Berichts über eine hohe CPU-Auslastung, der mit dem SNMP-Prozess verknüpft ist, besteht die erste Vorgehensweise darin, detaillierte Protokolle über einen festgelegten Zeitraum zu sammeln. Dies hilft, ein Muster oder einen Trend bei der CPU-Auslastung zu ermitteln, das bzw. der ausschlaggebend dafür ist, wann der SNMP-Prozess am aktivsten und ressourcenintensivsten ist.

Vor Beginn der Protokollsammlung müssen spezifische Informationen gesammelt werden, die zur Unterstützung des Fehlerbehebungsprozesses verwendet werden. Sammeln Sie zunächst nur wenige Informationen zu dem Problem.

- Kommt es im System zu Spitzenlasten oder ist die Nutzung durchgängig hoch?
- Wie hoch ist der prozentuale Anteil der Nutzung in beiden Fällen?
- Wie oft wird die CPU ausgelastet?
- Wie häufig fragt jeder SNMP-Server den WLC ab?
- Wer sind die Top Talkers?

Sammeln Sie die Befehlsausgabe von 9800 WLC in zweiminütigen Intervallen über einen Zeitraum von zehn Minuten. Diese Daten können verwendet werden, um Probleme mit der CPU-Auslastung zu analysieren, insbesondere solche, die mit dem SNMP-Prozess zusammenhängen.

```
#terminal length 0
#show clock
#show process cpu sorted | exclude 0.0
#show process cpu history
#show processes cpu platform sorted | exclude 0.0
#show snmp stats oid
#show snmp stats hosts
```

Protokollanalyse

Nachdem Sie diese Protokolle gesammelt haben, müssen Sie sie analysieren, um die Auswirkungen zu verstehen.

Betrachten wir ein Beispiel für CPU-Nutzungsprotokolle, um den SNMP-Prozess zu identifizieren, der die meiste CPU beansprucht.

<#root>

```
WLC#show process cpu sorted | exclude 0.0
CPU utilization for five seconds: 96%/7%; one minute: 76%; five minutes: 61%
  PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
  250   621290375         58215467    10672
58.34% 39.84% 34.11%    0 SNMP LA Cache pr <-- High utilization

  93   167960640         401289855      418 14.50% 11.88%  9.23%  0 IOSD ipc task
 739   141604259         102242639     1384  8.57%  6.95%  7.21%  0 SNMP ENGINE
 763      7752             34896         222  4.00%  3.41%  1.83%  5 SSH Process
 648   6216707           181047548      34  0.72%  0.37%  0.31%  0 IP SNMP
 376   3439332           51690423       66  0.40%  0.36%  0.25%  0 SNMP Timers
 143   3855538           107654825      35  0.40%  0.35%  0.23%  0 IOSXE-RP Punt Se
 108   6139618           17345934      353  0.40%  0.30%  0.34%  0 DBAL EVENTS
```

Die Ausgabe des Anzeigeprozesses `cpu sortiert | exclude 0.0`-Befehl gibt an, dass der SNMP-Prozess tatsächlich eine unverhältnismäßig große Menge an CPU-Ressourcen beansprucht. Insbesondere der SNMP LA Cache pro Prozess ist am CPU-intensivsten, gefolgt von anderen SNMP-bezogenen Prozessen.

Der nächste Befehlssatz soll uns dabei helfen, detaillierte Informationen zum Prozess der hohen SNMP-Auslastung zu erhalten.

<#root>

```
WLC#show snmp stats oid
```

```
time-stamp          #of times requested          OID
11:02:33 Austral Jun 8 2023

 27698              bsnAPIfDBNoisePower  <-- Frequently polled OID
11:02:23 Austral Jun 8 2023          1          sysUpTime
11:02:23 Austral Jun 8 2023          17         cLSiD11SpectrumIntelligenceEnable
11:02:23 Austral Jun 8 2023          1          cLSiD11SpectrumIntelligenceEnable
11:02:23 Austral Jun 8 2023          6          cLSiD11Band
11:02:23 Austral Jun 8 2023          1          cLSiD11Band
11:02:23 Austral Jun 8 2023          1          cLSiD11Band
11:02:23 Austral Jun 8 2023          1          cLSiD11Band
11:02:23 Austral Jun 8 2023          1          cLSiD11Band
11:02:19 Austral Jun 8 2023          24         cLcCdpApCacheApName
11:02:19 Austral Jun 8 2023          1          cLcCdpApCacheDeviceIndex
11:02:19 Austral Jun 8 2023          9          cLApCpuAverageUsage
11:02:19 Austral Jun 8 2023          1315       cLApCpuCurrentUsage
11:02:19 Austral Jun 8 2023          2550       bsnAPIfDBNoisePower
```

Die Ausgabe des Befehls `show snmp stats oid` gibt die Häufigkeit an, mit der verschiedene OIDs abgefragt werden. Eine bestimmte OID, `bsnAPIfDBNoisePower`, sticht durch die außerordentlich hohe Anzahl von Anfragen hervor. Dies deutet darauf hin, dass ein aggressives Polling dieser OID wahrscheinlich zu der hohen CPU-Auslastung beiträgt, die auf dem WLC beobachtet wird.

Versuchen wir zu verstehen, was die OID `bsnAPIfDBNoisePower` tut und seine Datenspeicherzeiten.

Navigieren Sie zu [SNMP Object Navigator](#), und suchen Sie die OID "`bsnAPIfDBNoisePower`".

Translate OID into object name or object name into OID to receive object details

Enter OID or object name: examples -
 OID: 1.3.6.1.4.1.9.9.27
Object Name: ifIndex

Object Information

Specific Object Information	
Object	bsnAPIfDBNoisePower
OID	1.3.6.1.4.1.14179.2.2.15.1.21
Type	Integer32
Permission	read-only
Status	current
MIB	AIRESpace-WIRELESS-MIB ; - View Supporting Images
Description	"This is the average noise power in dBm on each channel that is available to Airespace AP"

OID-Suchergebnis

Das Objekt bsnAPIfDBNoisePower gibt die Rauschleistung der einzelnen Kanäle an, die von den einzelnen Access Points gemeldet werden. Angesichts der großen Anzahl von Kanälen und APs, die vom WLC verwaltet werden, können die von dieser OID generierten SNMP-Daten erheblich sein. Wenn der WLC eine große Anzahl von APs bedient, kann das durch das Polling dieser OID erzeugte Datenvolumen immens sein. Dies kann zu einer hohen CPU-Auslastung führen, da der WLC diese umfangreichen SNMP-Anforderungen verarbeitet.

Ebenso müssen Sie das Verhalten der spezifischen OID verstehen, die aggressiv abgefragt wird.

Der nächste Befehl dient dazu, Sie über die SNMP-Server zu informieren, die den WLC abfragen.

```
WLC#show snmp stats hosts
Request Count   Last Timestamp   Address
77888844        00:00:00 ago     10.10.10.120
330242          00:00:08 ago     10.10.10.150
27930314        00:00:09 ago     10.10.10.130
839999          00:00:36 ago     10.10.10.170
6754377         19:45:34 ago     10.10.10.157
722             22:00:20 ago     10.10.10.11
```

Dieser Befehl stellt eine Liste der SNMP-Server mit ihrer Anfrageanzahl und dem letzten Zeitstempel ihrer Abfrageaktivität bereit.

Wie Sie sehen, werden vom 9800 WLC mehrere verschiedene Server abgefragt. Wenn Sie sich

die vollständigen Protokolldaten ansehen, die in den letzten 10 Minuten gesammelt wurden, können Sie auch deren Abfragehäufigkeit messen.

Sie können nun zu jedem Server gehen und sehen, wie oft die OID abgefragt wird, die eine Sicherheitsverletzung darstellt. In diesem Beispiel wird die OID alle 30 Sekunden abgefragt, was deutlich häufiger als erforderlich ist. Da der WLC alle 180 Sekunden RF/RRM-Daten empfängt, führt das Polling der OID alle 30 Sekunden zu unnötiger Verarbeitung und trägt zu einer hohen CPU-Auslastung bei.

Sobald die OID des Angreifers und der Server identifiziert wurden, können wir mehrere verschiedene Lösungen ausprobieren, um die Belastung des WLC zu reduzieren.

1. Reduzieren Sie die Abfragehäufigkeit auf dem SNMP-Server.
2. Wenn die OID für die Betriebsnutzung nicht benötigt wird, deaktivieren Sie das Polling dieser OID vom SNMP-Server.
3. Wenn Sie keine Kontrolle über den SNMP-Server haben, können Sie die SNMP-Ansicht verwenden, um die beanstandete OID zu blockieren.

Konfiguration der SNMP-Ansicht

Definieren Sie eine neue Ansicht, die die zu sperrende OID ausschließt. Sie möchten z. B. die OID 1.3.6.1.4.1.14179.2.2.15.1.21 blockieren, eine neue Ansicht erstellen und die OID an die Ansicht anhängen.

```
<#root>

snmp-server view blockOIDView
1.3.6.1.4.1.14179.2.2.15.1.21
  excluded

<-- This is the OID of bsnAPIfDBNoisePower

snmp-server community TAC view blockOIDView RO

<-- This command assigns the blockOIDView to the community myCommunity with read-only (RO) access.

snmp-server group TAC v3 priv read blockOIDView

<-- This command assigns the blockOIDView to the group myGroup with the priv security level for SNMPv3.
```

Tipp zur Fehlerbehebung

- Baseline-CPU-Auslastung: Dokumentieren der normalen CPU-Auslastung, wenn der SNMP-Prozess keine hohe Auslastung verursacht.
- SNMP-Konfiguration: Überprüfen Sie die aktuellen SNMP-Konfigurationseinstellungen, einschließlich Community-Strings, Version (v2c oder v3) und Zugriffslisten.

- SNMP Best Practice: Verwenden Sie das Dokument mit den Best Practices für den 9800 WLC, und ordnen Sie die vorgeschlagene Konfiguration für SNMP so genau wie möglich zu.

```
C9800(config)#snmp-server subagent cache
C9800(config)#snmp-server subagent cache timeout ?
<1-100> cache timeout interval (default 60 seconds)
```

- Häufigkeit des SNMP Polling: Bestimmen Sie, wie oft der WLC von SNMP-Abfragen abgefragt wird, da eine hohe Frequenz zu einer höheren CPU-Last beitragen kann.
- Netzwerktopologie und SNMP-Manager: Verstehen der Netzwerkeinrichtung und Identifizieren aller SNMP-Manager, die mit dem WLC interagieren.
- Systemverfügbarkeit: Überprüfen Sie die seit dem letzten Neustart verstrichene Zeit, um festzustellen, ob ein Zusammenhang zwischen der Verfügbarkeit und der CPU-Auslastung besteht.
- Zuletzt durchgeführte Änderungen: Notieren Sie alle aktuellen Änderungen an der WLC-Konfiguration oder am Netzwerk, die mit dem Beginn einer hohen CPU-Auslastung einhergehen können.
- Bei 9800 WLC liegt der Fokus auf Telemetrie. Die Telemetrie funktioniert in einem "Push"-Modell, bei dem der WLC relevante Informationen an den Server sendet, ohne dass eine Abfrage erforderlich ist. Wenn Ihre SNMP-Abfragen WLC-CPU-Zyklen beanspruchen und Betriebsprobleme verursachen, ist es besser, zu Telemetrie zu wechseln.

Schlussfolgerung

Durch eine methodische Analyse der CPU-Nutzungsdaten und deren Korrelation mit SNMP-Polling-Aktivitäten können Sie Probleme mit der CPU-Nutzung, die durch SNMP-Prozesse auf dem Cisco 9800 WLC verursacht werden, beheben und beheben. Die Überwachung nach der Implementierung ist wichtig, um den Erfolg der Fehlerbehebung zu bestätigen und eine optimale Netzwerkleistung sicherzustellen.

Zugehörige Informationen

- [Überwachung des Catalyst 9800 WLC über SNMP mit OIDs](#)
- [Management der Catalyst Wireless Controller der Serie 9800 mit Prime-Infrastruktur mit SNMP V2 und V3 und NetCONF](#)
- [Schützen Sie Ihr Simple Network Management Protocol](#)
- [Cisco Catalyst Serie 9800 - Best Practices für die Konfiguration](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.