

Technische Hinweise zur hohen CPU-Auslastung bei C170

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hohe CPU-Auslastung auf C170](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die CPU-Nutzung und den Betrieb einer Cisco E-Mail Security Appliance (ESA) der Serie C170.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Statusdetails und Systemauslastung im Hinblick auf ESA-Betrieb

Verwendete Komponenten

Die Informationen in diesem Dokument basieren nur auf dem Modell ESA C170.

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hohe CPU-Auslastung auf C170

Für eine ESA C170 ist die CPU-Auslastung von 40 % im Allgemeinen kein Grund zur Besorgnis und unter bestimmten Umständen normal.

Die Appliance ist nicht vollständig inaktiv. Die Appliance führt Service-Level-Aktionen aus, auch

wenn keine E-Mails verarbeitet werden. Basierend auf der CPU-Last sind dies einige Beispiele, die zur CPU-Nutzung beitragen können:

- Service-Updates werden verarbeitet (Anti-Spam, Anti-Virus usw.)
- Annehmen von Secure Shell (SSH)-Verbindungen von einer Security Management Appliance (SMA)
- Verarbeitung von Berichtsdaten

Anmerkung: Der C170 verfügt nur über zwei CPUs. Die relativ geringe CPU-Auslastung von Dingen wie Service-Updates und SSH-Verbindungen hat einen größeren Einfluss auf die CPU-Auslastungsberechnung von Appliances mit weniger integrierter CPU.

Einer der Hauptgründe für die CPU-Auslastung beim C170 sind Service-Updates. Wenn die ESA Service-Updates verarbeitet, werden die relevanten Prozesse gestoppt und neu gestartet, sobald Updates erfolgen. Dies kann erhebliche CPU-Zeit in Anspruch nehmen. Wenn Sie beispielsweise den CLI-Befehl **antispamupdate ironport force** ausführen, wird die Cisco Anti-Spam Engine (CASE) aktualisiert und neu gestartet. Der Dienst selbst kompiliert die Regeln und Updates für eine schnellere Gesamtleistung. Dieser momentane Neustart spiegelt sich in der beobachteten CPU-Abwanderung wider.

Anmerkung: Die vom Betriebssystem berechnete CPU-Auslastung ist eine fortlaufende Berechnung. Daher kann eine frühere hohe CPU die aktuelle gemeldete CPU-Auslastung auch dann beeinflussen, wenn die CPU-Auslastung derzeit nicht sehr hoch ist. Dies bedeutet, dass die CPU-Auslastung, obwohl die Service-Updates nur alle 5 Minuten erfolgen, die CPU-Auslastung beeinflussen kann, die im Intervall zwischen den Updates berechnet wird.

Ein zweiter Grund für die hohe CPU-Auslastung sind SSH-Verbindungen. Wenn eine ESA so konfiguriert ist, dass sie eine SMA für zentralisierte Berichte, Quarantänen usw. verwendet, besteht ein CPU-Overhead, der SSH-Verbindungen von der SMA akzeptiert, wenn die ESA zu Beginn mit ihr verbunden ist. Die Geschwindigkeit, mit der die ESA SSH-Verbindungen von der SMA empfängt, variiert, aber im Allgemeinen erhält die ESA etwa alle 30 Sekunden eine Verbindung. Sie können dies in den Authentifizierungsprotokollen anzeigen und sehen, wie der **smaduser** eine Verbindung herstellt:

```
myesa.local> tail authentication
```

```
Press Ctrl-C to stop.
```

```
Wed Apr 12 13:41:06 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:41:26 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:41:44 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

```
Wed Apr 12 13:42:01 2017 Info: The user smaduser successfully logged on from 172.16.1.100 by publickey based authentication using an SSH connection.
```

Ein weiterer Grund, den Sie bei der Überprüfung einer hohen CPU-Auslastung berücksichtigen sollten, ist die Appliance, die Berichtsdaten verarbeitet. Die ESA verarbeitet weiterhin Berichtsdaten, während sie E-Mails nicht verarbeitet. Beispielsweise werden Systemauslastungsmetriken für den Systemkapazitätsbericht verarbeitet. Darüber hinaus führt das ESG **Berichterstattungsrollups** durch, um eine angemessene Größe der Berichtsdatenbank zu gewährleisten. Diese Berichterstattungsrollups sind zu Beginn des Monats, wenn die

monatliche Zusammenfassung erfolgt, am wichtigsten.

Unterm Strich ist die CPU-Auslastung von 40 % beim C170 nicht ungewöhnlich, selbst wenn sich die Appliance im Leerlauf befindet und keine E-Mail-Nachrichten verarbeitet werden. Ein ESA-Administrator sollte nur dann betroffen sein, wenn die CPU-Last über einen längeren Zeitraum mit 100 % gekoppelt ist. Überprüfen Sie die Ausgabe der **Statusdetails** für die **Messanzeigen** der Systemressourcen und die Protokollausgabe des Statusprotokolls, wie im Bild dargestellt.

Beispiel aus **Statusdetail**:

Gauges:	Current
System	
RAM Utilization	1%
Overall CPU load average	5%
CPU Utilization	
MGA	0%
Anti-Spam	0%
Anti-Virus	0%
Reporting	0%
Quarantine	0%
Disk I/O Utilization	0%
Resource Conservation	0
Logging Disk Usage	2%
Logging Disk Available	182G
Connections	
Current Inbound Conn.	0
Current Outbound Conn.	0
Queue	
Active Recipients	0
Unattempted Recipients	0
Attempted Recipients	0
Messages In Work Queue	0
Destinations In Memory	3
Kilobytes Used	0
Kilobytes Free	8,388,608
Messages In Quarantine	
Policy, Virus and Outbreak	0
Kilobytes In Quarantine	
Policy, Virus and Outbreak	0

Beispiel aus Statusprotokollen:

```
myesa.local> tail status
```

Press Ctrl-C to stop.

```
Wed Apr 12 14:03:06 2017 Info: Status: CPULd 0 DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
```

CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382176 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 7
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Wed Apr 12 14:04:06 2017 Info: Status: **CPULd 0** DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382236 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 5
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Wed Apr 12 14:05:06 2017 Info: Status: **CPULd 45** DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID
23 CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382296 MaxIO 350 RAMUsd 74632122 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 5
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Wed Apr 12 14:06:06 2017 Info: Status: **CPULd 0** DskIO 0 RAMUtil 1 QKUsd 0 QKFre 8388608 CrtMID 23
CrtICID 8 CrtDCID 5 InjMsg 9 InjRcp 9 GenBncRcp 0 RejRcp 0 DrpMsg 0 SftBncEvt 0 CmpRcp 8
HrdBncRcp 0 DnsHrdBnc 0 5XXHrdBnc 0 FltrHrdBnc 0 ExpHrdBnc 0 OtrHrdBnc 0 DlvRcp 1 DelRcp 7
GlbUnsbHt 0 ActvRcp 0 UnatmptRcp 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 16 NetReq 6 CchHit
16 CchMis 6 CchEct 0 CchExp 2 CPUTTm 3139 CPUETm 4382356 MaxIO 350 RAMUsd 74632178 MMLen 0
DstInMem 3 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 2 SophLd 0 BMLd 0 CASELd 0 TotalLd 15
LogAvail 182G EuQ 0 EuqRls 0 CmrkLd 0 McafLd 0 SwIn 0 SwOut 0 SwPgIn 0 SwPgOut 0 RptLd 0 QtnLd 0
EncrQ 0 InjBytes 5891

Zugehörige Informationen

- [Cisco E-Mail Security Appliance C170](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

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.