

Analyse van AMP diagnostische bundel voor hoge CPU's

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[Controleer of er een ander antivirus op de machine is geïnstalleerd](#)

[Identificeer de hoge CPU wanneer een specifieke toepassing in gebruik is](#)

[Voer een diagnostische bundel voor analyse in](#)

[Debug Level in endpoint](#)

[Debug Level in de AMP-interface \(CLI\)](#)

[Debug Level in beleid](#)

[Uitsluiten van AMP van andere antivirusoplossingen](#)

[Reproduceert het probleem en verzamel een diagnostische bundel](#)

[Analyse van hoge CPU-prestaties](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven om een diagnostische bundel van Advanced Malware Protection (AMP) voor Endpoints Public Cloud op MACOS-apparaten te analyseren om een hoog CPU-gebruik te problemen oplossen.

Bijgedragen door Uriel Torres en bewerkt door Yeraldin Sanchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisnavigatie in AMP-console
- Navigatie van de MAC-terminal

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

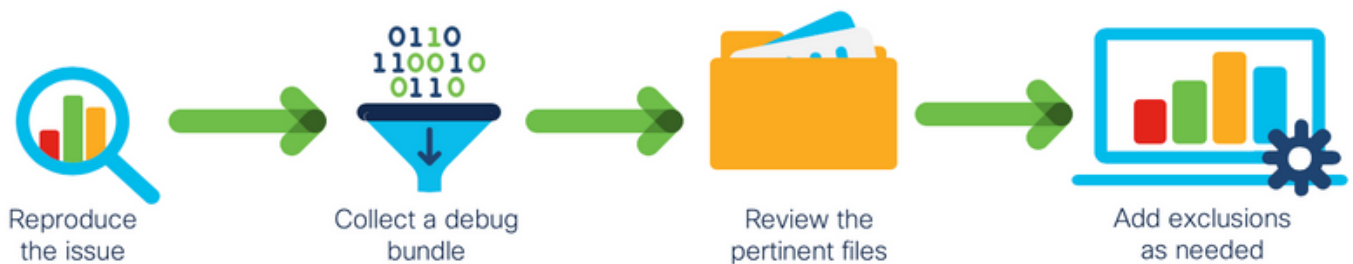
- Advanced Malware Protection voor endpoints, console 5.4.2005-12
- macOS Catalina versie 10.15.4
- AMP-connector 1.12.3.738

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De AMP-connector scant alle actieve bestanden (die die zichzelf verplaatsen, kopiëren en/of wijzigen) op een machine tenzij expliciet wordt aangegeven dat dit niet het geval is, waardoor onherroepelijk problemen ontstaan bij te veel processen en bewerkingen terwijl de connector wordt uitgevoerd, wat leidt tot een hoog CPU-gebruik, vertragingen en in sommige gevallen tot software die niet langzaam werkt of werkt. Bovendien kan de AMP-connector bestanden blokkeren op basis van hun cloudreputatie, die soms onjuist (fout-positief) kan zijn. De oplossing voor beide kwesties is deze paden en processen uit te sluiten.

De stroom van problemen met de prestaties bij het oplossen van problemen wordt in de afbeelding weergegeven.



Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

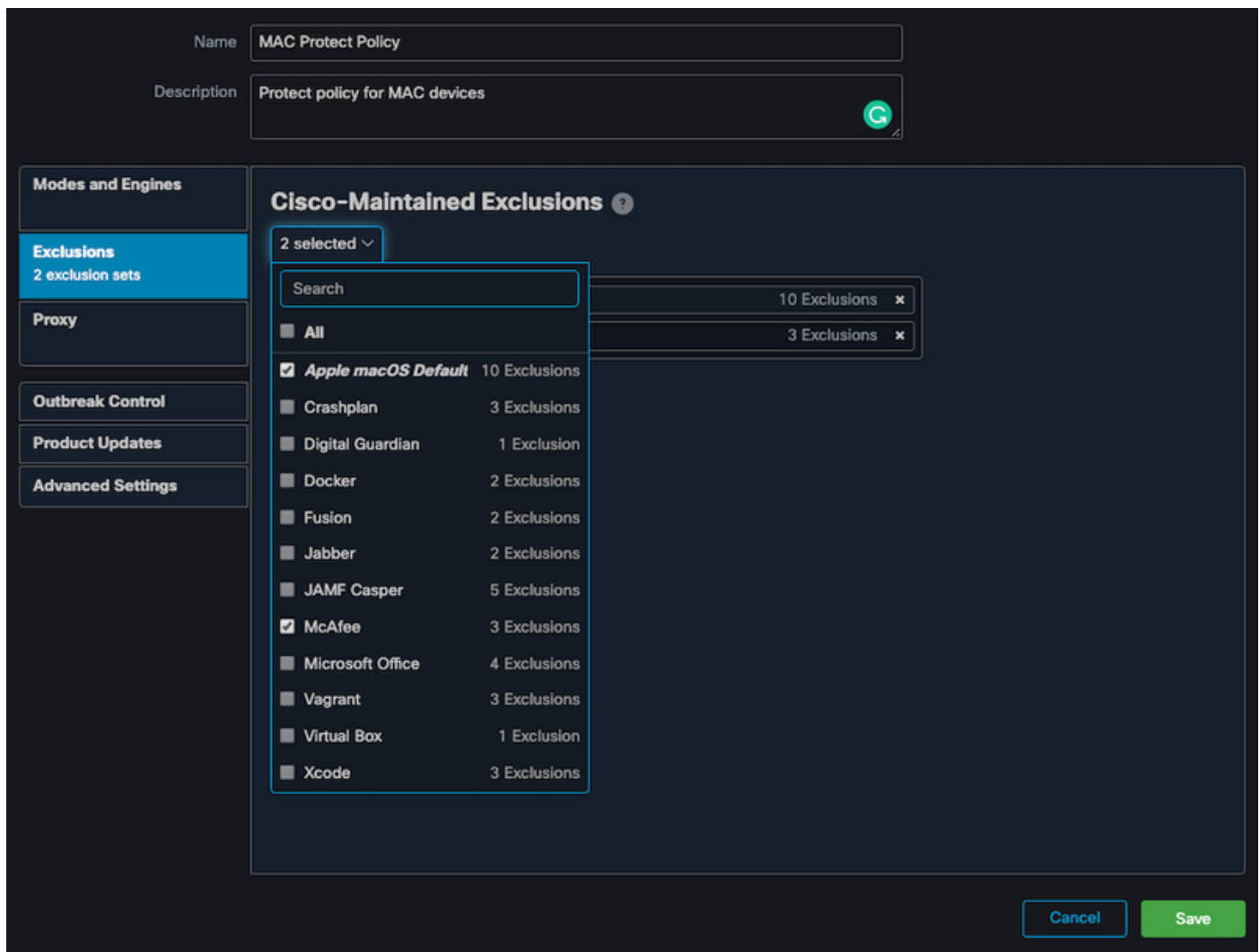
Controleer of er een ander antivirus op de machine is geïnstalleerd

Tip: Gebruik de door Cisco onderhouden uitsluitingen als de software die in de lijst staat, onthoudt dat deze uitsluitingen aan nieuwe versies van een toepassing kunnen worden toegevoegd.

Als u de lijsten in de door Cisco onderhouden uitsluitingssectie op de AMP-console wilt zien:

- Navigeren in naar **Beheer > Beleid**.
- Vind het beleid en klik op **Bewerken**.
- Klik in het beleidsvenster op **Uitsluitingen**.

Selecteer degenen die uw eindpunt nodig zouden hebben volgens de software die momenteel op de machine geïnstalleerd is. Sla het beleid vervolgens op zoals in de afbeelding.



Identificeer de hoge CPU wanneer een specifieke toepassing in gebruik is

Identificeer of het probleem gebeurt terwijl één toepassing of een paar ervan worden uitgevoerd als u in staat bent om de kwestie te repliceren helpt in het proces om potentiële uitsluitingen te identificeren.

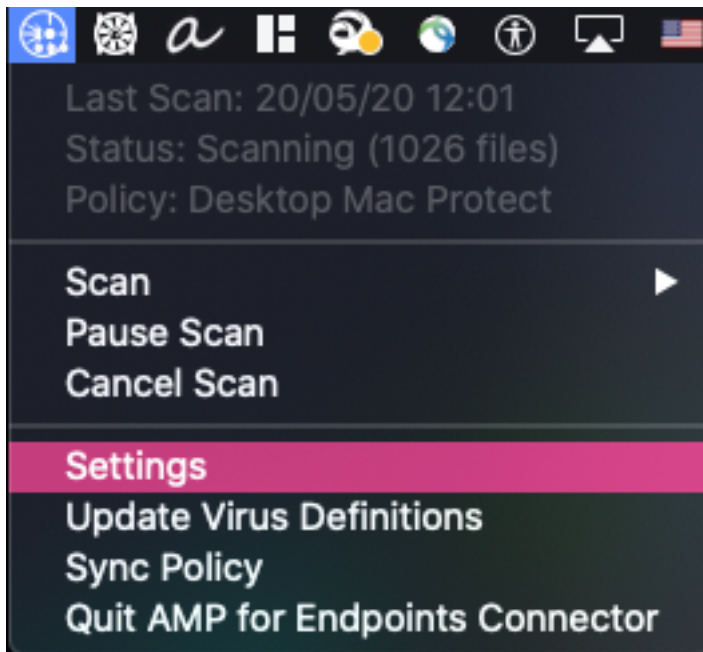
Voer een diagnostische bundel voor analyse in

Om een nuttige diagnostische bundel te verzamelen, moet het debug logniveau worden geactiveerd.

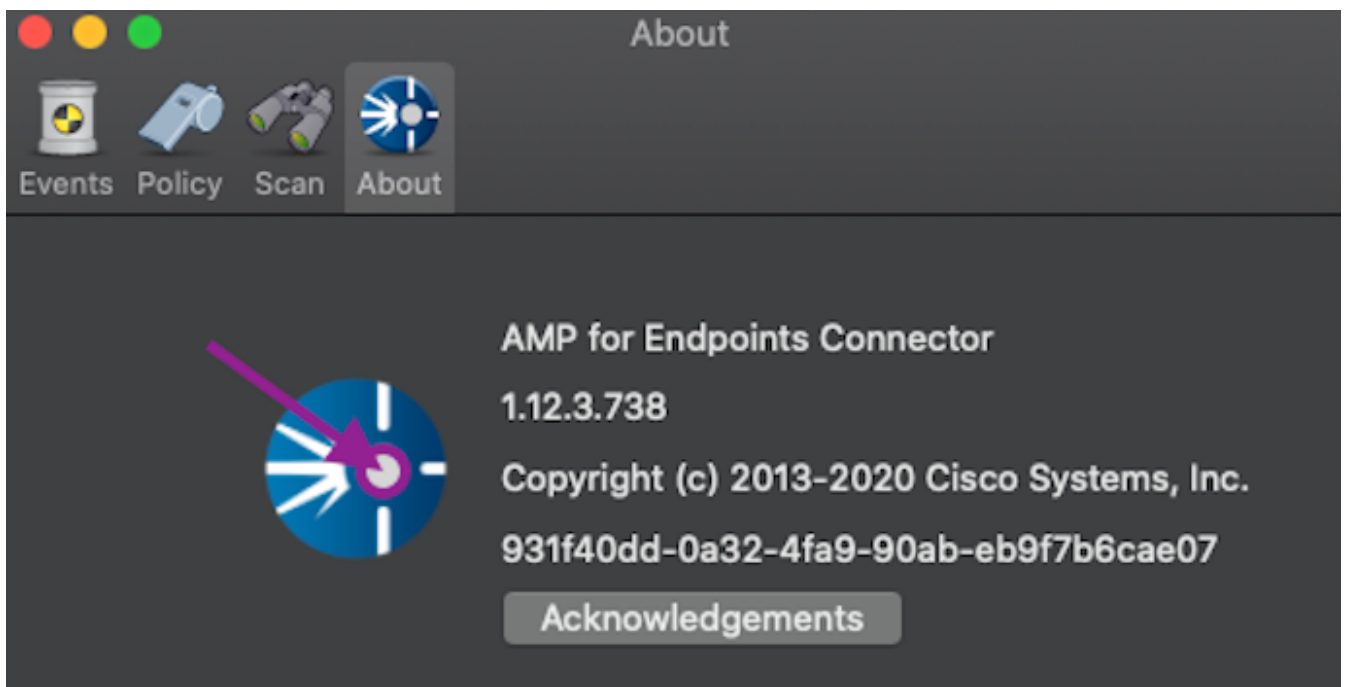
Debug Level in endpoint

Als u het probleem kunt reproduceren en toegang tot het eindpunt kunt hebben, is hieronder de beste procedure om het diagnostische pakket op te nemen.

- Klik in de werkbalk van het MAC-menu op het pictogram AMP.
- Navigeer naar **Instellingen**, zoals in de afbeelding.



- Navigeer in het instellingsvenster naar **About**.
- Klik in het AMP-logo, zoals in de afbeelding, om de bug in te schakelen.



Er verschijnt een melding dat de AMP-connector op de Debug Mode is

Deze procedure maakt logniveau te debug tot het volgende beleidshartslag interval mogelijk.

Debug Level in de AMP-interface (CLI)

- Een terminal openen
- Navigeren naar `/opt/cisco/amp/bin/naar/uit`
- Draai `ampcli`:
`./ampcli`
- Schakel in de AMP CLI de debug-modus in:
`ampcli>debuglevel 1`

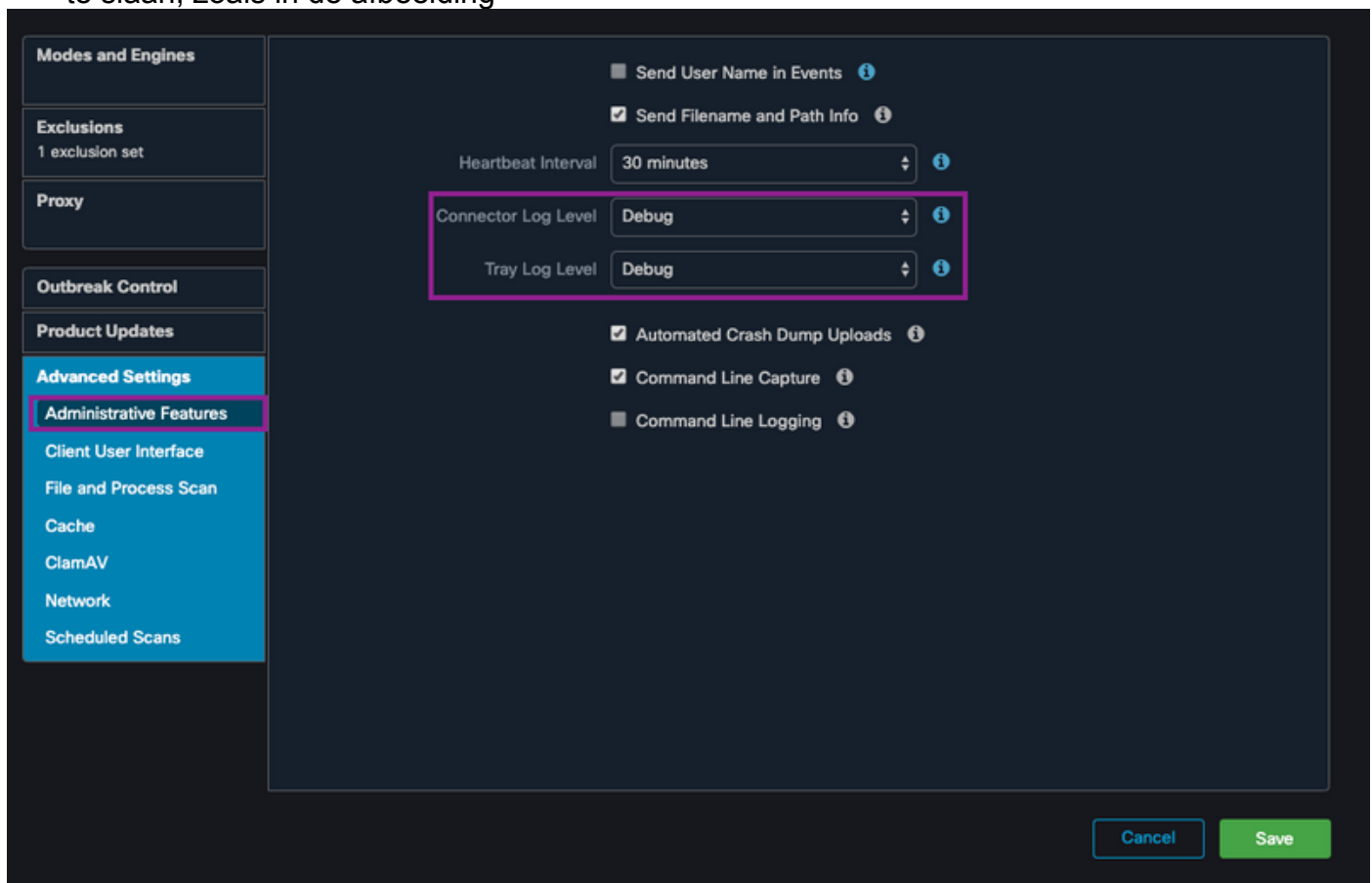
Dit proces maakt logniveau te debug tot het volgende beleidshartslag interval.

Debug Level in beleid

Als u geen toegang hebt tot het eindpunt of het probleem niet consistent kan worden gereproduceerd, moet het debug logniveau in het beleid worden ingeschakeld.

U kunt het logniveau van het wasprogramma als volgt definiëren:

- Navigeren in naar **Beheer > Beleid**
- Vind het beleid en klik op **Bewerken**
- Navigatie in naar **geavanceerde instellingen > Administratieve functies**
- **Logniveau** van de **connector** en **logniveau van de tray** instellen om het beleid te debug en op te slaan, zoals in de afbeelding



Voorzichtig: Als de debug-modus van het beleid is ingeschakeld, ontvangen alle endpoints deze configuratie.

Opmerking: Sync het beleid van het eindpunt om de debug-modus te garanderen.

Uitsluiten van AMP van andere antivirusoplossingen

Volgens de gebruikershandleiding moeten antivirusproducten de volgende directories en alle bestanden, directories en uitvoerbare bestanden binnen uitsluiten om compatibel te zijn met de AMP-connector voor MAC, de volgende directories die moeten worden uitgesloten:

- Ondersteuning/Cisco/Advanced/Malware Protection voor endpoints
- /opt/cisco/amp

Reproduceert het probleem en verzamel een diagnostische bundel

Wanneer het debug-niveau is ingesteld, wacht u tot de toestand van de hoge CPU op het systeem optreedt of reproduceren handmatig de eerder geïdentificeerde voorwaarden en verzamelen u vervolgens de diagnostische bundel.

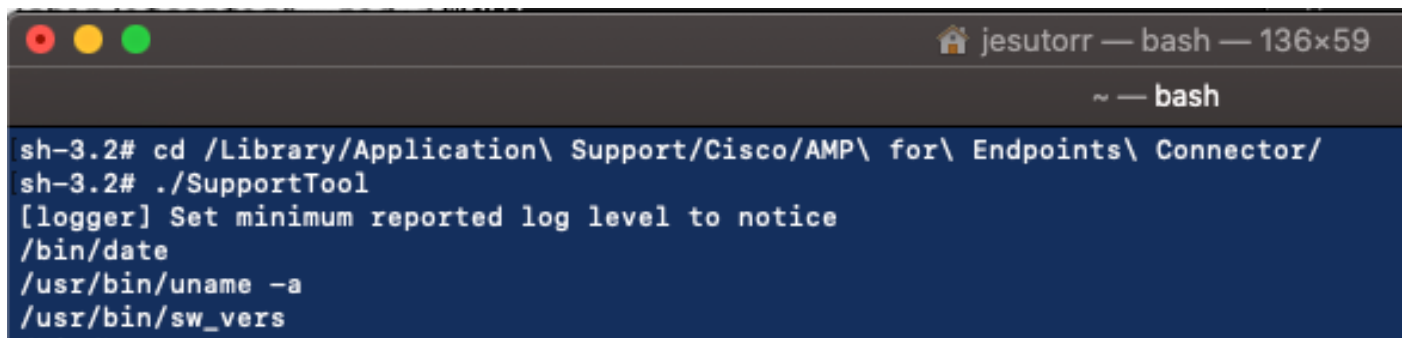
Zo verzamelt u de debug-bundel:

- Open een terminal.
- Toegang tot supergebruikersniveau en navigeer vervolgens naar **Library/Library/Application Support/Cisco/AMP voor Endpoints**:

```
cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
```

- Gebruik de volgende opdracht om het ondersteuningsgereedschap te gebruiken:

```
./SupportTool
```



```

jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers

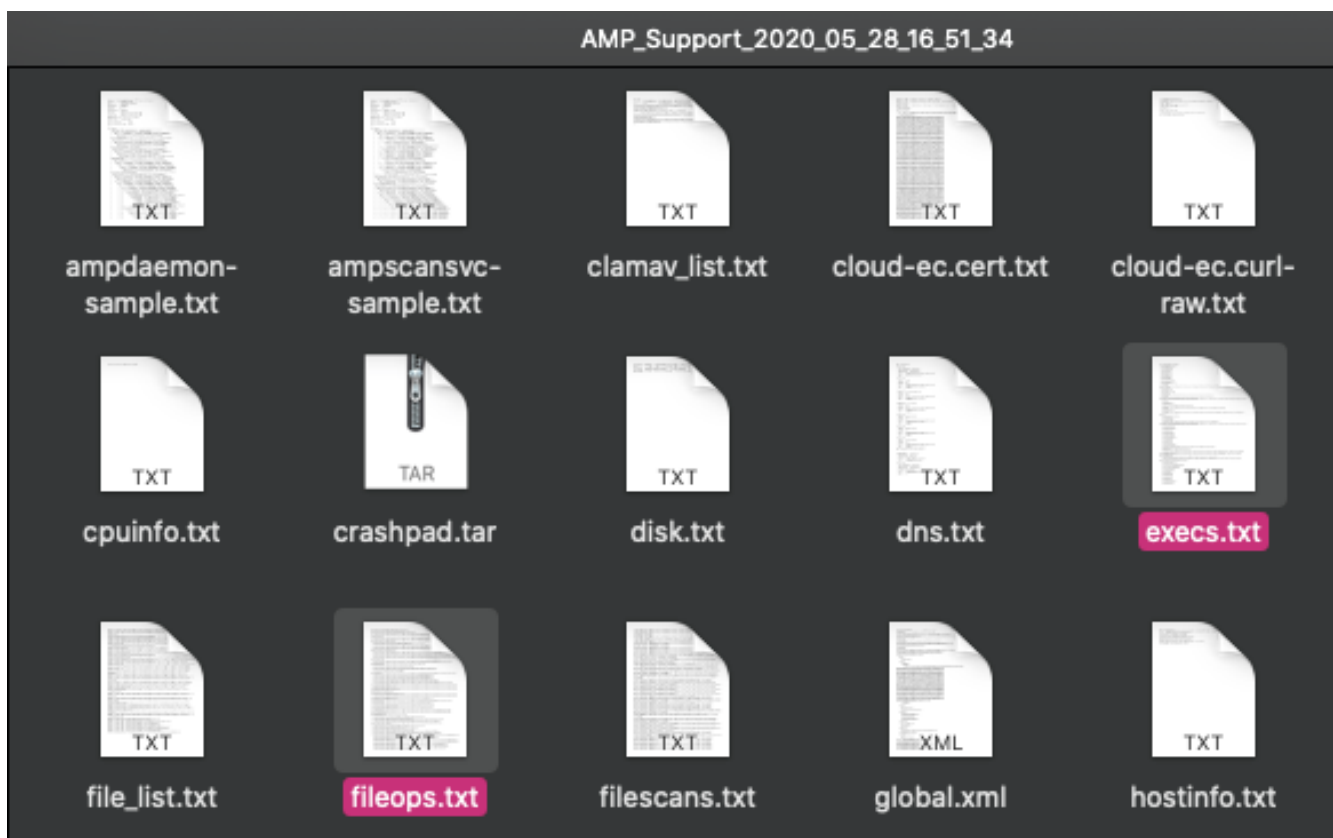
```

De debug-bundel wordt in de desktopmap opgeslagen als een .zip-bestandsextensie.

Analyse van hoge CPU-prestaties

debug diagnostische bundel is opslag in het Desktop, om de analyse te beginnen:

- Het diagnostische bundel decomprimeren
- Er zijn 2 bestanden om te bekijken Bestandsbewerkingen: fileops.txtBestandsexecuties: execs.txt



- The fileops.txt werkt als het belangrijkste prestatiegereedschap om problemen op te lossen. Dit overzicht bevat alle huidige actieve bewerkingen op uw eindpunt terwijl de connector draait. Het wordt als volgt gelezen:

<Nummerscans die op het pad worden uitgevoerd wanneer de bundel wordt verzameld> /
<Pad
gescand>

```

fileops.txt
19 /Library/Application Support/Apple/ParentalControls/Users/jesutorr/2020/05/21-usage.data
18 /Users/jesutorr/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/Config/dummy.phoneInfo
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyEventActivityStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.Settings.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/
Outlook.GovernedChannelStates.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json

```

Bijvoorbeeld, als u een homebrew toepassing hebt, toont fileops.txt de volgende actieve operaties:

```
639 /Users/jesutorr/Library/Bin/MyApplication/support/
```

```
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
```

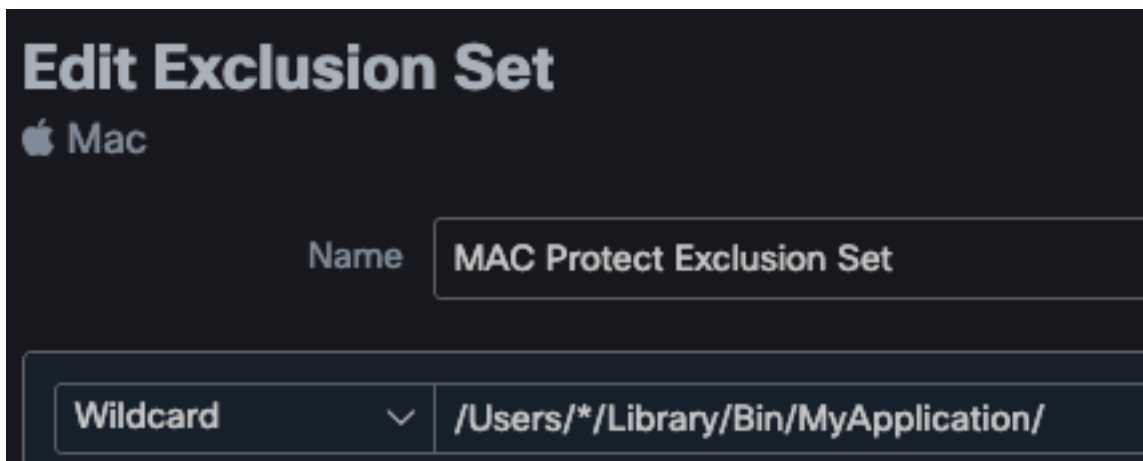
```
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```

```

fileops.txt — Edited
639 /Users/jesutorr/Library/Bin/MyApplication/support/
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/

```

- Wanneer het proces eenmaal is vastgesteld, kan een uitsluiting worden gecreëerd
- Om uitsluiting te creëren
- navigeer in de AMP-console naar **Management > uitsluitingen**
- Selecteer de uitsluitingsinstelling en klik op **Bewerken**
- De uitsluiting kan worden toegevoegd zoals in de afbeelding



- Het Execs.txt-bestand bevat alle opdrachten die door processen worden gebruikt terwijl de connector bundels verzamelt. De hier genoemde paden mogen niet worden uitgesloten van het AMP-beleid, omdat dit binaries (/bin) en system binaries(/sbin) zijn die alle processen gebruiken, echter op Execs.txt het hoofdproces kan leveren dat loopt. Bijvoorbeeld, als het Execs.txt bestand de volgende logs toont.

The image shows a terminal window with a title bar that says "execs.txt — Edited". The terminal displays the following lines of text:

```
501 /bin/bash
96 /usr/bin/defaults
91 /usr/bin/stat
91 /usr/bin/tr
90 /usr/bin/cut
```

Aangezien de homebrew-toepassing bash gebruikt, kunt u bevestigen dat de toepassing de oorzaak is van de hoge CPU.

Gerelateerde informatie

- [Advanced Malware Protection voor endpoints Procesuitsluitingen in macOS en Linux](#)
- [Best Practices for AMP voor uitsluitingen van endpoints](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)