Verzameling van diagnostische gegevens van AMP voor Endpoints Linux-connector

Inhoud

Inleiding

Dit document beschrijft de stappen om een diagnostisch bestand te genereren van de AMP for Endpoints Linux-connector. Als u een technisch probleem hebt met de Linux-connector, kan een Cisco Technical Support Engineer de logberichten die in een diagnostisch bestand beschikbaar zijn willen analyseren.

Diagnostisch bestand genereren

Met gebruik van deze opdracht kunt u direct een diagnostisch bestand vanuit de Linux opdrachtregel interface (CLI) genereren:

```
/opt/cisco/amp/bin/ampsupport
```

Dit creëert een .7z bestand op je bureaublad. U kunt dit bestand aan Cisco Technical Assistance Center (TAC) leveren voor verdere analyse.

Debug Mode

De debug-modus van de connector biedt extra breedtegraden aan de vastlegging. Het geeft meer inzicht in een probleem met de connector. In dit gedeelte wordt beschreven hoe u de bug-modus in een connector kunt inschakelen.

> **Waarschuwing**: Debug-modus moet alleen worden ingeschakeld als Cisco deze gegevens vraagt. Als u de bug-modus langer inschakelen, kan deze de schijfruimte heel snel vullen en kan het ondersteuningsdiagnostische bestand worden voorkomen om het **connector**-

logbestand te verzamelen vanwege de buitensporig grote bestandsgrootte.

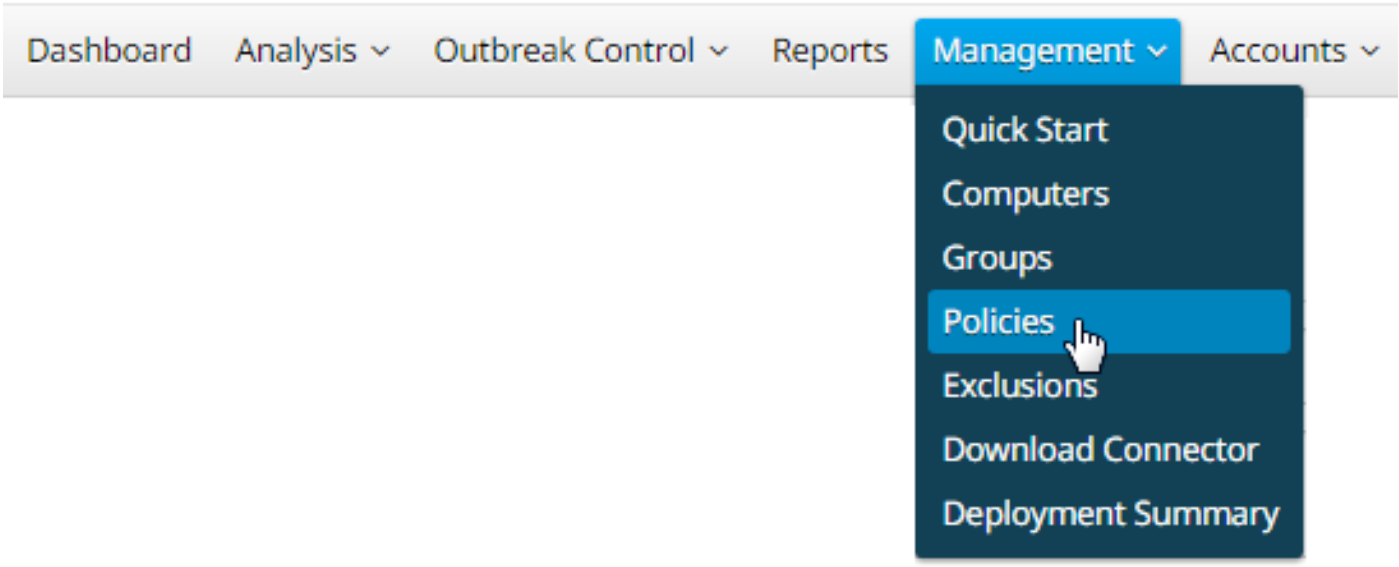
AMP-console gebruiken

Debug Mode inschakelen

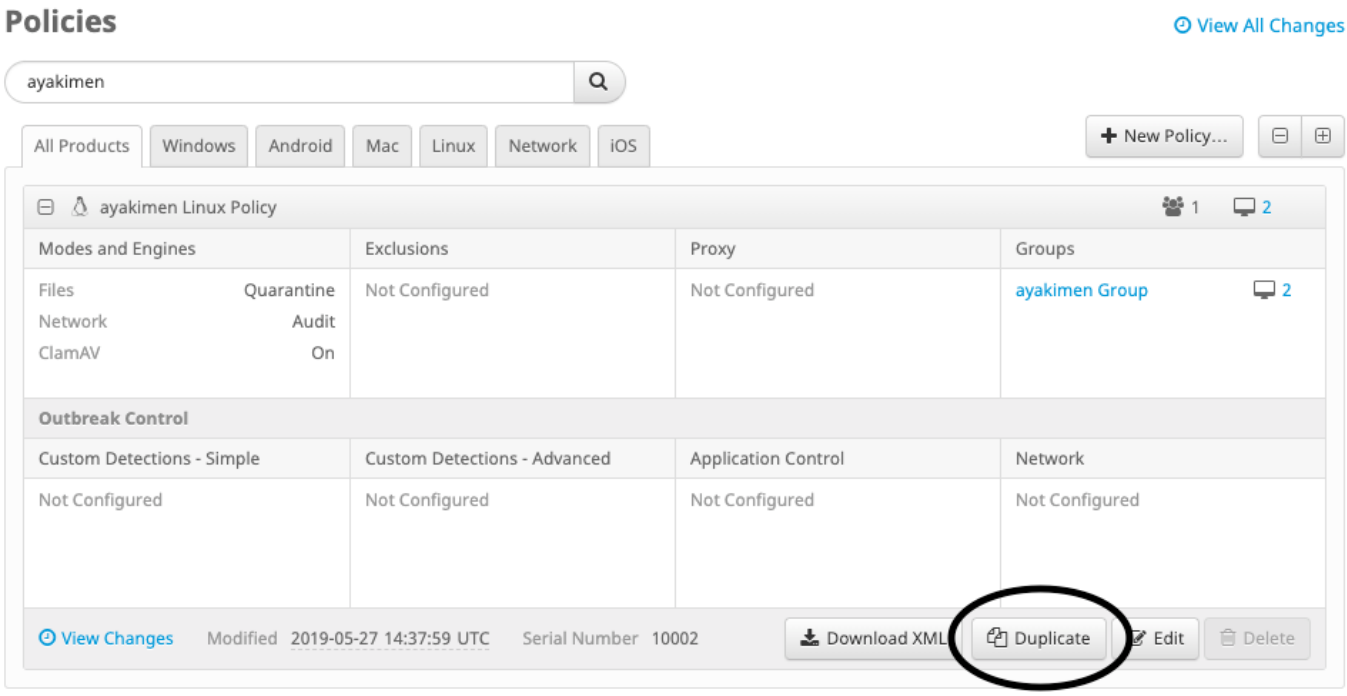
U kunt de debug-modus in het huidige beleid met stappen 5 - 7 inschakelen of u kunt met al deze stappen een nieuw beleid maken in de debug-modus:

Stap 1. Meld u aan bij de AMP-console.

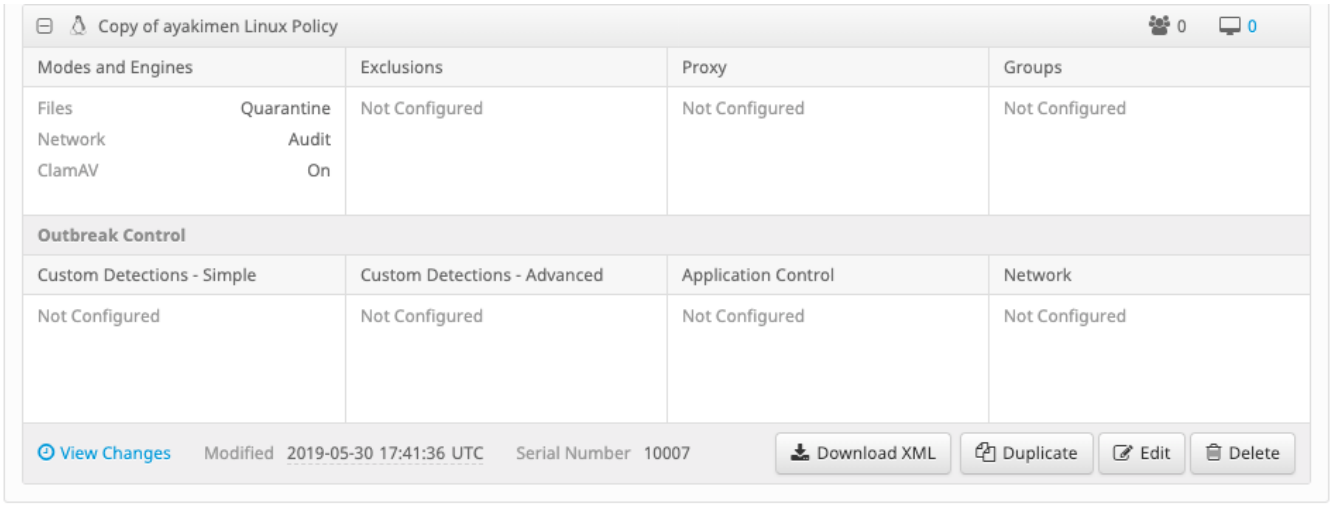
Stap 2. Selecteer **Beheer > Beleid**.



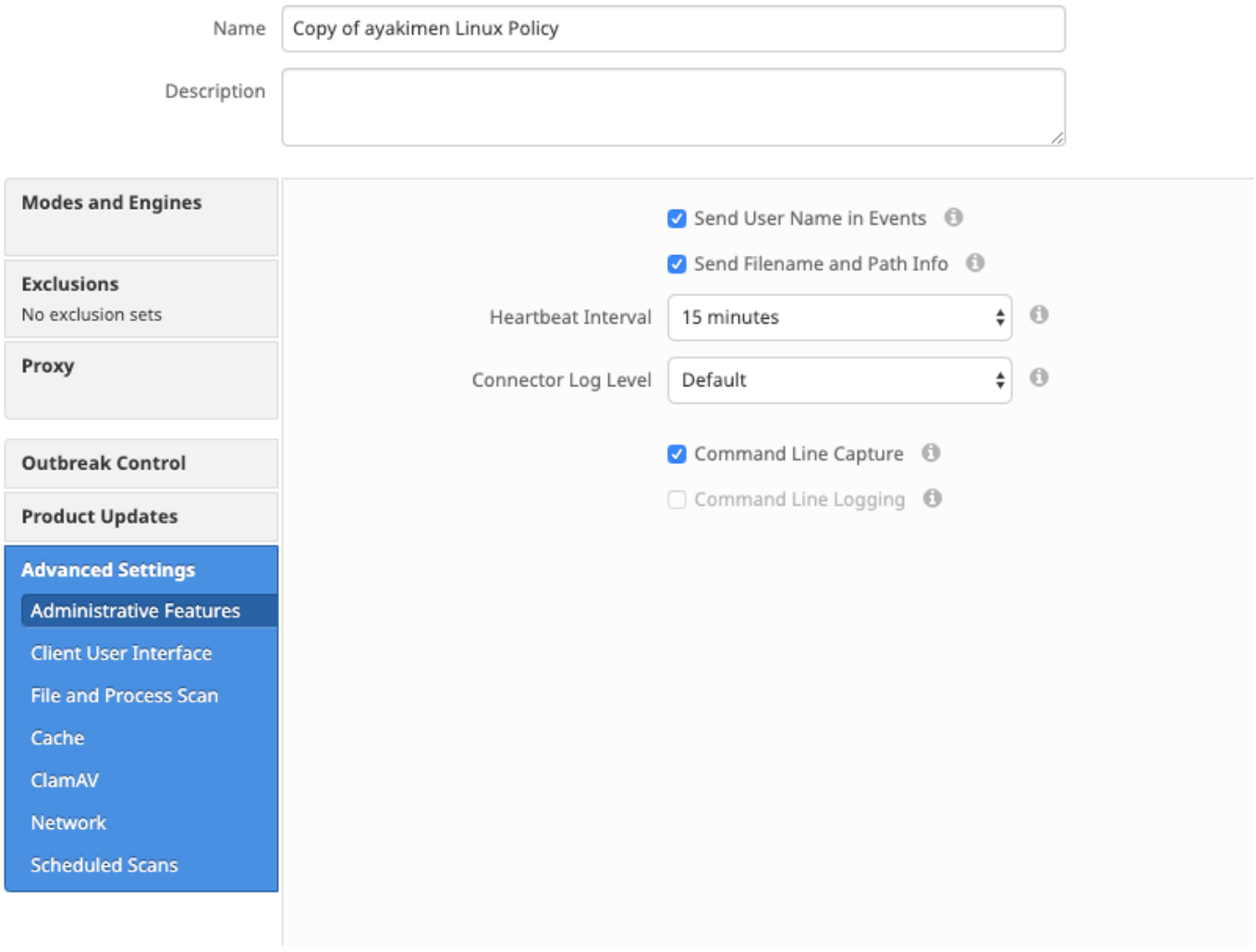
Stap 3. Pak het beleid vast dat op het eindapparaat of de computer is toegepast en klik op het beleid, dan wordt het beleidsvenster uitgebreid. **Klik op Duplicaat**.



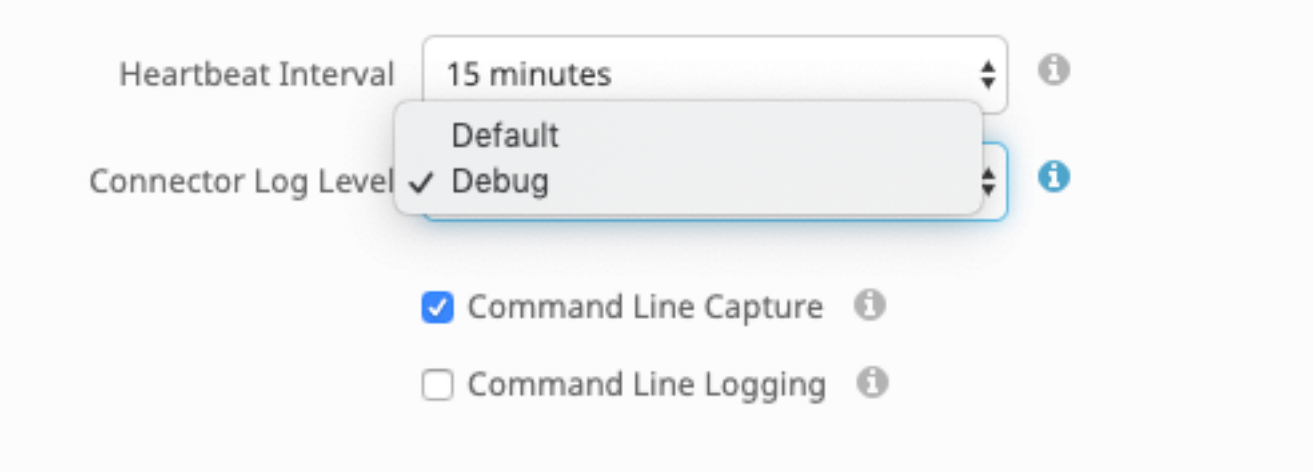
Stap 4. Nadat u op **Duplicaat klikt**, wordt de AMP-console bijgewerkt met het gekopieerde beleid.



Stap 5. **Klik op** Bewerken, **klik op Geavanceerde instellingen** en selecteer vanuit de knoppenbalk op **Administratieve** functies.



Stap 6. **VoorConnector** selecteert u Debuggen uit de vervolgkeuzelijsten.



Stap 7. Klik op Opslaan om de wijzigingen op te slaan.

Stap 8. Na het opslaan van het nieuwe beleid moet u een groep maken of wijzigen om *het nieuwe beleid* op te nemen, en *het* apparaat *waar* u debug-informatie wilt genereren.

Debug Mode uitschakelen

Om de debug-modus uit te schakelen, volgt u dezelfde stappen als u hebt voltooid om de debug-modus in te schakelen. U verandert echter het **logniveau** van de **connector** in **standaard**.

Opdracht gebruiken

Debug Mode inschakelen

Als u problemen hebt met de connectiviteit in de console en u wilt de bug-modus activeren, voert u deze opdrachten in op de CLI:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

Dit is de output:

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

Debug Mode uitschakelen

U kunt de debug-modus uitschakelen door deze opdrachten te gebruiken:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

Ondersteuningsgereedschap Tunnen tijdens in debug

De connector moet in de Debug Logging-modus worden geplaatst voordat de ondersteuning van het bestand wordt gestart. Dit gebeurt via de AMP-console, via de beleidsinstellingen van de connector *bij Management -> beleidslijnen*. Bewerk het beleid en ga naar *de* sectie

Administratieve Functies onder *de* Geavanceerd Instellingen. Wijzig *de* instelling *Log* Levelsetting *van de* connector **om te Debug**.

Bewaar je beleid. Controleer of uw beleid is opgeslagen en gesynchroniseerd op de connector. Draai de connector in deze modus ten minste 15-20 minuten voordat u doorgaat met de rest van de tuning.

NB: Vergeet niet om, wanneer de afstemming is voltooid, *de* standaardinstelling van *het* Log Levelsetting aan te passen zodat de connector op zijn meest efficiënte en effectieve modus werkt.

Ondersteunende tool uitvoeren

Deze methode omvat het gebruik van het Support Tool, een toepassing die met de AMP Mac-connector is geïnstalleerd. U hebt toegang tot de map Toepassingen door te dubbelklikken op <Application>Cisco Advanced Malware Protection>Support Tool.app. Dit zal een volledig steunpakket genereren dat extra diagnostische bestanden bevat.

Een alternatief, en sneller, methode is om de volgende opdrachtregelvan a terminal zitting :

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```

De eerste optie levert een veel kleiner ondersteuningsbestand op dat alleen de relevante tuning-bestanden bevat. De tweede optie biedt een volledig ondersteuningspakket met meer informatie, zoals logbestanden, die mogelijk vereist zijn voor het afstemmen van procesuitsluitingen (beschikbaar in Aansluitversies 1.11.0 en nieuwer).

Beide manieren waarop u ervoor kiest om deze functie uit te voeren, genereert Support Tool een zip-bestand op uw ~home dat twee tuning-ondersteuningsbestanden bevat: fileops.txt en execus.txt. fileops.txt bevat een lijst van de meest gemaakte en aangepaste bestanden op uw machine. Deze zijn handig voor de uitsluitingen van pad en kaart. execus.txt zal de lijst van de meest frequent uitgevoerde bestanden bevatten, zullen deze nuttig zijn voor Procesuitsluitingen. Beide lijsten worden gesorteerd door middel van een scan-telling, wat de meest gescande paden betekent, verschijnen boven in de lijst.

Laat de connector 15-20 minuten in de Debug-modus draaien en voer vervolgens het ondersteuningsgereedschap in. Een goede vuistregel is dat alle bestanden of paden die gemiddeld 1000 hits of meer in die tijd zijn, goede kandidaten zijn die moeten worden uitgesloten.

Afstemming van uitsluitingen

Uitsluitingen voor pad, jokerteken, bestandsnaam en bestandsextensie maken

Eén manier om te beginnen met de regels van de Uitsluiting van het Pad is het vaakst gescande bestand en mappenpaden vinden van bestanden.txt en overwegen dan om regels voor die paden te maken. Nadat het beleid is gedownload, controleert u het nieuwe CPU-gebruik. Het kan 5 tot 10 minuten duren nadat het beleid is bijgewerkt voordat u de CPU-gebruiksdaling opmerkt, aangezien het tijd kan duren voordat de datum wordt ingehaald. Als u nog problemen ziet, voert u het gereedschap opnieuw uit om te zien welke nieuwe paden u waarneemt.

- Een goede vuistregel is dat alles met een log- of een tijdschrift-bestandsextensie als een geschikte uitsluitingskandidaat moet worden beschouwd.

Procesuitsluitingen maken

NOTE: Process Exclusions on Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
Zie voor beste praktijken met betrekking tot procesuitsluitingen: Advanced Malware Protection voor endpoints Procesuitsluitingen in macOS en Linux

Een goed stempatroon is eerst het identificeren van de processen met een hoog volume executies van execus.txt, het pad naar het uitvoerbaar vinden en een uitsluiting voor dit pad creëren. Er zijn echter enkele processen die niet moeten worden opgenomen, zoals:

- Algemene hulpprogramma's - Het wordt niet aanbevolen algemene gebruiksprogramma's uit te sluiten (bijvoorbeeld: usr/bin/grep) zonder rekening te houden met het volgende: De gebruiker kan bepalen welke toepassing het proces oproept (bijvoorbeeld: het ouderproces vinden dat grijp uitvoert) en het ouderproces uitsluiten. Dit dient alleen te gebeuren als en alleen als het moederproces veilig kan worden afgesloten met een procesuitsluiting. Als de ouderuitsluiting van toepassing is op kinderen, dan worden de oproepen naar kinderen van het moederproces ook uitgesloten.De gebruiker die het proces uitvoert, kan worden vastgesteld. (ex: Als een proces bij een hoog volume door gebruiker "root" wordt opgeroepen, kan het proces worden

uitgesloten, maar alleen voor de gespecificeerde user 'root', dan kan AMP de uitvoering van een bepaald proces controleren door een gebruiker die geen 'root' is.**LET OP: Procesuitsluitingen zijn nieuw in Connector versies 1.11.0 en nieuwer. Daarom kunnen algemene hulpprogramma's worden gebruikt als Pad-uitsluiting in Connectorversies 1.10.2 en ouder. Deze praktijk wordt echter alleen aanbevolen wanneer een prestatietransactie absoluut noodzakelijk is.**

Het ouder maken is belangrijk voor procesuitsluitingen. Zodra het Parent-proces en/of de gebruiker van het proces zijn gevonden, kan de gebruiker de uitsluiting voor een specifieke gebruiker creëren en de procesuitsluiting toepassen op kinderprocessen, waardoor lawaaiprocessen die zelf niet in procesuitsluitingen kunnen worden omgezet, worden uitgesloten.

Parkeerproces identificeren

1. Volg stap 1-3 van het identificeren van het ouder proces van bovenaf.
2. Identificeer gebruiker van een proces met behulp van een van de volgende methoden: Vind de Gebruiker ID van het bepaalde proces in `U:` in de loglijn (bijvoorbeeld: U:0).Voer in het Terminalvenster de volgende opdracht in: `getent doorgestuurd # | versneden: -f1`, waarin #de gebruiker-ID is.U dient uitvoer vergelijkbaar met:`Gebruikersnaam` te zien, waar Gebruikersnaam de Gebruiker van het gegeven proces is.
3. Dit Gebruikersnaam kan worden toegevoegd aan een Procesuitsluiting in de categorie Gebruiker om het toepassingsgebied van de uitsluiting te beperken, hetgeen voor bepaalde Procesuitsluitingen belangrijk is. **OPMERKING: Als de gebruiker van een proces de lokale gebruiker van de machine is, en deze uitsluiting van toepassing moet zijn op meerdere machines met verschillende lokale gebruikers, moet de categorie Gebruiker leeg gelaten worden om de Procesuitsluiting op alle gebruikers van toepassing te laten zijn.**

Gerelateerde informatie

- Verzameling van diagnostische gegevens van een FirePOWER-connector die op Windows actief is
- Verzameling van diagnostische gegevens van een FireAMP-connector die op Mac OS draait
- **Technische ondersteuning en documentatie – Cisco Systems**