Advanced Malware Protection voor endpoints ClamAV Virus Definition Opties in Linux

Inhoud

Inleiding

Vanaf versie 1.11.0 van de Linux-connector biedt AMP voor Endpoints nu twee configuratieopties voor ClamAV Virus:

1. alleen Linux
2. Full ClamAV

Voordat de Linux-only optie beschikbaar wordt, heeft de Linux-connector gescande bestanden gescand met de volledige ClamAV-virusdefinitie. Deze set bevat malware handtekeningen voor Linux, macOS, Windows en Android. Hoewel dit uitgebreide bereik biedt, zijn er ook belangrijke bronnen nodig (d.w.z. CPU-tijd en -geheugen). Sommige Linux-systemen kunnen profiteren van het configureren van AMP om de kleinere Linux-only ClamAV-virusdefinitieset te gebruiken.

De Linux-only virusdefinitie is minder dan 10% van de volledige set. Een kleinere set gebruikt om overhead te reduceren en maakt het mogelijk om AMP te gebruiken op hulpbron-beperkte systemen. Ondanks de prestatievoordelen maakt een verminderde dekking voor niet-Linux malware deze configuratie alleen geschikt voor bepaalde toepassingen. Bijvoorbeeld, het zou geschikt zijn voor servers die alleen Linux-bestanden (zoals toepassingsservers) hosten/opslaan, maar niet geschikt zijn voor servers die ook niet-Linux-bestanden (zoals FTP-, mail- en MKB-bestandsservers) ontvangen/opslaan. De systeembeheerder moet deze ruil in evenwicht brengen om de juiste reeks virusdefinities te kiezen.

> **BELANGRIJK!**
>
> Het is sterk aanbevolen om alle endpoints te verbeteren naar Connector versie 1.11.0 of nieuwer voordat u de nieuwe Linux-only virusdefinitieoptie gebruikt. Hoewel versies van de 1.10.x- en oudere connector de nieuwe optie zullen accepteren, is het gedrag van de connector in sommige gevallen niet intuïtief. Raadpleeg het gedeelte *Compatibiliteit* achteruit voor meer informatie.

Compatibiliteit met achteren

Er is een belangrijk probleem op het gebied van compatibiliteit dat moet worden overwogen voordat u eindpunten configureren om de nieuwe Linux-only virusdefinitieoptie te gebruiken: 1.10.x en oudere connectors zullen de volledige virusdefinitie blijven gebruiken indien de volledige

set al was gedownload. Indien geconfigureerd om de nieuwe Linux-only virusdefinitie te gebruiken, zal de Connector stoppen met het bijwerken van de volledige virusdefinitie en alleen de Linux-virusdefinitie daarna bijwerken. Dit kan resulteren in het eindpunt dat gebruik maakt van bijgewerkte Linux virusdefinities maar verouderde macOS, Windows, en Android definities.

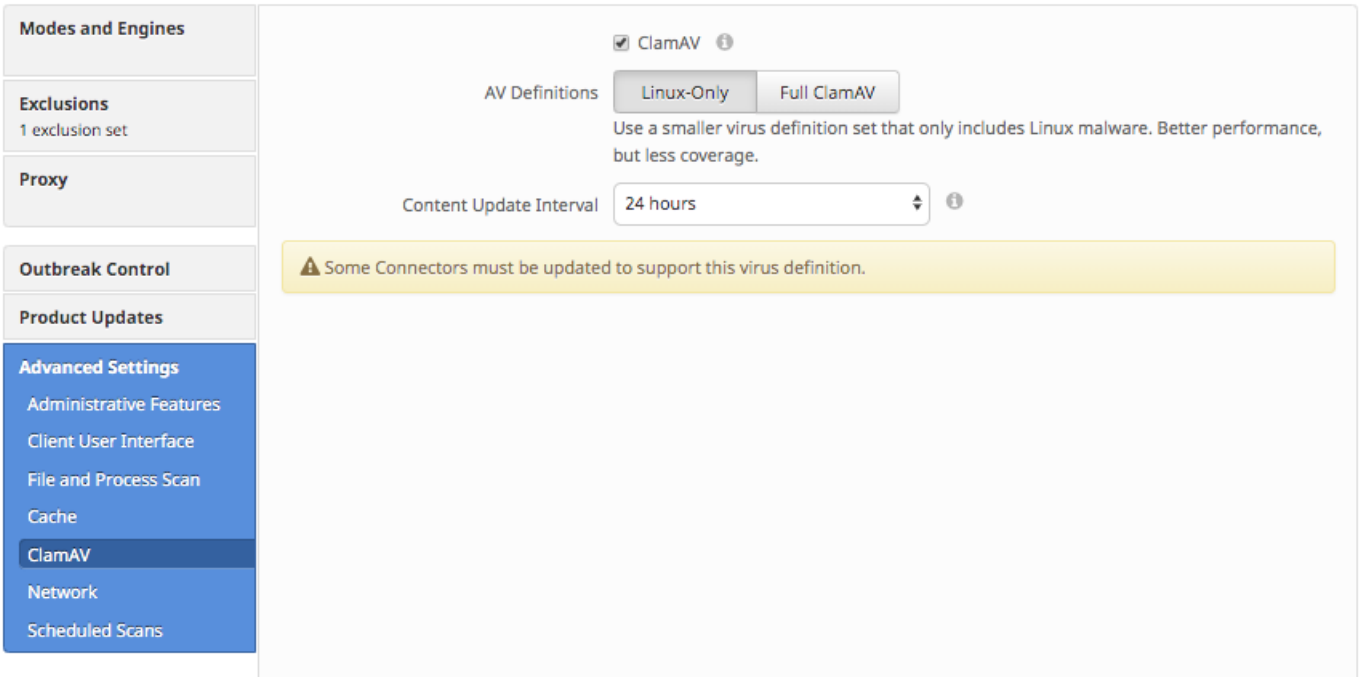
Er zijn twee mogelijke resoluties:

1. upgrade van de connector naar 1.11.0 of hoger.
2. Wijzig de definitie van ClamAV virus en stel deze weer in op Full ClamAV.

De optie ClamAV Virus Definities wijzigen

De optie ClamAV Virus Definition kan worden ingesteld met behulp van de Advanced Malware Protection voor Endpoints. De optie voor elk beleid kan worden gewijzigd door in:

Beheer > Beleid > [Linux Policy] > Bewerken > Geavanceerde instellingen > ClamAV



Nadat de beleidsinstelling voor AV - definities is gewijzigd, wordt de nieuwe instelling van kracht op de eindpunten bij de volgende geplande virusdefinitieupdate. Deze vertraging wordt beheerst door de beleidsinstelling "Content Update Internal".

De waarschuwing "Sommige connectors moeten worden bijgewerkt om deze virusdefinitie te ondersteunen" kan verschijnen in het ClamAV Advanced Settings-scherm als ten minste één connector die door het beleid wordt beheerd een onverenigbare Linux-connector versie voert. Het is sterk aanbevolen om de connectors te verbeteren en deze waarschuwing op te lossen voordat u de Linux-only definities-instelling gebruikt.

De nieuwe instelling op het eindpunt controleren

Indien geconfigureerd om Linux-only definities te gebruiken, moet de gecombineerde geheugen van de twee AMP-connector-processen kleiner zijn dan 100 MB.

U kunt deze opdracht als volgt analyseren:

```
top -p `pidof ampdaemon` -p `pidof ampscansvc`
```

Het volgende is een steekproefuitvoer: