Cisco Advanced Malware Protection voor endpoints Mac/Linux CLI

Inhoud

Inleiding

Dit document beschrijft de opdrachten van de Opdracht Line Interface (CLI) beschikbaar voor gebruik met de Cisco Advanced Malware Protection (AMP) voor Endpoints Connector op Mac of Linux-besturingssysteem.

De CLI is beschikbaar voor alle gebruikers van een systeem, hoewel de beschikbaarheid van bepaalde opdrachten kan afhangen van de configuratie van het beleid en/of de wortelrechten. De opdrachten die hiervan afhankelijk zijn, worden in dit artikel openbaar gemaakt.

Cisco Advanced Malware Protection voor endpoints Mac/Linux CLI

Navigeren naar de CLI

Het Cisco Advanced Malware Protection voor Endpoints CLI is beschikbaar wanneer de Advanced Malware Protection voor Endpoints Connector op het systeem is geïnstalleerd en uitgevoerd:

- Open het Terminalvenster op Mac/Linux.
- Start de CLI met de volgende paden: bij Linux:`/opt/cisco/amp/bin/ampcli` op Mac:`/opt/cisco/amp/ampcli`
- Wanneer de CLI wordt gestart, ziet de gebruiker het volgende bericht:

```
ampcli - AMP for Endpoints Connector Command Line Interface Interactive mode Enter 'q' or Ctrl+c to Exit [logger] Set minimum reported log level to notice Trying to connect... Connected.
ampcli>
```

Beschikbare CLI-opdrachten

OPMERKING: alle beschikbare CLI-opdrachten kunnen ook rechtstreeks vanaf de opdrachtregel worden uitgevoerd, d.w.z.`/opt/cisco/amp/bin/ampcli`-helpor`/opt/cisco/amp/ampcli` zullen hetzelfde werken als het starten van de CLI en het starten van de `hulp`.

- Voor een volledige lijst met CLI-opdrachten kan de gebruiker `helpen`:

```
ampcli> help scan Initiate/pause/stop a scan * See 'scan help' for more. status Get ampdaemon status sync Sync policy policy Show policy exclusions List custom exclusions history Show event history * See 'history help' for more. quarantine List/restore quarantined file(s) * See 'quarantine help' for more. about About AMP for Endpoints Connector defupdate Update virus definitions notify Toggle notifications verbose Toggle verbose mode q Quit ampcli interactive mode
```

- De opdrachten `scannen`, `historie`, en `quarantaine` neem extra parameters die worden beschreven als de gebruiker de opdracht samen met `hulp`:

```
ampcli> scan help Supported scan parameters: flash Perform a flash scan full Perform a full scan custom Perform a custom scan on a file or directory (recursive) e.g. '...> scan custom file_or_directory_to_scan' pause Pause a running scan resume Resume a paused scan cancel Cancel a running scan list List scheduled scans

ampcli> history help Supported history parameters: list List history * Listing starts at page 1. Each time 'list' is run we move to the next page. Specify a page number to jump directly to that page. pagesize Set history page size (max: 12) * e.g. 'ampcli> history pagesize 10'

ampcli> quarantine help Supported quarantine parameters: list List currently quarantined files * Listing starts at page 1. Each time 'list' is run we move to the next page. Specify a page number to jump directly to that page. restore Restore file by quarantine id e.g. '...> quarantine restore
```

Gebruik van CLI-opdracht

- `scannenscan flitser` - voer een flitsscan van het systeem uit.`een volledige scan` van het systeem uitvoeren.`een aangepaste <path_to_scan>` - een bepaald bestand of folder scannen.`scanpauze` - stop momenteel actieve scans.`resumé` - hervatten de momenteel stilstaande scans.`scannen` - alle huidige scanners annuleren.`scanlijst` - lijst van geplande scans die op het systeem moeten worden uitgevoerd.

- `status` - geeft de huidige status van de connector op het systeem weer:

```
ampcli> status Status: Connected Mode: Normal Scan: Ready for scan Last Scan: 2020-01-22 03:57 PM Policy: Audit Policy for AMP for Endpoints (#5755) Command-line: Enabled Faults: None
```

Als er fouten aanwezig zijn op een eindpunt, wordt in het veld Fouten het aantal fouten weergegeven dat aanwezig is voor elk ernst-niveau (Critical/Major/Minor). Om te beginnen met Connector, versie 1.12.3, zal de CLI ook een`Fout-ID's`veld, dat de foutcodes voor elke fout toont die op het eindpunt wordt opgehaald. Onder deze velden zal de CLI ook instructies geven voor elke fout die op het eindpunt aanwezig is.

ex:

```
Faults: 1 Critical, 1 Major Fault IDs: 1, 3 ID 1 - Critical: The system extensions failed to load. Approve the system extensions in Security & Privacy System Preferences. ID 3 - Major: Full Disk Access not granted. Grant access to the ampdaemon executable in Security & Privacy System Preferences.
```

- `sync` - sync de stekker voor de cloud, om optimaal beleid te garanderen.

- `beleid` - toont het huidige beleid voor de connector die op het systeem loopt:

```
ampcli> policy Quarantine Behavior: Quarantine malicious files. Protection: Monitor program
```

```
install. Monitor program start. Passive on-execute mode. Proxy: NONE Notifications: Do not
display cloud notifications. Policy: Audit Policy for AMP for Endpoints (#5755) Last Updated:
2020-01-08 04:49 PM Definition Version: ClamAV(bytecode.cvd: 331, daily.cvd: 25721, main.cvd:
59) Definitions Last Updated: 2020-01-08 05:09 PM
```

- `uitsluitingen` - de huidige uitsluitingen voor de connector tonen: Deze instelling moet ook in het Aansluitingsbeleid worden ingeschakeld om de uitsluitingen te laten zien.

```
ampcli> exclusions Exclusions: Path /home Path /mnt/hgfs Regular Expression /var/log/.*\.log
```

- `historie`
  `historie` - lijst van de geschiedenis van de connectoractiviteit (scans, quarantaine, enz.)`historiegrootte <numerieke_waarde>` - stelt de grootte van de pagina in voor het weergeven van de geschiedenis (max. 12)

```
ampcli> history pagesize 12 Page size set to 12
```

- `quarantaine`(*Deze optie is alleen beschikbaar voor gebruikers die als wortel actief zijn.*)
  `quarantainelijst` - lijst van in quarantaine geplaatste goederen op het systeem.`quarantaine terugzet <quarantaine_id>` - hiermee wordt een quarantainebestand hersteld via het quarantainebestand, dat kan worden gevonden in de opdracht `quarantaine`.

- `over` - verstrekt informatie, zoals versie en Madebuut voor de connector die op het systeem loopt.

```
ampcli> about AMP for Endpoints Connector v1.12.1.221 Copyright (c) 2013-2020 Cisco Systems,
Inc. All rights reserved. This product incorporates open source software; refer to
/opt/cisco/amp/doc/acknowledgement.txt for details. [ 22b608b3-b20e-4bd3-8b53-def824acce8a ]
```

- `deflatoire` - de Cloud een verzoek te doen toekomen om de virusdefinities te actualiseren.

- kennisgevingen van de draaiknop in de CLI aan/uit. Deze instelling moet ook worden ingeschakeld in het Aansluitingsbeleid.Op Mac heeft dit geen invloed op meldingen in de UI.

```
ampcli> notify Notifications set to on

ampcli> notify Notifications set to off
```

- `langdradig` - toggle breedband houtkap voor de CLI aan/uit.

```
ampcli> verbose Verbose mode set to on

ampcli> verbose Verbose mode set to off
```

- `q` - stop de AMP voor Endpoints Mac/Linux-connector CLI.

Aanvullende informatie

Technische ondersteuning en documentatie – Cisco Systems

Cisco Advanced Malware Protection voor endpoints - gebruikershandleiding