Verwenden der Secure Endpoint Mac/Linux CLI

Inhalt

Einleitung

In diesem Dokument werden die Befehle der Befehlszeilenschnittstelle (CLI) beschrieben, die für die Verwendung mit Secure Endpoint Connector unter Linux und MacOS verfügbar sind.

Hintergrundinformationen

Die CLI-Befehle stehen allen Benutzern eines Systems zur Verfügung. sEinige Befehle sind von der Richtlinienkonfiguration und/oder den Root-Berechtigungen abhängig. Die davon abhängigen Befehle sind in diesem Artikel beschrieben.

Cisco Secure Endpoint Mac/Linux-Kommandozeile

Navigieren zur CLI

Die Secure Endpoint CLI ist verfügbar, wenn der Secure Endpoint Connector installiert ist und auf dem System ausgeführt wird:

- Öffnen Sie das Terminal-Fenster unter Mac/Linux.
- Führen Sie die CLI über die folgenden Pfade aus:
  - unter Linux:`/opt/cisco/amp/bin/ampcli`
  - auf Mac:`/opt/cisco/amp/ampcli`
- Beim Start der CLI wird folgende Meldung angezeigt:

```
ampcli - Cisco Secure Endpoint 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>
```

Verfügbare CLI-Befehle

HINWEIS: Alle verfügbaren CLI-Befehle können auch direkt über die Befehlszeile ausgeführt werden, z. B. `/opt/cisco/amp/bin/ampcli` helpor/`opt/cisco/amp/ampcli` helpworks genauso wie beim Starten von CLI und `Runhelp`.

- Für eine vollständige Liste der CLI-Befehle kann der Benutzer `help ausführen`:

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

- Die Befehle `Abtastung`, `Geschichte`und `Quarantäne` zusätzliche Parameter übernehmen, die beschrieben werden, wenn der Benutzer den Befehl zusammen mit `helfen`:

```
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




      ' run 'quarantine list' first to find




       in listing
```

HINWEIS: Verwenden der `Hilfe`-Parameter, um die unterstützten Eingabeparameter für einen bestimmten Befehl bereitzustellen, mit Ausnahme der `Statushilfe`. Wann `Hilfe`mit dem CLI-Befehl status ausgegeben wird, zeigt es eine Liste aller unterstützten Steckerstatus an, mit einer kurzen Beschreibung und möglichen Gründen für jeden Status. Der aktuelle Steckerstatus ist in der Tabelle mit ** gekennzeichnet.

CLI-Befehlsverwendung

- `Abtastung`
    - `flash scannen`: Führt einen flash-scan des Systems durch.
    - `Vollständig scannen`: Führen Sie eine vollständige Systemprüfung durch.
    - `Benutzerdefiniert scannen <path_to_scan>` - eine bestimmte Datei oder ein Verzeichnis scannen.
    - `Abtastpause` - Alle derzeit ausgeführten Suchläufe anhalten.
    - `Scan-Lebenslauf` - Alle derzeit angehaltenen Suchläufe fortsetzen.
    - `Abbrechen der Suche` - alle laufenden Scans abbrechen.
    - `Scan-Liste` - Listen Sie alle geplanten Scans auf dem System durchgeführt werden.
- `status`: Zeigt den aktuellen Status des Anschlusses am System an.
    - `Statushilfe` - Anzeige einer Tabelle mit allen Steckerstatus, dem aktuellen Steckerstatus, mit Beschreibungen der einzelnen Statusstatus und den Gründen für einen bestimmten Status.

```
ampcli> status
Status:        Connected
Mode:        Normal
Scan:        Ready for scan
Last Scan:    2020-01-22 03:57 PM
Policy:        Audit Policy for Cisco Secure Endpoint (#5755)
Command-line:    Enabled
```

```
Faults:        None
```

Wenn an einem Endpunkt Fehler vorliegen, zeigt das Feld Faults (Fehler) die Anzahl der Fehler für jeden Schweregrad (Critical/Major/Minor) an. Ab Connector-Version 1.12.3 zeigt die CLI eine`Fehler-IDs`-Feld, das die Fehlercodes für jeden am Endpunkt ausgelösten Fehler anzeigt. Die CLI gibt Hinweise zu allen auf dem Endpunkt vorhandenen Fehlern aus.

Beispiel:

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

```
ampcli> status help
  Status         Description                Reason(s)
================================================================================
| Initializing...     | Program starting/loading.         | --
|             |                       |
| Provisioning...     | Endpoint identity             | --
|             | enrollment/subscription.         |
|             |                       |
| Provisioning         | Endpoint identity             | Cannot reach AMP services.
| failed, retrying     | enrollment/subscription failed.     | Missing SSL certificates.
|             | Connector will retry.         |
|             |                       |
| Registering...     | Registering endpoint identity.     | --
|             |                       |
| Registration         | Endpoint identity registration     | Cannot reach AMP services.
| failed, retrying     | failed. Connector will retry.     | Missing SSL certificates.
|             |                       |
| Connecting...     | Registering with disposition         | --
|             | service.                |
|             |                       |
| Connection failed,     | Registration with disposition     | Cannot reach AMP services.
| retrying         | service failed. Connector will     | Missing SSL certificates.
|             | retry.                 |
|             |                       |
| ** Connected         | Enrollment and registration         | --
|             | succeeded. Connected to AMP         |
|             | services. Connector is operating     |
|             | normally.                |
|             |                       |
| Disabled         | Connector is not operational.     | AMP subscription is invalid
|             |                       | or has expired.
|             |                       |
| Disconnected,     | Lost connection to the disposition     | Network connection to the
| retrying         | service after an initial         | disposition service has been
|             | connection was established.         | interrupted.
|             | Connector will attempt to         |
|             | reconnect.                |
|             |                       |
| Offline (the         | The local network has been         | Cable disconnected.
| network is down)     | disconnected.             | The network interface is
|             |                       | disabled.
```

```
|            |                     |
================================================================================
** indicates the current status of the Connector
```

Für Mac Connector Versionen 1.16.0 und neuere und für Linux Connector Versionen 1.17.0 und neuere, beinhaltet statusden aktuellen Status von Orbital auf dem Computer:

```
Orbital: Enabled (Running)
```

Es gibt drei Werte für den Orbitalstatus:

1. Enabled (Running) (Aktiviert (Wird ausgeführt)): gibt an, dass die aktuelle Richtlinie Orbital aktiviert hat und der Orbital-Dienst derzeit auf dem Computer ausgeführt wird.
2. Enabled (Not Running) (Aktiviert (Wird nicht ausgeführt)): gibt an, dass die aktuelle Richtlinie Orbital aktiviert hat, der Orbital-Dienst jedoch derzeit nicht auf dem Computer ausgeführt wird.
3. Disabled (Deaktiviert): gibt an, dass die aktuelle Richtlinie Orbital nicht aktiviert hat.

Für Mac Connector-Versionen 1.21.0 und höher (nicht unter Linux) beinhaltet status den aktuellen Status der Endpunktisolierung auf dem Computer:

```
Isolation: Isolated
```

Es gibt drei Werte für den Orbitalstatus:

1. Isolated (Isoliert): gibt an, dass die aktuelle Richtlinie die Endpunktisolierung aktiviert hat und der Computer vom Netzwerk isoliert ist.
2. Not Isolated (Nicht isoliert): gibt an, dass die aktuelle Richtlinie die Endpunktisolierung aktiviert hat und der Computer nicht isoliert ist.
3. Disabled in Policy (Deaktiviert in Richtlinie): gibt an, dass die aktuelle Richtlinie die Endpunktisolierung nicht aktiviert hat.

- `Synchronisierung` - Den Connector mit der Cloud synchronisieren, um die aktuellste Richtlinie sicherzustellen.

- `policy` - Zeigt die aktuelle Richtlinie für den Connector an:

```
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 Cisco Secure Endpoint (#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
```

Für Mac Connector-Versionen 1.16.0 und höher und für Linux Connector-Versionen 1.17.0 und höher enthält policy den Richtlinienstatus für Orbital:

```
Orbital: Enabled
```

Für die Orbitalrichtlinieneinstellung gibt es zwei Werte:

1. Enabled (Aktiviert): Orbital wird über Richtlinie aktiviert.
2. Disabled (Deaktiviert): Orbital wird über Richtlinie deaktiviert.

Für Mac Connector-Versionen 1.21.0 und höher (nicht unter Linux) enthält die Richtlinie den Richtlinienstatus für die Endpunktisolierung:

```
Isolation: Enabled
```

Es gibt zwei Werte für die Einstellung der Isolationsrichtlinie:

1. Enabled (Aktiviert): Endpunktisolierung wird über Richtlinie aktiviert.
2. Disabled (Deaktiviert): Endpunktisolierung ist über Richtlinie deaktiviert.

- `Ausschlüsse` - die aktuellen Ausschlüsse für den Anschluss anzeigen:
    - Diese Einstellung muss auch in der Connector-Richtlinie aktiviert sein, damit Ausschlüsse angezeigt werden.

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

- `Geschichte`
    - `Verlaufsliste`: Auflistung des Verlaufs der Connector-Aktivität (Scans, Quarantänen usw.)
    - `history pagesize <numeric_value>` - Legt die Seitengröße für die Verlaufsansicht fest (max. 12)

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

- `Quarantäne`(*Diese Option steht nur Benutzern mit Root-Berechtigungen zur Verfügung.*)
    - `Quarantäneliste` - die Quarantäneelemente auf dem System auflisten.

    - `quarantine restore <quarantine_id>` - Stellen Sie eine Quarantäne-Datei über die Quarantäne-ID wieder her, die Sie über den Befehl `quarantine` list finden.

- `isolieren` *(Diese Option ist nur für Mac-Connector-Versionen 1.21.0 und höher verfügbar (nicht unter Linux))*
    - `isolate stop <Token>` - Beendet die Endpunkt-Isolationssitzung mit dem Token, das zum Starten der Isolationssitzung verwendet wird.

- `about` - enthält Informationen wie Version und GUID des Connectors.

```
ampcli> about
Cisco Secure Endpoint Connector v1.16.0.123
Copyright (c) 2013-2021 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 ]
```

- `Defupdate` - eine Anforderung an die Cloud senden, um die Virendefinitionen zu aktualisieren.

- `Körperhaltung` - Steckerposition im JSON-Format anzeigen
    - `Posture Prettyprint` - Druckhaltung mit schönem Druck JSON-Format

```
ampcli> posture
{"running": true, "connected": true, "connector_version": "1.19.1.1419", "agent_uuid": "e03ecde8-1aee-4c
```

- `notify` - schaltet die Connector-Benachrichtigungen in der CLI ein/aus.
    - Diese Einstellung muss auch in der Connector-Richtlinie aktiviert werden.
    - Unter Mac hat dies keine Auswirkungen auf Benachrichtigungen in der Benutzeroberfläche.

```
ampcli> notify
Notifications set to on
```

```
ampcli> notify
Notifications set to off
```

- `ausführlich` - Aktivieren/Deaktivieren von ausführlichen Protokollen für die CLI.

```
ampcli> verbose
Verbose mode set to on
```

```
ampcli> verbose
Verbose mode set to off
```

- `quit (oder q)` - Beenden Sie die Secure Endpoint Mac/Linux Connector CLI.

Zusätzliche Informationen

Technischer Support und Dokumentation für Cisco Systeme

Cisco Secure Endpoint - Benutzerhandbuch

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.