Uso de la CLI de Mac/Linux para terminales seguros

Contenido

Introducción

Este documento describe los comandos de la Interfaz de línea de comandos (CLI) disponibles para su uso con el conector Secure Endpoint en Linux y MacOS.

Antecedentes

Los comandos de CLI están disponibles para su uso por parte de todos los usuarios de un sistema. Sin embargo, sAlgunos comandos dependen de la configuración de la política y/o de los permisos de root. Los comandos que dependen de esto se divulgan a lo largo de este artículo.

CLI de Cisco Secure Endpoint para Mac/Linux

Vaya a la CLI

La CLI de terminal seguro está disponible cuando el conector de terminal seguro está instalado y ejecutándose en el sistema:

- Abra la ventana Terminal en Mac/Linux.
- Ejecute la CLI con estas rutas:
  - en Linux:`/opt/cisco/amp/bin/ampcli`
  - en Mac:`/opt/cisco/amp/ampcli`
- Cuando se inicia la CLI, se muestra este mensaje:

```
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>
```

Comandos CLI disponibles

NOTA: todos los comandos de CLI disponibles también se pueden ejecutar directamente desde la línea de comandos; por ejemplo, `/opt/cisco/amp/bin/ampcli` helpor`/opt/cisco/amp/ampcli` **help** funciona de la misma manera que si se inicia CLI y `ejecuta ayuda`.

- Para obtener una lista completa de los comandos de CLI, el usuario puede `ejecutar help`:

```
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
```

- Los comandos `escanear`, `historial`,y `cuarentena` tomar parámetros adicionales, que se describen si el usuario ejecuta el comando junto con `auxilio`:

```
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
```

NOTE: Utilizar la `ayuda`para proporcionar los parámetros de entrada admitidos para un comando determinado, con la excepción de la `ayuda` de `estado`. Cuando `ayuda`se ejecuta con el comando status CLI, muestra una lista de todos los estados de conector admitidos, con una breve descripción y posibles razones para cada estado. El estado actual del conector se indica en la tabla mediante **.

Uso del comando CLI

- `escanear`
    - `scan flash`: realice un análisis flash del sistema.
    - `scan full` (análisis `completo`): realice un análisis completo del sistema.
    - `scan custom <path_to_scan>` : analiza un archivo o directorio especificado.
    - `pausa del análisis` - pausar los análisis que se estén ejecutando.
    - `reanudar escaneo` - reanude cualquier análisis que esté en pausa.
    - `scan cancel` - cancelar los análisis que se estén ejecutando.
    - `lista de escaneo` : enumera los análisis programados que se van a realizar en el sistema.
- `status`: indica el estado actual del conector en el sistema.
    - `ayuda de estado`: muestra una tabla de todos los estados del conector, el estado actual del conector, con descripciones de cada estado y los motivos de un estado determinado.

```
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
```

Si un terminal tiene fallos presentes, el campo Fallos muestra el número de fallos presentes para cada nivel de gravedad (Crítico/Principal/Secundario). A partir de la versión 1.12.3 del conector, la CLI muestra un`ID de fallos`, que muestra los Códigos de Falla para cada falla provocada en el punto final. La CLI proporciona orientación relacionada con cada falla presente en el terminal.

ej.:

```
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
```

Para las versiones 1.16.0 y posteriores del conector Mac y para las versiones 1.17.0 y posteriores del conector Linux, status incluye el estado actual de Orbital en el equipo:

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

Existen tres valores para el estado orbital:

1. Habilitado (en ejecución): indica que la directiva actual ha habilitado Orbital y que el servicio Orbital se está ejecutando actualmente en el equipo.
2. Habilitado (no en ejecución): indica que la directiva actual ha habilitado Orbital pero el servicio Orbital no se está ejecutando actualmente en el equipo.
3. Desactivado: indica que la política actual no ha activado Orbital.

Para las versiones 1.21.0 y posteriores del conector Mac (no en Linux), status incluye el estado actual de Endpoint Isolation en el equipo:

```
Isolation: Isolated
```

Existen tres valores para el estado orbital:

1. Aislado: indica que la directiva actual ha habilitado el aislamiento de extremos y que el equipo está aislado de la red.
2. No aislado: indica que la directiva actual ha habilitado el aislamiento de extremos y que el equipo no está aislado.
3. Deshabilitado en directiva: indica que la directiva actual no ha habilitado el aislamiento de terminales.

- `sincrónico` - sincronice el conector con la nube para garantizar la política más reciente.

- `policy` - muestra la política actual para el conector:

```
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
```

Para las versiones 1.16.0 y posteriores del conector Mac y para las versiones 1.17.0 y posteriores del conector Linux, la política incluye el estado de la política para Orbital:

```
Orbital: Enabled
```

Existen dos valores para la configuración de la directiva Orbital:

1. Habilitado: orbital está habilitado mediante directiva.
2. Desactivado: la órbita está desactivada mediante una política.

Para las versiones 1.21.0 y posteriores del conector Mac (no en Linux), la política incluye el estado de la política para el aislamiento de terminales:

```
Isolation: Enabled
```

Hay dos valores para la configuración de directiva de aislamiento:

1. Habilitado: el aislamiento de terminales se habilita mediante políticas.
2. Desactivado: el aislamiento de terminales está desactivado mediante una política.

- `exclusiones` - muestra las exclusiones actuales para el conector:
    - Esta configuración también debe estar habilitada en la directiva del conector para que se muestren las exclusiones.

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

- `historial`
    - `lista de historial`: enumera el historial de actividad del conector (análisis, cuarentenas, etc.)
    - `history pagesize <numeric_value>` - establece el tamaño de página para la vista de historial (máx. 12)

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

- `cuarentena`(*Esta opción sólo está disponible para los usuarios con privilegios raíz.*)
    - `lista de cuarentena` - enumere los elementos en cuarentena en el sistema.
    - `quarantine restore <quarantine_id>` - restaura un archivo en cuarentena a través del id de cuarentena, que se puede encontrar a través del comando `quarantine` listcommand.

- `aislar` *(Esta opción sólo está disponible para las versiones 1.21.0 y posteriores del conector Mac (no en Linux))*
  - `isolate stop <token>`: detiene la sesión de aislamiento del terminal con el token utilizado para iniciar la sesión de aislamiento

- `about`: proporciona información, como la versión y el GUID del conector.

```
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 ]
```

- `defupdar` - enviar una solicitud a la nube para actualizar las definiciones de virus.

- `postura` - show connector posture in JSON format
  - `postura prettyprint` - imprimir postura con formato JSON de impresión bonita

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

- `notify`: activa o desactiva las notificaciones del conector en la CLI.
  - Esta configuración también debe estar habilitada en la directiva del conector.
  - En Mac, esto no afecta a las notificaciones de la interfaz de usuario.

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

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

- `verboso` - activa o desactiva los registros detallados de la CLI.

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

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

- `quit (o q)` - salga de la CLI del conector Secure Endpoint para Mac/Linux.

Additional Information

Soporte Técnico y Documentación - Cisco Systems

Cisco Secure Endpoint - Guía del usuario

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).