Utiliser l'interface de ligne de commande Secure Endpoint Mac/Linux

Table des matières

Introduction

Informations générales

CLI pour Mac/Linux Cisco Secure Endpoint

- Accédez à la CLI
- Commandes CLI disponibles
- Utilisation des commandes CLI
- Additional Information

Introduction

Ce document décrit les commandes CLI (Command Line Interface) disponibles pour être utilisées avec le connecteur Secure Endpoint sous Linux et MacOS.

Informations générales

Les commandes CLI peuvent être utilisées par tous les utilisateurs d'un système ; cependant, certaines commandes dépendent de la configuration de la stratégie et/ou de l'autorisation racine. Les commandes qui en dépendent sont décrites tout au long de cet article.

CLI pour Mac/Linux Cisco Secure Endpoint

Accédez à la CLI

L'interface de ligne de commande Secure Endpoint est disponible lorsque le connecteur Secure Endpoint est installé et exécuté sur le système :

- Ouvrez la fenêtre Terminal sur Mac/Linux.
- Exécutez l'outil CLI dans les chemins suivants :
  - sous Linux : `/opt/cisco/amp/bin/ampcli`
  - sur Mac : `/opt/cisco/amp/ampcli`
- Lorsque l'interface de ligne de commande démarre, le message suivant s'affiche :

```
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>
```

Commandes CLI disponibles

REMARQUE : toutes les commandes CLI disponibles peuvent également être exécutées directement à partir de la ligne de commande, par exemple`/opt/cisco/amp/bin/ampcli helpor`/opt/cisco/amp/ampcli help fonctionne de la même manière que si vous démarriez l'interface de ligne de commande et que vous exécutez l'aide.

- Pour obtenir la liste complète des commandes CLI, l'utilisateur peut `exécuter l'aide` :

```
ampcli> help
    about               About Cisco Secure Endpoint connector
    bp                  Show and sync behavioral protection signatures
                         * See 'bp help' for more.
    clamav              Show and sync ClamAV definitions
                         * See 'clamav help' for more.
    connectivity-test   Run connection tests
                         * See 'connectivity-test help' for more.
    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
```

- Les commandes bp, clamav, connectivity-test, history , `scan`, et quarantinetake prennent des paramètres supplémentaires, qui sont décrits si l'utilisateur exécute la commande avec l'`aide` :

```
ampcli> bp help
Supported bp parameters:
  status        Display engine and definition information
  sync          Synchronizes BP signatures
```

```
ampcli> clamav help
```

```
Supported clamav parameters:
  status        Display engine and definition information
  sync          Synchronizes ClamAV definitions



ampcli> connectivity-test help
Supported connectivity-test parameters:
  all           Performs all connectivity tests
  bpsig         Performs a Behavioral Protection signature fetch test
  crashdump     Performs an upload test of a crash diagnostic
  event         Verifies connectivity to the event intake server
  hc            Performs a minimal connection test with the registration server
  orbitalupdate Performs an orbital update download test
  policy        Performs a policy fetch test of the current policy. A policy serial number can be provi
                 * Usage: 'policy [serial number]' (optional serial number, must be greater than 0)
  fileupload    Performs a file upload test
  update        Performs a connector update download test



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> 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> 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
```

REMARQUE : utilisez le paramètre help pour fournir les paramètres d'entrée pris en charge pour une commande donnée, à l'exception de l'`aide` sur l'`état`. Lorsque la commande status CLI est utilisée, elle affiche une liste de tous les états de connecteur pris en charge, avec une brève description et les raisons possibles de chaque état. L'état actuel du connecteur est indiqué dans le tableau par **.

Utilisation des commandes CLI

- `about` - fournit des informations, telles que la version et le GUID du connecteur.

```
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 ]
```

- `bp`(Cette option n'est disponible que pour les versions 1.22.0+ sur Linux et 1.24.0+ sur macOS)
    - `status` - affiche le moteur de protection comportementale et les informations de définition
        - Si la protection comportementale n'est pas activée, aucune information de moteur ou de signature supplémentaire n'est fournie :

```
ampcli> bp status
Behavioral Protection is not enabled
```

        - Si la protection comportementale est activée, les informations relatives au moteur, au mode et à la signature sont affichées :

```
ampcli> bp status
APDE Engine Version:            3.1.0.0
BP Mode:                        Protect
BP Signature Serial Number:     8071
```

```
BP Signature Last Loaded:         2023-05-02 05:44:09 PM
```

    - `sync` - synchroniser les signatures de la protection comportementale

- `clamav`
    - `état` - affichage des informations relatives au moteur clamav et à sa définition

```
ampcli> clamav status
Definition Version:       ClamAV(bytecode.cvd: 334, daily.cvd: 26893, main.cvd: 62)
Definitions Published:    bytecode.cvd: 22 Feb 2023 16-33 -0500
                          daily.cvd: 01 May 2023 03-22 -0400
                          main.cvd: 16 Sep 2021 08-32 -0400
Definitions Last Updated: 2023-05-01 04:01:55 PM
```

    - `sync` - synchroniser les signatures clamav

- `test de connectivité`
    - `all` - Effectue tous les tests de connectivité
    - `bpsig` - Effectue un test d'extraction de signature de protection comportementale
    - `crashdump` - Effectue un test de téléchargement d'un diagnostic de panne
    - `event` - Vérifie la connectivité au serveur d'accueil d'événements
    - `hc` - Effectue un test de connexion minimal avec le serveur d'enregistrement
    - `orbitalupdate` - Effectue un test de téléchargement de mise à jour orbitale
    - `policy [numéro de série]` - Effectue un test d'extraction de stratégie de la stratégie actuelle. Un numéro de série de politique peut être fourni pour extraire une politique spécifique
    - `fileupload` - Effectue un test de téléchargement de fichier
    - `update` - Effectue un test de téléchargement de la mise à jour du connecteur

- `defupdate` : envoie une demande de mise à jour des définitions de virus au cloud.

- `exclusions` - affiche les exclusions actuelles pour le connecteur :
    - Ce paramètre doit également être activé dans la stratégie de connecteur pour que les exclusions s'affichent.

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

- `historique`
    - `liste historique` - répertorie l'historique de l'activité des connecteurs (analyses, quarantaines, etc.)

    - `history pagesize <numeric_value>` - définit la taille des pages pour la vue d'historique (12 max.)

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

- `isolate` (Cette option est uniquement disponible pour les versions 1.21.0 et ultérieures du connecteur Mac (pas sur Linux))
    - `isolate stop <token>` - arrête la session d'isolation du point d'extrémité avec le jeton utilisé pour démarrer la session d'isolation
- `notify` : active/désactive les notifications du connecteur dans l'interface de ligne de commande.
    - Ce paramètre doit également être activé dans la stratégie de connecteur.
    - Sur Mac, cela n'affecte pas les notifications dans l'interface utilisateur.

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

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

- `policy` - affiche la stratégie actuelle pour le connecteur :

```
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
```

Pour les connecteurs Mac versions 1.16.0 et ultérieures et pour les connecteurs Linux versions 1.17.0 et ultérieures, la stratégie inclut l'état de la stratégie pour Orbital :

```
Orbital: Enabled
```

Il existe deux valeurs pour le paramètre de stratégie Orbitale :

1. Activée: Orbital est activé via la politique.
2. Désactivé: Orbital est désactivé via la politique.

Pour les versions 1.21.0 et ultérieures du connecteur Mac (pas sous Linux), la stratégie inclut l'état de la stratégie pour Endpoint Isolation :

```
Isolation: Enabled
```

Il existe deux valeurs pour le paramètre de stratégie Isolation :

1. Activée: L'isolation des terminaux est activée via une stratégie.
2. Désactivé: L'isolation des points de terminaison est désactivée via une stratégie.

- `posture` - affiche la position du connecteur au format JSON
    - `posture prettyprint` - imprimer posture avec jolie impression format JSON

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

- `quarantine`(Cette option n'est disponible que pour les utilisateurs disposant de privilèges root.)
    - `liste de quarantaine` - répertorie les éléments mis en quarantaine sur le système.
    - `quarantine restore <quarantine_id>` - restaure un fichier mis en quarantaine via l'id de quarantaine, qui peut être trouvé via la commande `quarantine` list.
- `quit (ou q)` : quittez l'interface de ligne de commande du connecteur Secure Endpoint Mac/Linux.
- `scanographie`
    - `scan flash` : effectuez une analyse flash du système.
    - `scan full (analyse complète)` : analyse complète du système.
    - `scan custom <path_to_scan>` - analyse un fichier ou répertoire spécifié.
    - `pause d'analyse` - interrompt toutes les analyses en cours.
    - `reprise de l'analyse` - reprendre toutes les analyses actuellement suspendues.
    - `annuler l'analyse` - annule toutes les analyses en cours.
    - `scan list` - répertorie toutes les analyses planifiées à effectuer sur le système.
- `status` : indique l'état actuel du connecteur sur le système.

- `aide sur l'état` - affiche un tableau de tous les états de connecteur, l'état actuel du connecteur, avec des descriptions de chaque état et les raisons d'un état donné.

```
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 présente des défaillances, le champ Faults indique le nombre de défaillances présentes pour chaque niveau de gravité (Critique/Majeur/Mineur). À partir de la version 1.12.3 du connecteur, l'interface de ligne de commande affiche le champ `Fault` IDsfield, qui affiche les codes de panne pour chaque panne déclenchée sur le point d'extrémité. L'interface de ligne de commande fournit des conseils relatifs à chaque défaut présent sur le point d'extrémité.

ex :

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

```
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
Run "ampcli connectivity-test" to help diagnose connection errors
```

Pour les connecteurs Mac versions 1.16.0 et ultérieures et pour les connecteurs Linux versions 1.17.0 et ultérieures, l'état inclut l'état actuel d'Orbital sur l'ordinateur :

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

Il existe trois valeurs pour l'état orbital :

1. Activé (en cours) : indique que la stratégie actuelle a activé Orbital et que le service Orbital est en cours d'exécution sur l'ordinateur.
2. Activé (non en cours d'exécution) : indique que la stratégie actuelle a activé Orbital mais que le service Orbital n'est pas en cours d'exécution sur l'ordinateur.
3. Désactivé: indique que la stratégie actuelle n'a pas activé Orbital.

Pour les versions 1.21.0 et ultérieures du connecteur Mac (pas sous Linux), l'état inclut l'état actuel de l'isolation des points de terminaison sur l'ordinateur :

```
Isolation: Isolated
```

Il existe trois valeurs pour l'état orbital :

1. Isolé : indique que la stratégie actuelle a activé l'isolation des points de terminaison et que l'ordinateur est isolé du réseau.
2. Non isolé : indique que la stratégie actuelle a activé l'isolation des points de terminaison et que l'ordinateur n'est pas isolé.
3. Désactivé dans la stratégie : indique que la stratégie actuelle n'a pas activé l'isolation des

terminaux.

- `sync` : synchronisez le connecteur avec le cloud pour garantir la dernière stratégie.
- `verbose` - active/désactive les journaux de verbose pour l'interface de ligne de commande.

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

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

Additional Information

[Assistance et documentation techniques - Cisco Systems]

[Cisco Secure Endpoint - Guide de l'utilisateur]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.