セキュアエンドポイントMac/Linux CLIの使用

内容

はじめに

このドキュメントでは、LinuxおよびMacOS上のSecure Endpoint Connector(SEEM)で使用できるコマンドラインインターフェイス(CLI)コマンドについて説明します。

背景説明

CLIコマンドは、システム上のすべてのユーザが使用できますが、一部のコマンドは、ポリシー設定やルート権限によって異なります。これに依存するコマンドは、この記事の全体を通して開示されています。

Cisco Secure Endpoint Mac/Linux CLI

CLIに移動します。

Secure Endpoint CLIは、Secure Endpointコネクタがシステムにインストールされ、実行されている場合に使用できます。

- Mac/Linuxでターミナルウィンドウを開きます。
- 次のパスを使用してCLIを実行します。
  - linuxの場合：`/opt/cisco/amp/bin/ampcli`
  - Macの場合：`/opt/cisco/amp/ampcli`
- CLIが起動すると、次のメッセージが表示されます。

```
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>
```

使用可能なCLIコマンド

注：使用可能なすべてのCLIコマンドは、コマンドラインから直接実行することもできます。たとえば、/opt/cisco/amp/bin/ampcli helpor/opt/cisco/amp/ampcli helpworksは、CLIとrunhelpを起動した場合と同じです。

- CLIコマンドの完全なリストについては、ユーザはrunhelpを実行できます。

```
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.
    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
```

- コマンドスキャン、履歴、quarantine、clamav、およびbptake追加パラメータを設定します。これらのパラメータは、ユーザがこのサイトについて：を入力します。

```
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









ampcli> clamav help
Supported clamav parameters:
  status        Display engine and definition information
  sync          Synchronizes ClamAV definitions



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

注：ヘルプを使用するstatus helpを除く、指定されたコマンドでサポートされる入力パラメータを提供するパラメータを参照。ヘルプの表示時status CLIコマンドを使用して発行すると、サポートされているすべてのコネクタ状態のリストが、各ステータスの簡単な説明と考えられる理由とともに表示されます。現在のコネクタのステータスは、**によって表に示されます。

CLIコマンドの使用方法

- about：コネクタのバージョンやGUIDなどの情報を提供します。

```
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(このオプションは、Linuxコネクタバージョン1.22.0以降でのみ使用できます（Macでは使用できません）)。
  - status：動作保護エンジンおよび定義情報の表示
    - 動作保護が有効になっていない場合は、エンジンまたはシグニチャの追加情報は提供されません。

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

    - 動作保護を有効にすると、エンジン、モード、およびシグニチャ情報が表示されます。

```
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：動作保護シグニチャを同期します

- クラマフ
  - status:clamavエンジンおよび定義情報の表示

```
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:clamavシグニチャを同期します。

- デアップデート – クラウドにウイルス定義の更新要求を送信します。

- 除外 – コネクタの現在の除外を表示します。
    - 除外を表示するには、コネクタポリシーでこの設定を有効にする必要があります。

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

- 履歴
    - history list：コネクタアクティビティの履歴（スキャン、検疫など）をリストします。
    - history pagesize <numeric_value>：履歴ビューのページサイズを設定します（最大12）。

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

- 分離する (このオプションは、Macコネクタバージョン1.21.0以降でのみ使用できます（Linuxでは使用できません）)。
    - isolate stop <token>：分離セッションの開始に使用されたトークンでエンドポイント分離セッションを停止します。

- notify:CLIでのコネクタ通知のオン/オフを切り替えます。
    - この設定は、コネクタポリシーでも有効にする必要があります。
    - Macでは、これはUIの通知には影響しません。

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

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

- policy：コネクタの現在のポリシーを表示します。

```
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
```

Macコネクタバージョン1.16.0以降およびLinuxコネクタバージョン1.17.0以降の場合、policyにはOrbitalのポリシーステータスが含まれます。

```
Orbital: Enabled
```

[軌道]ポリシー設定には、次の2つの値があります。

1. [有効]：オービタルはポリシーによって有効になります。
2. [無効]：オービタルはポリシーによって無効にされています。

Macコネクタバージョン1.21.0以降（Linux以外）の場合、policyにはEndpoint Isolationのポリシーステータスが含まれます。

```
Isolation: Enabled
```

Isolationポリシー設定には、次の2つの値があります。

1. Enabled：エンドポイントの分離がポリシーによって有効になっています。
2. Disabled：エンドポイントの分離は、ポリシーによって無効にされています。

- ポスチャ - JSON形式でコネクタポスチャを表示します
  - posture prettyprint:プリティプリントJSON形式でポスチャを印刷します。

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

- quarantine(このオプションは、ルート権限を持つユーザだけが使用できます。)
  - 検疫リスト – システム上の隔離された項目をリストします。
  - quarantine restore

<quarantine_id>：検疫idを使用して、検疫されたファイルを復元します。これは、quarantine listcommandコマンドを使用して確認できます。

- quit （またはq） - Secure Endpoint Mac/LinuxコネクタのCLIを終了します。
- スキャン
  - scan flash：システムのフラッシュスキャンを実行します。
  - scan full：システムのフルスキャンを実行します。
  - スキャンカスタム<path_to_scan> – 指定したファイルまたはディレクトリをスキャンします。
  - スキャン一時停止 – 現在実行中のスキャンを一時停止します。
  - スキャン再開 – 現在一時停止されているスキャンを再開します。
  - スキャンキャンセル – 現在実行中のスキャンをすべてキャンセルします。
  - スキャンリスト – システムで実行するスケジュール済みスキャンを一覧表示します。
- status：システム上のコネクタの現在のステータスを示します。
  - ステータスヘルプ:すべてのコネクタステータス、現在のコネクタステータス、各ステータスの説明、および特定のステータスの理由を示すテーブルを表示します。

```
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
```

エンドポイントに障害が存在する場合、[障害]フィールドには、各重大度レベル（クリティカル/メジャー/マイナー）に存在する障害の数が表示されます。コネクタバージョン1.12.3では、CLIに障害IDフィールドに入力します。このフィールドには、エンドポイントで発生した各障害の障害コードが表示されます。CLIは、エンドポイントに存在する各障害に関するガイダンスを出力します。

例：

```
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 failed, retrying | Endpoint identity enrollment/subscription failed. Connector will retry. | Cannot reach AMP services. Missing SSL certificates.
| Registering... | Registering endpoint identity. | --
| Registration failed, retrying | Endpoint identity registration failed. Connector will retry. | Cannot reach AMP services. Missing SSL certificates.
| Connecting... | Registering with disposition service. | --
| Connection failed, retrying | Registration with disposition service failed. Connector will retry. | Cannot reach AMP services. Missing SSL certificates.
| ** 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, retrying | Lost connection to the disposition service after an initial connection was established. Connector will attempt to reconnect. | Network connection to the disposition service has been interrupted.
| Offline (the network is down) | The local network has been disconnected. | Cable disconnected. The network interface is disabled.

** indicates the current status of the Connector

Macコネクタバージョン1.16.0以降およびLinuxコネクタバージョン1.17.0以降の場合、statusにはコンピュータ上のOrbitalの現在のステータスが含まれます。

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

軌道ステータスには、次の3つの値があります。

1. 有効（実行中）：現在のポリシーでOrbitalが有効になっており、Orbitalサービスが現在コンピューターで実行されていることを示します。
2. 有効（実行されていません）：現在のポリシーでOrbitalが有効になっていますが、Orbitalサービスが現在コンピューターで実行されていないことを示します。

3. [無効]：現在のポリシーでオービタルが有効になっていないことを示します。

Macコネクタバージョン1.21.0以降（Linux以外）の場合、statusincludesにはコンピュータのエンドポイント分離の現在のステータスが含まれます。

```
Isolation: Isolated
```

軌道ステータスには、次の3つの値があります。

1. [分離]：現在のポリシーでエンドポイントの分離が有効になっており、コンピューターがネットワークから分離されていることを示します。
2. 非分離：現在のポリシーでエンドポイントの分離が有効になっており、コンピューターが分離されていないことを示します。
3. Disabled in Policy：現在のポリシーでエンドポイントの分離が有効になっていないことを示します。

- `sync` – コネクタをクラウドと同期して、最新のポリシーを確認します。
- `冗長` - CLIの詳細ログのオン/オフを切り替えます。

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

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

追加情報

テクニカル サポートとドキュメント - Cisco Systems

Cisco Secure Endpoint – ユーザガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。