使用安全终端Mac/Linux CLI

目录

[简介](#)

[背景信息](#)

[思科安全终端Mac/Linux CLI](#)

- [导航至CLI](#)
- [可用的CLI命令](#)
- [CLI命令用法](#)
- [其他信息](#)

简介

本文档介绍可用于Linux和MacOS上的安全终端连接器的命令行界面(CLI)命令。

背景信息

CLI命令可供系统上的所有用户使用；但是，某些命令取决于策略配置和/或根权限。依赖于此的命令将在本文中介绍。

思科安全终端Mac/Linux CLI

导航至CLI

当系统上安装并运行安全终端连接器时，安全终端CLI可用：

- 打开Mac/Linux上的Terminal（终端）窗口。
- 使用以下路径运行CLI:
  - 在Linux上:`/opt/cisco/amp/bin/ampcli`
  - 在Mac上:`/opt/cisco/amp/ampcli`
- 当CLI启动时，将显示以下消息：

```
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>
```

可用的CLI命令

注意：所有可用的CLI命令也可直接从命令行运行，例如/opt/cisco/amp/bin/ampcli helpor/opt/cisco/amp/ampcli helpworks与启动CLI和runhelp相同。

- 对于CLI命令的完整列表，用户可以运行help:

```
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
```

- 命令 扫描, 历史记录, 隔离 clamav和bptake additional parameters，如果用户随同运行该命令，则会对其进行描述 帮助:

```
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
```

NOTE:使用帮助参数，为给定命令提供支持的输入参数，状态帮助除外除外.获得帮助使用status CLI命令发出，它将显示所有支持的连接器状态的列表，以及每种状态的简短说明和可能原因。表格中当前连接器状态由**表示。

CLI命令用法

- about — 提供连接器的版本和GUID等信息。

```
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(此选项仅适用于Linux连接器版本1.22.0及更高版本（不在Mac上））
  - status — 显示行为保护引擎和定义信息
    - 如果未启用行为保护，则不提供其他引擎或签名信息：

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

    - 如果启用了行为保护，则会显示引擎、模式和签名信息：

```
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 — 同步行为保护签名
- 克拉马夫
  - 状态 — 显示clamav引擎和定义信息

```
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 — 同步clamav签名
- defupdate — 向云发送更新病毒定义的请求。
- 排除 — 显示连接器的当前例外项：
  - 此设置还必须在连接器策略中启用，以便显示例外项。

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

- 历史记录
  - history list — 列出连接器活动的历史记录（扫描、隔离区等）
  - history pagesize <numeric_value> — 设置历史记录视图的pagesize（最多12个）

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

- 隔离 (此选项仅适用于Mac连接器版本1.21.0及更高版本（不适用于Linux））
  - isolate stop <token> — 使用用于启动隔离会话的令牌停止终端隔离会话

- notify — 在CLI中打开/关闭连接器通知。
  - 此设置还必须在连接器策略中启用。
  - 在Mac上，这不会影响用户界面中的通知。

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

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

- policy — 显示连接器的当前策略：

```
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
```

对于Mac连接器版本1.16.0及更高版本，对于Linux连接器版本1.17.0及更高版本，策略包括Orbital的策略状态：

```
Orbital: Enabled
```

轨道策略设置有两个值：

1. 已启用：通过策略启用轨道。
2. 禁用：通过策略禁用轨道。

对于Mac连接器版本1.21.0及更高版本（不在Linux上），策略包括终端隔离的策略状态：

```
Isolation: Enabled
```

隔离策略设置有两个值：

1. 已启用：通过策略启用终端隔离。
2. 已禁用：通过策略禁用终端隔离。

- 状态 — 以JSON格式显示连接器状态
  - posture prettyprint - pretty print JSON格式的打印状态

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

- 隔离(此选项仅对具有root权限的用户可用。)
  - 隔离列表 — 列出系统上的隔离项目。
  - quarantine restore <quarantine_id> — 通过隔离id(可通过quarantine lists命令找到)恢复隔离文件。
- quit（或q） — 退出安全终端Mac/Linux连接器CLI。
- 扫描
  - scan flash — 执行系统的快速扫描。
  - scan full — 执行系统的完全扫描。
  - scan custom <path_to_scan> — 扫描指定的文件或目录。
  - 扫描暂停 — 暂停当前运行的所有扫描。
  - 扫描恢复 — 恢复所有当前暂停的扫描。
  - 扫描取消 — 取消当前运行的所有扫描。
  - 扫描列表 — 列出要在系统上执行的所有计划扫描。

- status — 提供系统上连接器的当前状态。
    - 状态帮助 — 显示一个表，其中包含所有连接器状态、当前连接器状态、每个状态状态的说明以及给定状态的原因。

```
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
```

如果端点存在故障，故障字段显示每个严重性级别（严重/主要/次要）的故障数。从连接器版本1.12.3开始，CLI显示故障ID字段，显示终端上出现的每个故障的故障代码。CLI输出与终端上存在的每个故障相关的指南。

例如：

```
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
```

对于Mac连接器版本1.16.0及更高版本，对于Linux连接器版本1.17.0及更高版本，状态包括计算机上轨道的当前状态：

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

轨道状态有三个值：

1. Enabled(Running)：表示当前策略已启用Orbital，并且Orbital服务当前正在计算机上运行。
2. Enabled(Not Running)：表示当前策略已启用Orbital，但Orbital服务当前未在计算机上运行。
3. 已禁用：表示当前策略未启用轨道。

对于Mac连接器版本1.21.0及更高版本（不在Linux上），status包括计算机上终端隔离的当前状态：

```
Isolation: Isolated
```

轨道状态有三个值：

1. 隔离：表示当前策略已启用终端隔离，并且计算机与网络隔离。
2. Not Isolated：表示当前策略已启用Endpoint Isolation，且计算机未隔离。
3. Disabled in Policy：表示当前策略未启用Endpoint Isolation。

- 同步 — 将连接器与云同步以确保最新策略。
- 详细 — 打开/关闭CLI的详细日志。

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

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

其他信息

[技术支持和文档 - Cisco Systems]

[思科安全终端 — 用户指南]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。