보안 엔드포인트 Mac/Linux CLI 사용

목차

[소개](#)

[배경 정보](#)

[Cisco Secure Endpoint Mac/Linux CLI](#)

- [CLI로 이동합니다](#)
- [사용 가능한 CLI 명령](#)
- [CLI 명령 사용](#)
- [추가 정보](#)

소개

이 문서에서는 Linux 및 MacOS의 보안 엔드포인트 커넥터에서 사용할 수 있는 CLI(Command Line Interface) 명령에 대해 설명합니다.

배경 정보

CLI 명령은 시스템의 모든 사용자가 사용할 수 있지만일부 명령은 정책 컨피그레이션 및/또는 루트 권한에 따라 달라집니다. 이에 종속된 명령은 이 기사 전반에 걸쳐 개시되어 있다.

Cisco Secure Endpoint Mac/Linux CLI

CLI로 이동합니다

Secure Endpoint CLI는 시스템에 Secure Endpoint Connector가 설치되어 실행 중일 때 사용할 수 있습니다.

- Mac/Linux에서 터미널 창을 엽니다.
- 다음 경로로 CLI를 실행합니다.
  - Linux: `/opt/cisco/amp/bin/ampcli`
  - mac: `/opt/cisco/amp/ampcli`
- CLI가 시작되면 다음 메시지가 표시됩니다.

```
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>
```

사용 가능한 CLI 명령

참고: 사용 가능한 모든 CLI 명령은 명령줄에서 직접 실행할 수도 있습니다. 예를 들어 /opt/cisco/amp/bin/ampcli help 또는/opt/cisco/amp/ampcli help는 CLI를 시작하고 runhelp를 시작하는 경우와 동일합니다.

- 전체 CLI 명령 목록의 경우 사용자는 다음을 실행할 수 있습니다.

```
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
```

- 명령 스캔, 역사, 격리 , clamav, bptake 추가 매개 변수. 사용자가 명령을 실행할 때 도움말:

```
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
```

참고:도움말 사용상태 도움말을 제외하고 지정된 명령에 대해 지원되는 입력 매개 변수를 제공하는 매개 변수입니다. 도움이 필요한 경우status CLI 명령을 실행하면 지원되는 모든 커넥터 상태의 목록이 표시되며 각 상태에 대한 간단한 설명과 가능한 이유가 표시됩니다. 현재 커넥터 상태는 테이블에 기본적으로 **.

CLI 명령 사용

- 정보 - 커넥터의 버전 및 GUID와 같은 정보를 제공합니다.

```
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(이 옵션은 Linux 커넥터 버전 1.22.0 이상에서만 사용할 수 있으며 Mac에서는 사용할 수 없습니다.)
  - 상태 - 동작 보호 엔진 및 정의 정보 표시
    - 동작 보호가 활성화되어 있지 않으면 추가 엔진 또는 서명 정보가 제공되지 않습니다.

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

    - 동작 보호가 활성화된 경우 엔진, 모드 및 서명 정보가 표시됩니다.

```
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 - 동작 보호 시그니처 동기화

- 클라마프
  - status - clamav 엔진 및 정의 정보 표시

```
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 서명 동기화

- 해동 - 클라우드에 바이러스 정의를 업데이트하라는 요청을 보냅니다.
- 제외 - 커넥터에 대한 현재 제외 항목을 표시합니다.
    - 제외를 표시하려면 커넥터 정책에서도 이 설정을 활성화해야 합니다.

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

- 역사
    - `history list` - 커넥터 활동 기록(스캔, 격리 등)을 나열합니다.
    - `history pagesize <numeric_value>` - 기록 보기의 페이지 크기를 설정합니다(최대 12).

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

- 격리됨 (이 옵션은 Mac 커넥터 버전 1.21.0 이상에서만 사용할 수 있습니다(Linux에서는 사용할 수 없음).
    - `isolate stop <token>` - 격리 세션을 시작하는 데 사용되는 토큰으로 엔드포인트 격리 세션을 중지합니다.
- `notify` - CLI에서 커넥터 알림을 설정/해제합니다.
    - 이 설정은 커넥터 정책에서도 활성화해야 합니다.
    - Mac에서는 UI의 알림에 영향을 주지 않습니다.

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

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

- `policy` - 커넥터에 대한 현재 정책을 표시합니다.

```
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 커넥터 버전 1.16.0 이상 및 Linux 커넥터 버전 1.17.0 이상의 경우 정책에는 Orbital에 대한 정책 상태가 포함됩니다.

```
Orbital: Enabled
```

Orbital 정책 설정에는 두 가지 값이 있습니다.

1. Enabled(활성화됨): Orbital이 정책을 통해 활성화됩니다.
2. Disabled(비활성화됨): 정책을 통해 Orbital을 비활성화합니다.

Mac 커넥터 버전 1.21.0 이상(Linux에는 없음)의 경우 정책에는 엔드포인트 격리에 대한 정책 상태가 포함됩니다.

```
Isolation: Enabled
```

격리 정책 설정에는 두 가지 값이 있습니다.

1. Enabled(활성화됨): 정책을 통해 엔드포인트 격리가 활성화됩니다.
2. Disabled(비활성화됨): 정책을 통해 엔드포인트 격리를 비활성화합니다.

- 상태 - JSON 형식의 커넥터 상태 표시
  - `posture prettyprint` - 예쁜 인쇄 JSON 형식의 인쇄 상태

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

- 격리(이 옵션은 루트 권한이 있는 사용자만 사용할 수 있습니다.)
  - 쿼런틴 목록 - 시스템의 격리된 항목을 나열합니다.
  - `quarantine restore <quarantine_id>` - quarantine listcommand를 통해 찾을 수 있는 quarantine id를 통해 격리된 파일을 복원합니다.
- `quit(또는 q)` - Secure Endpoint Mac/Linux 커넥터 CLI를 종료합니다.

- 스캔
    - scan flash(플래시 스캔) - 시스템의 플래시 스캔을 수행합니다.
    - scan full(전체 스캔) - 시스템의 전체 스캔을 수행합니다.
    - 스캔 사용자 지정 <path_to_scan> - 지정한 파일 또는 디렉터리를 검사합니다.
    - 스캔 일시 중지 - 현재 실행 중인 스캔을 일시 중지합니다.
    - 스캔 다시 시작 - 현재 일시 중지된 스캔을 다시 시작합니다.
    - 스캔 취소 - 현재 실행 중인 스캔을 취소합니다.
    - 검사 목록 - 시스템에서 수행할 예약된 스캔을 나열합니다.
- status - 시스템에 있는 커넥터의 현재 상태를 제공합니다.
    - 상태 도움말 - 모든 커넥터 상태, 현재 커넥터 상태, 각 상태 설명 및 특정 상태에 대한 이유를 보여 줍니다.

```
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
```

엔드포인트에 결함이 있는 경우, Faults 필드에는 심각도 수준(Critical/Major/Minor)별로 존재하는 결함의 수가 표시됩니다. 커넥터 버전 1.12.3부터 CLI에는결함 ID필드 - 엔드포인트에서 발생한 각 결함의 Fault Codes(결함 코드)를 표시합니다. CLI는 엔드포인트에 있는 각 결함과 관련된 지침을 출력합니다.

예:

```
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
```

Mac 커넥터 버전 1.16.0 이상 및 Linux 커넥터 버전 1.17.0 이상의상태에는 컴퓨터의 Orbital의 현재 상태가 포함됩니다.

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

Orbital 상태에는 세 가지 값이 있습니다.

1. Enabled(실행 중): 현재 정책이 Orbital을 활성화했으며 컴퓨터에서 Orbital 서비스가 현재 실행 중임을 나타냅니다.
2. Enabled (Not Running)(활성화됨(실행 중이 아님)): 현재 정책에서 Orbital을 활성화했지만 컴퓨터에서 Orbital 서비스가 현재 실행되고 있지 않음을 나타냅니다.
3. Disabled(비활성화됨): 현재 정책이 Orbital을 활성화하지 않았음을 나타냅니다.

Mac 커넥터 버전 1.21.0 이상(Linux가 아님)의 경우 상태에는 컴퓨터의 엔드포인트 격리의 현재 상태가 포함됩니다.

```
Isolation: Isolated
```

Orbital 상태에는 세 가지 값이 있습니다.

1. Isolated(격리): 현재 정책에서 엔드포인트 격리를 활성화했으며 컴퓨터가 네트워크에서 격리되었음을 나타냅니다.
2. Not Isolated(격리되지 않음): 현재 정책에서 엔드포인트 격리를 활성화했으며 컴퓨터가 격리되지 않았음을 나타냅니다.
3. Disabled in Policy(정책에서 비활성화됨): 현재 정책이 엔드포인트 격리를 활성화하지 않았음을 나타냅니다.

- 동기화 - 커넥터를 클라우드와 동기화하여 최신 정책을 확인합니다.
- 말이 많 - CLI에 대한 자세한 정보 로그를 설정/해제합니다.

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

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

추가 정보

[기술 지원 및 문서 – Cisco Systems]

[Cisco Secure Endpoint - 사용 설명서]

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.