ä½¿ç”¨å®‰å…¨çµ‚ç«¯Mac/Linux CLI

ç›®éŒ„

ç°¡ä»‹

æœ¬æ–‡æª”ä»‹ç´¹å�¯ç”¨æ–¼Linuxå’ŒMacOSä¸Šçš„å®‰å…¨çµ‚ç«¯è�¯çµ�å™¨çš„å‘½ä»¤åˆ—ä»‹é�

èƒŒæ™¯è³‡è¨Š

CLIå‘½ä»¤å�¯ä¾›ç³»çµ±ä¸Šçš„æ‰€æœ‰ä½¿ç”¨è€…ä½¿ç”¨ï¼›ä½†æ˜¯ï¼ŒæŸ�äº›å‘½ä»¤å�–æ±ºæ–

Ciscoå®‰å…¨çµ‚ç«¯Mac/Linux CLI

å°Žè¦½è‡³CLI

åœ¨ç³»çµ±ä¸Šå®‰è£�ä¸¦é�‹è¡Œå®‰å…¨çµ‚ç«¯è�¯çµ�å™¨æ™‚ï¼Œå®‰å…¨çµ‚ç«¯CLIå�¯ç”¨ï¼š

- é–‹å•ŸMac/Linuxä¸Šçš„Terminalè¦–çª—ã€‚
- ä½¿ç”¨ä»¥ä¸‹è·¯å¾‘é�‹è¡ŒCLI:
  - åœ¨Linuxä¸Š:`/opt/cisco/amp/bin/ampcli`
  - åœ¨Macä¸Š:`/opt/cisco/amp/ampcli`
- CLIå•Ÿå‹•æ™‚ï¼Œç³»çµ±æœƒé¡¯ç¤ºä»¥ä¸‹æ¶ˆæ�¯ï¼š

```
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>
```

å�¯ç”¨çš„CLIå‘½ä»¤

æ³¨æ„�ï¼šæ‰€æœ‰å�¯ç”¨çš„CLIå‘½ä»¤ä¹Ÿå�¯ç›´æŽ¥å¾žå‘½ä»¤åˆ—é�‹è¡Œï¼Œä¾‹å¦‚`/opt/c`
helpor`/opt/cisco/amp/ampcli` helpworksèˆ‡å•Ÿå‹•CLIå’Œ`runhelp`çš„ç›¸å�Œã€‚

- å¦‚éœ€å®Œæ•´çš„CLIå‘½ä»¤æ¸…å–®ï¼Œä½¿ç”¨è€…å�¯ä»¥åŸ·è¡Œhelp:

```
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
```

- æŒ‡ä»¤ æžƒæ� �ä¸ï¼Œ æ·å�²ä¸ï¼Œ éš”é›¢ ã€�clamavå’Œbptakeé™„åŠ å¼•æ•¸ï¼Œé€™äº›å¼•æ•¸åœ¨ä

```
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
```

é™„è¨»ï¼šä½¿ç”¨å¹«åŠ©å¼•æ•¸ç‚ºç¦å®šå‘½ä»¤æ��ä¾›æ”¯æ�´çš„è¼¸å…¥å¼•æ•¸ï¼Œç‹€æ…‹å¹«åŠ©é™¤å
CLIå‘½ä»¤ç™¼å‡ºçš„ï¼Œå®ƒé¡¯ç¤ºæ‰€æœ‰æ”¯æ�´çš„è�¯çµ�å™¨ç‹€æ…‹çš„æ¸…å–®ï¼Œä»¥å�Šæ¯

CLIå‘½ä»¤ç”¨æ³•

- about â€” æ��ä¾›è�¯çµ�å™¨çš„ç‰ˆæœ¬å’ŒGUIDç‰è³‡è¨Šã€,

```
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*(æ¤é�¸é …åƒ…é�©ç”¨æ–¼Linuxè�¯çµ�å™¨ç‰ˆæœ¬1.22.0å�Šæ›´é«˜ç‰ˆæœ¬ï¼ˆä¸�é�©ç”¨*
    - status â€” é¡¯ç¤ºè¡Œç‚ºä¿�è·å¼•æ“Žå’Œå®šç¾©è³‡è¨Š
        - å¦‚æžœæœªå•Ÿç”¨è¡Œç‚ºä¿�è·ï¼Œå‰‡ä¸�æœ�ä¾›å…¶ä»–å¼•æ“Žæˆ–ç°½å��è³‡è¨Š

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

        - å¦‚æžœå•Ÿç”¨è¡Œç‚ºä¿�è·ï¼Œå‰‡æœƒé¡¯ç¤ºå¼•æ“Žã€�æ¨¡å¼�å’Œç°½å��è³‡è¨Šï

```
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 â€” å�Œæ¥è¡Œç‚ºä¿�è·ç°½å��

- å…‹æ‹‰é¦¬ä¼•
    - ç‹€æ…‹ â€” é¡¯ç¤ºçˆ¬ç¶²å¼•æ“Žå’Œå®šç¾©è³‡è¨Š

```
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 â€” å�Œæ¥claavç°½å��

- defupdate â€” å�‘é›²å¸³é€�æ›´æ–°ç—…æ¯’å®šç¾©çš„è«‹æ±‚ã€‚

- æŽ’é™¤ â€” é¡¯ç¤ºè�¯çµ�å™¨çš„ç•¶å‰�æŽ’é™¤é …ï¼š
    - æ¤è¨å®šé‚„å¿…é ˆåœ¨è�¯çµ�å™¨ç–ç•¥ä¸å•Ÿç”¨ï¼Œä»¥ä¾¿é¡¯ç¤ºæŽ’é™¤ã€‚

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

- æ·å�²
    - history list â€”
      åˆ—å‡ºè

�¯çµ�å™¨æ´»å‹•çš„æ·å�²è¨˜éŒ„ï¼ˆæŽƒæ��ã€�éš”é›¢å�€ç‰ï¼‰
  - `history pagesize <numeric_value>` â€” è¨å®šæ·å�²è¨˜éŒ„æª¢è¦–çš„pagesizeï¼ˆæœ€å¤š12å€‹ï¼‰

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

- å¤ç«‹
  (æ¤é�¸é …åƒ…é�©ç”¨æ–¼Macè�¯çµ�å™¨ç‰ˆæœ¬1.21.0å�Šæ›´é«˜ç‰ˆæœ¬ï¼ˆä¸�é�©ç”¨æ–
  - `isolate stop <token>` â€” ä½¿ç”¨ç”¨æ–¼å•Ÿå‹•éš”é›¢æœƒè©±çš„ä»¤ç‰Œå�œæ¢çµ‚ç«¯éš”é›¢æœƒè©±
- `notify` â€” åœ¨CLIä¸é–‹å•Ÿ/é—œé–‰è�¯çµ�å™¨é€šçŸ¥ã€‚
  - å¿…é ˆåœ¨è�¯çµ�å™¨ç–ç•¥ä¸å•Ÿç”¨æ¤è¨å®šã€‚
  - åœ¨Macä¸Šï¼Œé€™ä¸�æœƒå½±éŸ¿UIä¸çš„é€šçŸ¥ã€‚

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

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

- `policy` â€” é¡¯ç¤ºè�¯çµ�å™¨çš„ç•¶å‰�ç–ç•¥ï¼š

```
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
```

å°�æ–¼Macè�¯çµ�å™¨ç‰ˆæœ¬1.16.0å’Œæ›´é«˜ç‰ˆæœ¬ï¼Œå°�æ–¼Linuxè�¯çµ�å™¨ç‰ˆæœ

```
Orbital: Enabled
```

è»Œé�“æ”¿ç–è¨å®šæœ‰å…©å€‹å€¼ï¼š

1. å·²å•Ÿç”¨ï¼šé€šé�Žç–ç•¥å•Ÿç”¨è»Œé�“ã€‚
2. å·²ç¦�ç”¨ï¼šé€šé�Žç–ç•¥ç¦�ç”¨è»Œé�“ã€‚

å°�æ–¼Macè�¯çµ�å™¨ç‰ˆæœ¬1.21.0å�Šæ›´é«˜ç‰ˆæœ¬ï¼ˆä¸�åœ¨Linuxä¸Šï¼‰ï¼Œç–ç•¥åŒ..

```
Isolation: Enabled
```

éš”é›¢ç–ç•¥è¨å®šæœ‰å…©å€‹å€¼ï¼š

1. å·²å•Ÿç”¨ï¼šé€šé�Žç–ç•¥å•Ÿç”¨çµ‚ç«¯éš”é›¢ã€‚
2. å·²ç¦�ç”¨ï¼šé€šé�Žç–ç•¥ç¦�ç”¨çµ‚ç«¯éš”é›¢ã€‚

- ç‹€æ…‹ â€” ä»¥JSONæ ¼å¼�é¡¯ç¤ºè�¯çµ�å™¨ç‹€æ…‹
  - `posture prettyprint` - åˆ—å�°å¸¶æœ‰æ¼‚äº®åˆ—å�°JSONæ ¼å¼�çš„posture

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

- éš”é›¢(*æ¤é�¸é …åƒ…å°�å…·æœ‰rootè¨±å�¯æ¬Šçš„ä½¿ç”¨è€…å�¯ç”¨ã€‚*)
  - éš”é›¢æ¸…å–® â€” åˆ—å‡ºç³»çµ±ä¸Šçš„éš”é›¢å°ˆæ¡ˆã€‚
  - `quarantine restore <quarantine_id>` â€” é€šé�Žéš”é›¢id(å�¯é€šé�Žquarantine listå‘½ä»¤æ‰¾å ˆ°)æ�¢å¾©éš”é›¢æª”æ¡ˆã€‚
- `quitï¼ˆæˆ–qï¼‰` â€” é€€å‡ºå®‰å…¨çµ‚ç«¯Mac/Linuxè�¯çµ�å™¨CLIã€‚
- æŽƒæ� �
  - `scan flash` â€” åŸ·è¡Œç³»çµ±çš„å¿«é€Ÿè¨˜æ†¶é«”æŽƒæ��ã€‚
  - `scan full` â€” åŸ·è¡Œç³»çµ±çš„å®Œå…¨æŽƒæ��ã€‚
  - æŽƒæ� �è‡ªå®šç¾©<path_to_scan> â€” æŽƒæ��æŒ‡å®šçš„æª”æ¡ˆæˆ–ç›®éŒ„ã€‚
  - æŽƒæ� �æš«å�œ â€” æš«å�œç•¶å‰�é�‹è¡Œçš„æ‰€æœ‰æŽƒæ��ã€‚
  - æŽƒæ� �æ�¢å¾© â€” æ�¢å¾©ç•¶å‰�æš«å�œçš„æ‰€æœ‰æŽƒæ��ã€‚
  - æŽƒæ� �å�–æ¶ˆ â€” å�–æ¶ˆç•¶å‰�é�‹è¡Œçš„æ‰€æœ‰æŽƒæ��ã€‚
  - æŽƒæ� �æ¸…å–® â€” åˆ—å‡ºè¦�åœ¨ç³»çµ±ä¸ŠåŸ·è¡Œçš„æ‰€æœ‰è¨ˆç•«æŽƒæ��ã€‚
- `status` â€” æ��ä¾›ç³»çµ±ä¸Šè�¯çµ�å™¨çš„ç•¶å‰�ç‹€æ…‹ã€‚
  - ç‹€æ…‹å¹«åŠ©-é¡¯ç¤ºä¸€å€‹è¨ï¼Œå…¶ä¸åŒ…å�«æ‰€æœ‰è�¯çµ�å™¨ç‹€æ…‹ã€�ç•¶å‰�è�¯çµ�å™

```
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
```

å¦‚æžœç«¯é»žå˜åœ¨æ•…éšœï¼Œã€Œæ•…éšœã€�æ¬„ä½�å°‡é¡¯ç¤ºæ¯�å€‹åš´é‡�æ€§çš„åˆ¥ï¼ˆåš´é‡�/ä

ä¾‹å¦‚ï¼š

```
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
```

å°�æ–¼Macè�¯çµ�å™¨ç‰ˆæœ¬1.16.0å’Œæ›´é«˜ç‰ˆæœ¬ï¼Œå°�æ–¼Linuxè�¯çµ�å™¨ç‰ˆæœ

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

è»Œé�“ç‹€æ…‹æœ‰ä¸‰å€‹å€¼ï¼š

1. å·²å•Ÿç”¨ï¼ˆæ£åœ¨é�‹è¡Œï¼‰ï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥å·²å•Ÿç”¨Orbitalï¼Œä¸¦ä¸"Orbitalæœ�å‹™ç
2. å·²å•Ÿç”¨ï¼ˆæœªé�‹è¡Œï¼‰ï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥å·²å•Ÿç”¨Orbitalï¼Œä½†Orbitalæœ�å‹™ç•¶å
3. å·²ç¦�ç"¨ï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥æœªå•Ÿç"¨è»Œé�"ã€‚

å°�æ–¼Macè�¯çµ�å™¨ç‰ˆæœ¬1.21.0å�Šæ›´é«˜ç‰ˆæœ¬ï¼ˆä¸�é�©ç"¨æ–¼Linuxï¼‰ï¼Œç‹€æ

```
Isolation: Isolated
```

è»Œé�“ç‹€æ…‹æœ‰ä¸‰å€‹å€¼ï¼š

1. Isolatedï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥å·²å•Ÿç"¨ç«¯é»žéš"é›¢ï¼Œä¸¦ä¸"é›»è…¦è¨ç¶²è·¯éš"é›¢ã€‚
2. Not Isolatedï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥å·²å•Ÿç"¨Endpoint Isolationï¼Œä½†é›»è…¦æœªéš"é›¢ã€‚
3. Disabled in Policyï¼šè¡¨ç¤ºç•¶å‰�ç–ç•¥æœªå•Ÿç"¨ç«¯é»žéš"é›¢ã€‚

- å�Œæ¥ â€" å°‡è�¯çµ�å™¨è¨å®šç‚ºå¾žé›²å�Œæ¥ä»¥ç¢ºä¿�æœ€æ–°ç–ç•¥ã€‚
- è©³ç´° â€" é–‹å•Ÿ/é—œé–‰CLIçš„è©³ç´°æ—¥èªŒã€‚

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

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

å…¶ä»–è³‡è¨Š

[æŠ€è¡"æ"¯æ�´èˆ‡æ–‡ä»¶ - Cisco Systems]()

æ€�ç§‘å®‰å…¨çµ‚ç«¯ â€” ä½¿ç”¨æ‰‹å†Š