Uso della CLI di Secure Endpoint Mac/Linux

Sommario

Introduzione

In questo documento vengono descritti i comandi dell'interfaccia della riga di comando (CLI) disponibili per l'uso con il connettore Secure Endpoint su Linux e MacOS.

Premesse

i comandi CLI sono disponibili per l'uso da parte di tutti gli utenti di un sistema; tuttavia, sAlcuni comandi dipendono dalla configurazione dei criteri e/o dalle autorizzazioni della directory principale. I comandi dipendenti da questa funzione sono illustrati in questo articolo.

CLI di Cisco Secure Endpoint Mac/Linux

Passare alla CLI

Secure Endpoint CLI è disponibile quando il connettore Secure Endpoint è installato e in esecuzione sul sistema:

- Aprire la finestra Terminale su Mac/Linux.
- Eseguire la CLI con questi percorsi: su Linux:`/opt/cisco/amp/bin/ampcli` su Mac:`/opt/cisco/amp/ampcli`
- All'avvio della CLI, viene visualizzato questo messaggio:

```
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>
```

Comandi CLI disponibili

NOTA: tutti i comandi CLI disponibili possono essere eseguiti direttamente dalla riga di comando, ad esempio`/opt/cisco/amp/bin/ampcli` helpor`/opt/cisco/amp/ampcli` helpworks come se si avviasse CLI e `runhelp`.

- Per un elenco completo dei comandi CLI, l'utente può `eseguire` la `guida`:

```
ampcli> help scan Initiate/pause/stop a scan * See 'scan help' for more. status Get ampdaemon
status
* See 'status help' for more. sync Sync policy policy Show policy exclusions List custom
exclusions history Show event history * See 'history help' for more. quarantine List/restore
quarantined file(s) * See 'quarantine help' for more. about About Cisco Secure Endpoint
Connector defupdate Update virus definitions
posture Show Connector posture in JSON format notify Toggle notifications verbose Toggle verbose
mode q Quit ampcli interactive mode
```

- I comandi `scansione`, `cronologia`,e `quarantena` accetta parametri aggiuntivi, descritti se l'utente esegue il comando insieme a `Help`:

```
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
```

NOTA: Utilizzare la `Guida`per fornire i parametri di input supportati per un determinato comando, ad eccezione della `guida sullo stato`. Quando `aiuto`viene emesso con il comando status CLI e visualizza un elenco di tutti gli stati dei connettori supportati, con una breve descrizione e i possibili motivi per ciascuno stato. Lo stato corrente del connettore è indicato nella tabella da **.

Uso del comando CLI

- `scansionescansione flash`: eseguire una scansione flash del sistema.`scansione completa`: eseguire una scansione completa del sistema.`scan custom <percorso_scansione>` - eseguire la scansione di un file o di una directory specificata.`pausa scansione` - sospendere le analisi in esecuzione.`ripresa dell'analisi` - riprendere le analisi in pausa.`annulla scansione` - annullare tutte le analisi in esecuzione.`elenco di scansione` - elencare tutte le scansioni pianificate da eseguire sul sistema.

- `status` - fornisce lo stato corrente del connettore sul sistema. `guida sullo stato`: visualizza una tabella con tutti gli stati dei connettori, lo stato corrente del connettore, con le descrizioni di ciascuno stato e i motivi per un determinato stato.

```
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
```

Se un endpoint presenta errori, il campo Errori mostra il numero di errori presenti per ciascun livello di gravità (Critico/Maggiore/Minore). A partire dalla versione 1.12.3 del connettore, la CLI mostra un`ID errore`che mostra i codici di errore per ogni errore generato sull'endpoint. La CLI restituisce le linee guida relative a ciascun errore presente sull'endpoint.

es:

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


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
```

Per il connettore Mac versione 1.16.0 e successive e per il connettore Linux versione 1.17.0 e successive, statusinclude lo stato corrente di Orbital sul computer:

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

Esistono tre valori per lo stato orbitale:

1. Abilitato (in esecuzione): indica che il criterio corrente ha abilitato Orbital e che il servizio Orbital è attualmente in esecuzione nel computer.
2. Abilitato (non in esecuzione): indica che il criterio corrente ha abilitato Orbital ma il servizio Orbital non è attualmente in esecuzione nel computer.
3. Disabilitato: indica che il criterio corrente non ha abilitato Orbital.

Per il connettore Mac versione 1.21.0 e successive (non su Linux), statusinclude lo stato corrente di Isolamento degli endpoint sul computer:

```
Isolation: Isolated
```

Esistono tre valori per lo stato orbitale:

1. Isolato: indica che il criterio corrente ha attivato l'isolamento degli endpoint e che il computer è isolato dalla rete.
2. Non isolato: indica che il criterio corrente ha attivato l'isolamento degli endpoint e che il computer non è isolato.
3. Disattivato nei criteri: indica che i criteri correnti non hanno attivato l'isolamento degli endpoint.

- `sincronizzazione` - sincronizzare il connettore con il cloud per garantire i criteri più recenti.

- `criterio`: visualizza il criterio corrente per il connettore:

```
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
```

Per il connettore Mac versione 1.16.0 e successive e per il connettore Linux versione 1.17.0 e successive, il criterio include lo stato del criterio per Orbital:

```
Orbital: Enabled
```

Esistono due valori per l'impostazione della politica Orbital:

1. Abilitato: Orbital è abilitato tramite criteri.
2. Disabilitato: orbitale disabilitato tramite criteri.

Per il connettore Mac versione 1.21.0 e successive (non su Linux), il criterio include lo stato del criterio per Isolamento endpoint:

```
Isolation: Enabled
```

Esistono due valori per l'impostazione del criterio Isolamento:

1. Abilitato: l'isolamento degli endpoint è abilitato tramite i criteri.
2. Disabilitato: l'isolamento degli endpoint è disabilitato tramite i criteri.

- `esclusioni` - visualizzare le esclusioni correnti per il connettore: Per visualizzare le esclusioni, è inoltre necessario attivare questa impostazione nel criterio dei connettori.

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

- `cronologia`
  `elenco cronologia` - elenca la cronologia dell'attività del connettore (analisi, quarantene e così via)`history pagesize <numeric_value>` - imposta le dimensioni della pagina per la vista cronologia (max 12)

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

- `quarantena`(*Questa opzione è disponibile solo per gli utenti con privilegi root.*) `elenco quarantena` - elencare gli elementi in quarantena nel sistema.`quarantine restore <quarantine_id>` - ripristina un file in quarantena tramite l'id di quarantena, disponibile tramite il comando `quarantine` list.

- `isolare` *(Questa opzione è disponibile solo per il connettore Mac versione 1.21.0 e successive (non su Linux))*
  `isolate stop <token>` - arresta la sessione di isolamento dell'endpoint con il token utilizzato per avviare la sessione di isolamento

- `about` - fornisce informazioni, ad esempio la versione e il GUID del connettore.

```
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 ]
```

- `disaggiornare` - inviare una richiesta al cloud per aggiornare le definizioni dei virus.

- `postura` - mostra la postura del connettore in formato JSON `posture pretyprint` - posture di stampa con formato JSON

```
ampcli> posture
{"running": true, "connected": true, "connector_version": "1.19.1.1419", "agent_uuid":
"e03ecde8-1aee-4d15-8bca-100e952ee4b9", "offline_engine": "ClamAV", "offline_engine_version":
"0.103.5", "definition_version": "osx.cvd:1152", "last_definition_update_published": "osx.cvd:
05 May 2022 13-00 -0400", "last_definition_update_success": 1651857785, "last_scan": 1651857897,
"last_scan_status": false, "protect_file_mode": true, "protect_process_mode": true, "scans":
[{"scan_type": "flash", "scan_in_progress": false, "last_scan_finished": 1651857039},
{"scan_type": "full", "scan_in_progress": false, "last_scan_finished": 1651857897},
{"scan_type": "custom", "scan_in_progress": false, "last_scan_finished": 1651856819}],
"engines": [{"enabled": true, "name": "ClamAV", "version": "0.103.5", "definitions":
[{"version": 1152, "name": "osx.cvd", "timestamp": 1651770000, "last_successful_update":
1651857785}]}]}
```

- `notification` - attiva/disattiva le notifiche dei connettori nella CLI. Questa impostazione deve essere attivata anche nel criterio del connettore.In Mac, ciò non influisce sulle notifiche nell'interfaccia utente.

```
ampcli> notify Notifications set to on

ampcli> notify Notifications set to off
```

- `dettagliato` - attiva/disattiva i log dettagliati per la CLI.

```
ampcli> verbose Verbose mode set to on

ampcli> verbose Verbose mode set to off
```

- `d` - uscire dalla CLI del connettore Mac/Linux dell'endpoint protetto.

Ulteriori informazioni

[Documentazione e supporto tecnico – Cisco Systems]

[Cisco Secure Endpoint - Guida per l'utente]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).