Usar a CLI do Secure Endpoint para Mac/Linux

Contents

Introduction

Este documento descreve os comandos CLI (Command Line Interface, interface de linha de comando) disponíveis para uso com o conector Secure Endpoint no Linux e no MacOS.

Informações de Apoio

Os comandos CLI estão disponíveis para uso por todos os usuários de um sistema; no entanto, sAlguns comandos dependem da configuração da política e/ou das permissões raiz. Os comandos que dependem disso são divulgados em todo este artigo.

Cisco Secure Endpoint Mac/Linux CLI

Navegue até a CLI

A CLI do Secure Endpoint está disponível quando o conector do Secure Endpoint está instalado e em execução no sistema:

- Abra a janela Terminal no Mac/Linux.
- Execute o CLI com estes caminhos:
  - no Linux:`/opt/cisco/amp/bin/ampcli`
  - no Mac:`/opt/cisco/amp/ampcli`
- Quando o CLI for iniciado, esta mensagem será exibida:

```
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>
```

Comandos CLI disponíveis

OBSERVAÇÃO: todos os comandos CLI disponíveis também podem ser executados diretamente da linha de comando, por exemplo`/opt/cisco/amp/bin/ampcli` helpor**/opt/cisco/amp/ampcli** ajuda funciona da mesma forma como se você iniciasse o CLI e `runhelp`.

- Para obter uma lista completa de comandos CLI, o usuário pode `executar help`:

```
ampcli> help
    about               About Cisco Secure Endpoint connector
    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
```

- Os comandos `varredura`, `histórico`,e `quarentena` obter parâmetros adicionais, que são descritos se o usuário executar o comando junto com `ajuda`:

```
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
```

NOTE: Use a `ajuda`parâmetro para fornecer os parâmetros de entrada suportados para um determinado comando, com exceção da `ajuda de status`. Quando `ajuda`é emitido com o comando CLI status, ele exibe uma lista de todos os estados de conectores suportados, com uma breve descrição e possíveis motivos para cada status. O status do conector atual é indicado na tabela por **.

Uso do comando CLI

- `varredura`
    - `scan flash`- executa uma varredura flash do sistema.
    - `scan full`- executa uma varredura completa do sistema.
    - `scan custom <path_to_scan>` - verificar um arquivo ou diretório especificado.
    - `pausa de varredura` - pause todas as varreduras em execução no momento.
    - `continuar varredura` - retoma todas as varreduras em pausa no momento.
    - `verificar cancelar` - cancele qualquer varredura em execução no momento.
    - `lista de verificação` - liste todas as varreduras programadas a serem executadas no sistema.
- `status` - fornece o status atual do conector no sistema.
    - `ajuda de status`- exibe uma tabela de todos os status do conector, o status atual do conector, com descrições de cada estado de status e os motivos de um determinado estado.

```
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 um endpoint tiver falhas presentes, o campo Falhas mostrará o número de falhas presentes para cada nível de gravidade (Crítico/Principal/Secundário). A partir da versão 1.12.3 do conector, a CLI mostra um`IDs de falha`, que mostra os Códigos de Falha para cada falha levantada no ponto final. A CLI fornece orientações relacionadas a cada falha presente no endpoint.

ex.:

```
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
```

Para as versões 1.16.0 e mais recentes do conector Mac e para as versões 1.17.0 e mais recentes do conector Linux, o status inclui o status atual do Orbital no computador:

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

Existem três valores para o estado Orbital:

1. Ativado (Em execução): indica que a política atual ativou o Orbital e que o serviço Orbital está em execução no computador.
2. Ativado (Não está em execução): indica que a política atual ativou o Orbital, mas que o serviço Orbital não está em execução no computador.
3. Desativado: indica que a política atual não ativou o Orbital.

Para as versões 1.21.0 e mais recentes do conector Mac (não no Linux), o status inclui o status atual do Endpoint Isolation no computador:

```
Isolation: Isolated
```

Existem três valores para o estado Orbital:

1. Isolado: indica que a política atual habilitou o Isolamento de Ponto de Extremidade e que o computador está isolado da rede.
2. Não Isolado: indica que a política atual habilitou o Isolamento de Ponto de Extremidade e que o computador não está isolado.
3. Desabilitado na Política: indica que a política atual não habilitou o Isolamento de Ponto de Extremidade.

- `sync` - sincronize o conector com a nuvem para garantir a política mais recente.

- `policy` - mostra a política atual para o conector:

```
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
```

Para as versões 1.16.0 e mais recentes do conector Mac e para as versões 1.17.0 e mais recentes do conector Linux, a política inclui o status da política para Orbital:

```
Orbital: Enabled
```

Há dois valores para a configuração de política Orbital:

1. Habilitado: Orbital é habilitado por meio da política.
2. Desativado: Orbital é desativado por meio da política.

Para as versões 1.21.0 e mais recentes do conector Mac (não no Linux), a política inclui o status da política para o Endpoint Isolation:

```
Isolation: Enabled
```

Há dois valores para a configuração da política de Isolamento:

1. Habilitado: o Isolamento de Ponto de Extremidade está habilitado via política.
2. Desabilitado: o Isolamento de Ponto de Extremidade está desabilitado via política.

- `exclusões` - mostrar as exclusões atuais do conector:
    - Essa configuração também deve ser habilitada na política de conectores para que as exclusões sejam exibidas.

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

- `histórico`
    - `lista do histórico` - lista o histórico da atividade do conector (varreduras, quarentenas etc.)
    - `history pagesize <numeric_value>` - define o tamanho da página para a exibição do histórico (máx. 12)

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

- `quarentena`(*Essa opção está disponível apenas para usuários com privilégios de raiz.*)
    - `lista de quarentena` - liste os itens em quarentena no sistema.
    - `quarantine restore <quarantine_id>` - restaura um arquivo em quarentena por meio da id de quarentena, que pode ser encontrada por meio do comando `quarantine` list.

- `isolar` *(Essa opção só está disponível para as versões 1.21.0 e posteriores do conector Mac (não no Linux))*
  - `isolate stop <token>` - para a sessão de isolamento de ponto final com o token usado para iniciar a sessão de isolamento

- `about` - fornece informações, como a versão e o GUID do conector.

```
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 ]
```

- `defupdate` - envie uma solicitação à nuvem para atualizar as definições de vírus.

- `postura` - show connector posture no formato JSON
  - `postura de impressão` - postura de impressão com formato JSON de impressão bonita

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

- `notify` - ativa/desativa as notificações do conector na CLI.
  - Essa configuração também deve ser habilitada na política de conector.
  - No Mac, isso não afeta as notificações na interface do usuário.

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

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

- `detalhamento` - ativar/desativar registros verbosos da CLI.

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

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

- `quit (ou q)` - saia da CLI do conector Secure Endpoint Mac/Linux.

Additional Information

Suporte Técnico e Documentação - Cisco Systems

Endpoint Cisco Secure - Guia do usuário

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.