コマンドライン インターフェイス

この章で説明する内容は、次のとおりです。

- コマンド ライン インターフェイスの概要 （1 ページ）
- コマンドライン インターフェイスへのアクセス （1 ページ）
- 汎用 CLI コマンド （5 ページ）
- Web セキュリティアプライアンス CLI コマンド （6 ページ）

コマンド ライン インターフェイスの概要

AsyncOS コマンドライン インターフェイス（CLI）を使用して、Web セキュリティアプライアンス を設定したりモニタすることができます。コマンドライン インターフェイスには、それらのサービスがイネーブルに設定されている IP インターフェイスで SSH を使用してアクセスするか、シリアルポートで端末エミュレーション ソフトウェアを使用してアクセスできます。デフォルトでは、SSH は管理ポートに設定されます。

コマンドは、引数の有無を問わず、コマンド名を入力すると起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報の入力を求めるプロンプトが表示されます。

コマンドライン インターフェイスへのアクセス

以下のいずれかの方法で接続できます。

- **イーサネット。**Web セキュリティアプライアンス の IP アドレスを使用して SSH セッションを開始します。工場出荷時のデフォルト IP アドレスは 192.168.42.42 です。SSH は、ポート 22 を使用するように設定されています。
- **シリアル接続**シリアル ケーブルが接続されているパーソナル コンピュータの通信ポートを使用して、ターミナル セッションを開始します。

初回アクセス

admin アカウントを使用して初めて CLI にアクセスした後は、さまざまな許可レベルにより他のユーザーを追加できます。以下のデフォルトの **admin** ユーザー名とパスフレーズを入力してアプライアンスにログインします。

- ユーザー名：**admin**
- パスフレーズ：**ironport**

デフォルトのパスフレーズで初めてログインすると、システム セットアップ ウィザードのプロンプトにより **admin** アカウントのパスフレーズを変更するよう求められます。

admin アカウントのパスフレーズは、`passwd` コマンドを使用していつでもリセットできます。

以降のアクセス

有効なユーザー名とパスフレーズを使用して、いつでもアプライアンス接続してログインできます。現在のユーザー名での最近のアプライアンスへのアクセス試行（成功、失敗を含む）の一覧が、ログイン時に自動的に表示されることに注意してください。

追加のユーザーの設定については、`userconfig` コマンド、または ユーザー アカウントの管理 を参照してください。

コマンド プロンプトの使用

最上位のコマンド プロンプトは、完全修飾ホスト名に続いて大なり（>）記号とスペース 1 つで構成されます。次に例を示します。

```
example.com>
```

コマンドを実行すると、CLI によりユーザーの入力が要求されます。CLI が入力を待機しているときは、プロンプトとして、角カッコ（[]）で囲まれたデフォルト値の後ろに大なり記号（>）が表示されます。デフォル値がない場合、カッコ内は空です。

次に例を示します。

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

デフォルト設定がある場合は、コマンドプロンプトのカッコ内にその設定が表示されます。次に例を示します。

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
```

```
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

デフォルト設定が表示されたときにReturnキーを押すと、デフォルト値を受け入れたことになります。

コマンドの構文

インタラクティブモードで操作している場合、CLIコマンド構文は単一のコマンドから構成されます。スペースは含まれず、引数やパラメータもありません。次に例を示します。

```
example.com> logconfig
```

選択リスト

入力できる複数の選択肢がある場合、コマンドによっては番号付きリストを使用します。プロンプトで選択する番号を入力します。

次に例を示します。

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Yes/No クエリー

yesまたはnoのオプションがある場合、質問はデフォルト値（カッコ内表示）を付けて表示されます。**Y**、**N**、**Yes**、または **No** で返答できます。大文字と小文字の区別はありません。

次に例を示します。

```
Do you want to enable the proxy? [Y]> Y
```

サブコマンド

一部のコマンドでは、NEW、EDIT、DELETE などのサブコマンド命令を使用できます。EDIT および DELETE 関数では、設定されている値のリストが表示されます。

次に例を示します。

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
```

```
- DELETE - Remove an interface.
[]>
```

サブコマンド内からメイン コマンドに戻るには、空のプロンプトで Enter または Return を押します。

サブコマンドのエスケープ

サブコマンド内ではいつでも Ctrl+C キーボード ショートカットを使用して、ただちに最上位の CLI に戻ることができます。

コマンド履歴

CLI は、セッション中に入力されたすべてのコマンドの履歴を保持します。最近使用したコマンドの実行リストをスクロールするには、キーボードの上下矢印キーを使用するか、Ctrl+P キーと Ctrl+N キーを組み合わせて使用します。

コマンドのオートコンプリート

AsyncOS CLI は、コマンド補完機能をサポートしています。コマンドの先頭の数文字を入力して Tab キーを押すと、CLI によって残りの文字列が補完されます。入力した文字が複数のコマンドに該当する場合、CLI はそのセットをさらに「絞り込み」ます。次に例を示します。

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

CLI を使用した設定変更の確定

- 設定の変更の多くは、確定するまで有効になりません。
- `commit` コマンドを使用すると、他の操作を通常どおりに実行しながら設定を変更できます。
- 変更を正常に確定するには、最上位のコマンドプロンプトになっている必要があります。コマンド ライン階層の 1 つ上のレベルに移動するには、空のプロンプトで Return キーを押します。
- 確定されていない設定の変更は記録されますが、`commit` コマンドを実行するまで有効になりません。ただし、一部のコマンドは `commit` コマンドを実行しなくても有効になります。CLI セッションの終了、システムのシャットダウン、再起動、障害、または `clear` コマンドの発行により、確定されていない変更はクリアされます。
- ユーザーが確認とタイムスタンプを受け取るまで、変更は実際に確定されません。

汎用 CLI コマンド

ここでは、変更の確定やクリアなど、一般的なCLIセッションで使用される基本的なコマンドについて説明します。

CLI の例：設定変更の確定

commit コマンドの後のコメントの入力は任意です。

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

CLI の例：設定変更のクリア

clear コマンドは、commit または clear コマンドが最後に実行された以降にアプライアンスの設定に対して行われた変更をすべてクリアします。

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

CLI の例：コマンドライン インターフェイス セッションの終了

exit コマンドを実行すると、CLI アプリケーションからログアウトされます。確定されていない設定変更はクリアされます。

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

CLI の例：コマンドライン インターフェイスでのヘルプの検索

help コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。help コマンドは、コマンド プロンプトで help と入力するか、疑問符（?）を 1 つ入力して実行できます。

```
example.com> help
```

さらに、**help** commandname を入力して、特定のコマンドのヘルプにアクセスできます。

関連項目

- Web セキュリティアプライアンス CLI コマンド （6 ページ）

Web セキュリティアプライアンス CLI コマンド

Web セキュリティアプライアンス の CLI は、システムへのアクセスおよびシステムのアップグレードと管理を実行する、一連のプロキシコマンドと UNIX コマンドをサポートしています。

（注） すべての CLI コマンドをすべての動作モード（標準およびクラウド Web セキュリティ コネクタ）で適用/使用できるわけではありません。

adminaccessconfig

Web セキュリティアプライアンス の設定で、アプライアンスにログインする管理者に対して厳しいアクセス要件を設け、非アクティブ タイムアウトの値を指定できます。詳細については、アプライアンスの割り当てに対するセキュリティ設定の追加と ユーザー ネットワーク アクセスを参照してください。

advancedproxyconfig

Web プロキシの詳細オプションを設定します。サブコマンドは以下のとおりです。

AUTHENTICATION：認証設定オプション。

- When would you like to forward authorization request headers to a parent proxy
- Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog
- Would you like to log the username that appears in the request URI
- Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)
- Would you like to use advanced Active Directory connectivity checks
- Would you like to allow case insensitive username matching in policies
- Would you like to allow wild card matching with the character * for LDAP group names
- Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]
- Would you like to enable referrals for LDAP
- Would you like to enable secure authentication
- Enter the hostname to redirect clients for authentication
- Enter the surrogate timeout for user credentials

- Enter the surrogate timeout for machine credentials
- Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability
- Enter re-auth on request denied option [disabled / embedlinkinblockpage]
- Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication
- Configure username and IP address masking in logs and reports

CACHING：プロキシ キャッシュ モード。以下のうち 1 つを選択します。

- Safe Mode
- Optimized Mode
- Aggressive Mode
- Customized Mode

Web プロキシのキャッシュ モードの選択も参照してください。

DNS：DNS 設定オプション。

- Enter the URL format for the HTTP 307 redirection on DNS lookup failure
- Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure
- Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive
- Do you want to disable IP address in Host Header
- Find web server by:

  0 = Always use DNS answers in order

  1 = Use client-supplied address then DNS

  2 = Limited DNS usage

  3 = Very limited DNS usage

  デフォルト値は 0 です。オプション 1 および 2 では、[Webレピュテーション（Web Reputation）]がイネーブルに設定されている場合、DNS が使用されます。オプション 2 および 3 では、DNS は、アップストリーム プロキシがない場合、または設定されたアップストリームプロキシが失敗するイベントで、明示的なプロキシ要求に使用されます。すべてのオプションで、[宛先 IP アドレス（Destination IP Addresses）]がポリシー メンバーシップで使用されている場合、DNS が使用されます。

EUN：エンドユーザー通知パラメータ。

- Choose:

  1. Refresh EUN pages

  2. Use Custom EUN pages

コマンドライン インターフェイス

3. Use Standard EUN pages

- Would you like to turn on presentation of the User Acknowledgement page?

Web プロキシ使用規約と エンドユーザー通知の概要も参照してください。

NATIVEFTP：ネイティブ FTP の設定。

- Would you like to enable FTP proxy
- Enter the ports that FTP proxy listens on
- Enter the range of port numbers for the proxy to listen on for passive FTP connections
- Enter the range of port numbers for the proxy to listen on for active FTP connections
- Enter the authentication format:

  1. Check Point
  2. No Proxy Authentication
  3. Raptor

- Would you like to enable caching
- Would you like to enable server IP spoofing
- Would you like to pass FTP server welcome message to the clients
- Enter the max path size for the ftp server directory

FTP プロキシ サービスの概要も参照してください。

FTPOVERHTTP：FTP Over HTTP オプション。

- Enter the login name to be used for anonymous FTP access
- Enter the password to be used for anonymous FTP access

FTP プロキシ サービスの概要も参照してください。

HTTPS：HTTPS 関連のオプション。

- HTTPS URI Logging Style - fulluri or stripquery
- Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose
- Would you like to decrypt HTTPS requests for End User Notification purpose
- Action to be taken when HTTPS servers ask for client certificate during handshake:

  1. Pass through the transaction
  2. Reply with certificate unavailable

- Do you want to enable server name indication (SNI) extension?
- Do you want to enable automatic discovery and download of missing Intermediate Certificates?

- `Do you want to enable session resumption?`

HTTPS トラフィックを制御する復号ポリシーの作成：概要も参照してください。

SCANNING：スキャン オプション。

- `Would you like the proxy to do malware scanning all content regardless of content type`
- `Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds`
- `Do you want to disable Webroot body scanning`

マルウェア対策スキャンの概要と 発信トラフィックのスキャンの概要も参照してください。

SCANNERS： AMP エンジンによるスキャンからの MIME タイプの除外が可能。scanners サブコマンドを使用するには、「Adaptive Scanning」機能を無効にする必要があります。このサブコマンドを使用して、 AMP エンジンでスキャンする必要のない MIME タイプを追加し、スキャンのパフォーマンスを向上させることができます。デフォルトの MIME タイプのオプションは、「image/ALL and text/ALL」です。

MIME タイプを追加するには、デフォルトのオプションの後に追加する必要があります。たとえば、ビデオと音声の MIME タイプを追加する場合は、次の形式にする必要があります。

「image/ALL and text/ALL video/ALL audio/ALL」

PROXYCONN：プロキシ接続ヘッダーを含むことができないユーザー エージェントのリストを管理します。リストのエントリは、Flex（Fast Lexical Analyzer）の正規表現として解釈されます。その文字列の一部がリスト内の正規表現のいずれかに一致するユーザーエージェントは、一致とされます。

- 実行する操作を選択します。

  `NEW - Add an entry to the list of user agents`

  `DELETE - Remove an entry from the list`

CUSTOMHEADERS：特定のドメインのカスタム要求ヘッダーを管理します。

- 実行する操作を選択します。

  `DELETE - Delete entries`

  `NEW - Add new entries`

  `EDIT - Edit entries`

Web 要求へのカスタム ヘッダーの追加も参照してください。

MISCELLANEOUS：その他のプロキシ関連パラメータ。

- `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)`
- `Would you like proxy to perform dynamic adjustment of TCP receive window size`
- `Would you like proxy to perform dynamic adjustment of TCP send window size`

コマンドライン インターフェイス

- Do you want to filter non-HTTP responses?

  （HTTP 以外の応答はデフォルトでフィルタされます。プロキシ経由で HTTP 以外の応答を許可する場合は、**N** と入力します。）
- Enable caching of HTTPS responses
- Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)
- Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)
- Mode of the proxy:

  1. Explicit forward mode only
  2. Transparent mode with L4 Switch or no device for redirection
  3. Transparent mode with WCCP v2 Router for redirection
- Spoofing of the client IP by the proxy:

  1. ディセーブル
  2. すべての要求に対してイネーブル
  3. 透過的要求に対してのみイネーブル
- Do you want to pass HTTP X-Forwarded-For headers?
- Do you want to enable server connection sharing?
- Would you like to permit tunneling of non-HTTP requests on HTTP ports?
- Would you like to block tunneling of non-SSL transactions on SSL Ports?
- Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?
- Do you want proxy to throttle content served from cache?
- Would you like the proxy to use client IP addresses from X-Forwarded-For headers
- Do you want to forward TCP RST sent by server to client?
- Do you want to enable WCCP proxy health check?
- Do you want to enable URL lower case conversion for velocity regex?

Web プロキシ データに対する P2 データ インターフェイスの使用と Web プロキシの設定も参照してください。

socks：SOCKS プロキシのオプション。

- Would you like to enable SOCKS proxy
- プロキシ ネゴシエーション タイムアウト（Proxy Negotiation Timeout）
- UDP トンネル タイムアウト（Tunnel Timeout）
- SOCKS コントロール ポート（SOCKS Control Ports）
- UDP リクエスト ポート（UDP Request Ports）

Web プロキシ データに対する P2 データ インターフェイスの使用 とSOCKS プロキシ サービス も参照してください。

CONTENT-ENCODING：コンテンツエンコーディング タイプを許可およびブロックします。

現在許可されているコンテンツエンコーディング タイプ：compress、deflate、gzip

現在ブロックされているコンテンツエンコーディング タイプ：該当なし

特定のコンテンツエンコーディングタイプの設定を変更するには、次のオプションを選択します。

1. compress

2. deflate

3. gzip

[1]>

The encoding type "compress" is currently allowed

Do you want to block it? [N]>

adminaccessconfig

アプライアンスにログインする管理者の認証により厳しいアクセス要件を設けるように、Web セキュリティアプライアンス を設定できます。

alertconfig

アラートの受信者を指定し、システム アラートを送信するためのパラメータを設定します。

authcache

認証キャッシュから 1 つまたはすべてのエントリ（ユーザー）を削除できるようにします。また、その時点で認証キャッシュに含まれているすべてのユーザーのリストを表示できます。

bwcontrol

デフォルトのプロキシ ログ ファイルの帯域幅制御デバッグ メッセージを有効にします。

- **bwcontrol startlog**：プロキシログへの帯域幅制御デバッグメッセージのロギングを有効にします。
- **bwcontrol startlog**：帯域幅制御デバッグメッセージのロギングを無効にします。

certconfig

SETUP：セキュリティ証明書とキーを設定します。

OCSPVALIDATION：アップロード時に証明書の OCSP 検証を有効/無効にします。

clear

前回の確定以降の保留されている設定変更をクリアします。

コミット

システム設定に対する保留中の変更を確定します。

createcomputerobject

指定された場所にコンピュータ オブジェクトを作成します。

curl

cURL 要求を、Web サーバーに直接またはプロキシ経由で送信します。要求および返される応答の HTTP ヘッダーから、Web ページをロードできなかった理由を判別できます。

（注） このコマンドは、TAC の監督のもとで管理者またはオペレータだけが使用できます。

サブコマンドは次のとおりです:

- DIRECT：直接 URL アクセス
- APPLIANCE：アプライアンス経由での URL アクセス

datasecurityconfig

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は Cisco データ セキュリティ フィルタによってスキャンされません。

date

現在の日付を表示します。例：

```
Thu Jan 10 23:13:40 2013 GMT
```

diagnostic

プロキシおよびレポート関連のサブコマンド：

NET：ネットワーク診断ユーティリティ

このコマンドは廃止されました。アプライアンスでネットワーク トラフィックをキャプチャするには、packetcapture を使用します。

PROXY：プロキシ デバッグ ユーティリティ

実行する操作を選択します。

- SNAP：プロキシのスナップショットを取得します。
- OFFLINE：プロキシをオフラインにします（WCCP 経由）。
- RESUME：プロキシのトラフィックを再開します（WCCP 経由）。
- CACHE：プロキシのキャッシュをクリアします。

REPORTING：レポート ユーティリティ

レポート システムは現在有効になっています。

実行する操作を選択します。

- DELETEDB：レポート データベースを再度初期化します。
- DISABLE：レポート システムを無効にします。
- DBSTATS：DB とエクスポート ファイルをリストします（export_files および always_onbox フォルダに含まれる未処理のファイルとフォルダのリストを表示します）。
- DELETEEXPORTDB：エクスポート ファイルを削除します（export_files および always_onbox フォルダに含まれる未処理のファイルとフォルダをすべて削除します）。
- DELETEJOURNAL：ジャーナル ファイルを削除します（aclog_journal_file をすべて削除します）。

dnsflush

アプライアンスの DNS エントリをフラッシュします。

etherconfig

イーサネット ポート接続を設定します。

Choose the operation you want to perform:

- MEDIA：イーサネット メディアの設定を表示して編集します。
- PAIRING：NIC ペアリングを表示して設定します。
- VLAN：VLAN を表示して設定します。
- MTU：MTU を表示して設定します。

externaldlpconfig

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバーでスキャンされません。

externaldlpconfig

要求の最小本文サイズを定義します。これよりも本文サイズが小さい場合、アップロード要求は外部 DLP サーバーでスキャンされません。

featurekey

有効なキーを送信して、ライセンスされた機能をアクティブ化します。

featurekeyconfig

自動的に機能キーをチェックして更新します。

fipsconfig

SETUP：FIPS 140-2 準拠とCritical Sensitive Parameter（CSP）の暗号化を有効/無効にします。即時リブートが必要となる点に注意してください。

FIPSCHECK：FIPXモードに準拠しているかどうかを確認します。各種証明書とサービスがFIPSに準拠しているかどうかを示します。

詳細については、FIPS Complianceを参照してください。

grep

指定された入力ファイルを検索して、特定のパターンに一致するものを含む行を見つけます。

gathererdconfig

アプライアンスと認証サーバーの間にポーリング機能を設定します。

help

コマンドのリストを返します。

httppatchconfig

発信 HTTP パッチ要求を有効または無効にします。デフォルトでは、無効に設定されています。

iccm_message

このWebセキュリティアプライアンスがセキュリティ管理アプライアンス（M-Series）によって管理される時期を示すメッセージを、Web インターフェイスと CLI からクリアします。

ifconfig または interfaceconfig

M1、P1、P2などのネットワーク インターフェイスを設定して管理します。現在設定されているインターフェイスを表示し、インターフェイスの作成、編集、削除のための操作メニューを提供します。

iseconfig

現在の ISE 設定パラメータを表示します。実行する ISE 設定操作を指定できます。

`setup`：ISE の設定項目を設定します（有効化/無効化、ISE サーバー名または IPv4 アドレス、プロキシキャッシュのタイムアウト、統計情報のバックアップ間隔）。

isedata

ISE データ関連の操作を指定します。

`statistics`：ISE サーバーのステータスと ISE 統計情報を表示します。

`cache`：ISE キャッシュを表示するか、IP アドレスを確認します。

`sgts`：ISE セキュア グループ タグ（SGT）テーブルを表示します。

`groups`：ISE グループ テーブルを表示します。

VDI が実装されている場合、メインコマンド `cache` の下のサブコマンド `show` および `checkip` に詳細が表示されます。`show` サブコマンドはポート範囲に関する詳細を表示し、`checkip` サブコマンドは IP アドレス、名前、ポート範囲などの VDI ユーザーに関する詳細を表示します。

```
[]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
```

last

tty やホストなどのユーザー固有のユーザー情報を新しい順に並べて一覧表示したり、指定した日時にログインしたユーザーのリストを表示します。

loadconfig

システム コンフィギュレーション ファイルをロードします。

logconfig

ログ ファイルへのアクセスを設定します。

mailconfig

指定されたアドレスに現在のコンフィギュレーション ファイルをメールで送信します。

maxhttpheadersize

プロキシ要求の最大 HTTP ヘッダー サイズまたは URL サイズを設定します。値をバイト単位で入力するか、キロバイトを表す場合は数値に K を付記します。

多数の認証グループに属するユーザーの場合はポリシー トレースが失敗する可能性があります。また、HTTP 応答ヘッダーのサイズまたは URL サイズが現在の「最大ヘッダー サイズ」よりも大きい場合、失敗することがあります。この値を大きくすると、このような障害を軽減できます。最小値は 32 KB、デフォルト値は 32 KB、最大値は 1024 KB です。

modifyauthhelpers

このコマンドを使用して、BASIC、NTLMSSP、および NEGO の Kerberos 認証ヘルパーを 5 ～ 21 の範囲内の数値で設定します。

musconfig

このコマンドを使用してセキュア モビリティを有効化し、リモート ユーザーの識別方法を設定します（IP アドレスによって識別するか、1 つ以上の Cisco 適応型セキュリティ アプライアンスと統合することで識別）。

（注） このコマンドを使って変更すると、Web プロキシが再起動されます。

musstatus

Web セキュリティアプライアンス を適応型セキュリティアプライアンスと統合したときに、このコマンドを使用してセキュアモビリティに関連する情報を表示します。

このコマンドにより、以下の情報が表示されます。

- Web セキュリティアプライアンス と個々の適応型セキュリティ アプライアンスとの接続状態。
- Web セキュリティアプライアンス と個々の適応型セキュリティ アプライアンスとの接続時間（分単位）。
- 個々の適応型セキュリティ アプライアンスからのリモート クライアントの数。
- サービス対象のリモート クライアントの数。これは、Web セキュリティアプライアンスを介してトラフィックの受け渡しを行ったリモート クライアントの数です。
- リモート クライアントの合計数。

networktuning

Web セキュリティアプライアンス は、複数のバッファおよび最適化アルゴリズムを使用して何百もの TCP 接続を同時に処理し、一般的な Web トラフィック（つまり、一時的な HTTP 接続）に対して高いパフォーマンスを実現します。

大容量ファイル（100 MB 以上）が頻繁にダウンロードされるような特定の状況では、バッファが大きいほど接続ごとのパフォーマンスが向上する可能性があります。ただし、全体的なメモリ使用量が増加するため、システムで使用可能なメモリに応じてバッファを増やす必要があります。

送信および受信スペース変数は、指定の TCP ソケットを介した通信用にデータを保存するために使用されるバッファを表します。自動送信および受信変数は、ウィンドウ サイズを動的に制御するための FreeBSD 自動調整アルゴリズムを有効または無効にするために使用されます。これら 2 つのパラメータは、FreeBSD カーネルに直接適用されます。

SEND_AUTO と RECV_AUTO が有効な場合、システムの負荷と使用可能なリソースに基づいてウィンドウ サイズが動的に調整されます。負荷が小さい Web セキュリティアプライアンス では、トランザクションあたりの遅延を削減するためウィンドウサイズが大きく維持されます。動的に調整されるウィンドウ サイズの最大値は、設定されている mbuf クラスタの数に依存します。つまり、システムで使用可能な RAM の合計に応じて異なります。クライアント接続の合計数が増加する場合、または使用可能なネットワーク バッファ リソースが非常に少なくなる場合には、すべてのネットワーク バッファ リソースがプロキシ トラフィックにより使用されることを防いでシステムを保護するため、ウィンドウ サイズが削減されます。

このコマンドの使用に関する詳細については、アップロード/ダウンロード速度の問題を参照してください。

`networktuning` サブコマンドは、次のとおりです。

SENDSPACE：TCP 送信スペースのバッファ サイズ。8192 ～ 131072 バイトの範囲で、デフォルトは 16000 バイトです。

RECVSPACE：TCP 受信スペースのバッファ サイズ。8192 ～ 131072 バイトの範囲で、デフォルトは 32768 バイトです。

SEND-AUTO：TCP 送信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオフです。TCP 送信の自動調整を有効にする場合、必ず `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size?` の順に使用して、送信バッファの自動調整を無効にしてください。

RECV-AUTO：TCP 受信の自動調整を有効または無効にします。1 はオン、0 はオフで、デフォルトはオフです。TCP 受信の自動調整を有効にする場合、必ず `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size?` の順に使用して、受信バッファの自動調整を無効にしてください。

MBUF CLUSTER COUNT：使用可能な mbuf クラスタの数を変更します。許容範囲は 98304 ～ 1572864 です。この値は、インストールされたシステム メモリによって変わります。98304 *（X/Y）の計算を使用し、X はシステム上の RAM のギガバイトで、Y は 4 GB です。たとえば 4 GB RAM の場合、推奨値は 98304 *（4/4）＝98304 になります。RAM が増加する場合は、線形スケーリングが推奨されます。

SENDBUF-MAX：最大送信バッファ サイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 1 MB（1048576 バイト）です。

RECVBUF-MAX：最大受信バッファ サイズを指定します。範囲は 131072 ～ 2097152 バイトで、デフォルトは 1 MB（1048576 バイト）です。

CLEAN-FIB-1：データルーティング テーブルからすべての M1/M2 エントリを削除します。基本的には、コントロールプレーン/データプレーンの分離を有効にします。つまり、「分離ルーティング」が有効になっている場合に M1 インターフェイス経由のデータ送信からデータプレーン プロセスを無効にします。データプレーン プロセスは、「データ ルーティング テーブルの使用」が有効になっているプロセス、または非管理トラフィックを厳密に伝達するプロセスです。コントロールプレーン プロセスでは、依然として M1 または P1 インターフェイスのいずれかを介してデータを送信できます。

これらのパラメータに何らかの変更を行った後は、必ず変更を確定してアプライアンスを再起動してください。

⚠

注意 副次的な影響を理解している場合にのみ、このコマンドを使用してください。TAC ガイダンスを受けている場合にのみ使用することを推奨します。

nslookup

指定されたホストとドメインの情報を取得したり、ドメイン内のホストのリストを印刷するために、インターネット ドメイン ネーム サーバーに照会します。

ntpconfig

NTP サーバーの設定現在設定されているインターフェイスを表示し、インターフェイスを追加、削除、または設定する操作メニューを提供します。このインターフェイスの IP アドレスから NTP クエリーが発信されます。

packetcapture

アプライアンスが接続されているネットワーク上で送受信されている TCP/IP などのパケットを代行受信して表示します。

passwd

パスフレーズを設定します。

pathmtudiscovery

パス MTU ディスカバリをイネーブルまたはディセーブルにします。

パケット フラグメンテーションが必要な場合は、パス MTU ディスカバリをディセーブルにすることができます。

ping

指定されたホストまたはゲートウェイに ICMP エコー要求を送信します。

proxyconfig <enable | disable>

Web プロキシをイネーブルまたはディセーブルにします。

proxystat

Web プロキシの統計情報を表示します。

quit、q、exit

アクティブなプロセスまたはセッションを終了します。

reboot

ファイル システム キャッシュをディスクにフラッシュし、実行中のすべてのプロセスを停止して、システムを再起動します。

reportingconfig

レポーティング システムを設定します。

resetconfig

出荷時の初期状態に設定を復元します。

revert

Web オペレーティング システム用の AsyncOS を以前の認定済みビルドに復元します。これは非常に危険な操作で、すべての設定ログおよびデータベースを破棄します。このコマンドの使用については、以前のバージョンの AsyncOS for Web への復元を参照してください。

rollbackconfig

直前に確定した 10 の設定のうち 1 つをロールバックできます。デフォルトでは、ロールバック設定機能が有効になっています。

rollovernow

ログ ファイルをロール オーバーします。

routeconfig

トラフィックの宛先 IP アドレスとゲートウェイを設定します。現在設定されているルートを表示し、エントリを作成、編集、削除、クリアするための操作メニューを提供します。

saveconfig

現在の設定のコピーをファイルに保存します。必要に応じて、このファイルを使用してデフォルトを復元できます。

FIPS モードが有効な場合は、パスフレーズ処理オプション `Mask passphrases` または `Encrypt passphrases` を指定します。

setgateway

マシンのデフォルト ゲートウェイを設定します。

sethostname

hostname パラメータを設定します。

setntlmsecuritymode

NTLM 認証レルムのセキュリティ設定を、「ads」または「domain」に変更します。

- `domain`：AsyncOS は Active Directory ドメインにドメイン セキュリティ信頼アカウントを結合します。AsyncOS では、Active Directory はこのモードでネストされた Active Directory グループだけを使用する必要があります。
- `ads`：AsyncOS は、Active Directory のネイティブ メンバーとしてドメインを結合します。

デフォルト設定は `ads` です。

settime

システム時刻を設定します。

settz

現在のタイム ゾーンとタイム ゾーンのバージョンを表示します。ローカル タイム ゾーンを設定する操作メニューを提供します。

showconfig

すべての設定値を表示します。

（注） ユーザーのパスフレーズは暗号化されます。

shutdown

接続を終了してシステムをシャット ダウンします。

smtprelay

内部的に生成された電子メールの SMTP リレー ホストを設定します。SMTP リレー ホストは、システムで生成された電子メールやアラートを受け取るために必要です。

smtpconfig

SNMP クエリーをリッスンして SNMP 要求を受け入れるように、ローカル ホストを設定します。

sshconfig

信頼できるサーバーのホスト名とホスト キー オプションを設定します。

sslconfig

AsyncOS バージョン 9.0 以前のデフォルトの暗号は、`DEFAULT:+kEDH` です。

AsyncOS バージョン 9.1 ～ 11.8 のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

この場合、デフォルトの暗号は ECDHE 暗号の選択によって変わる場合があります。

AsyncOS バージョン 12.0 以降のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

（注） 新しい AsyncOS バージョンにアップグレードする際に、デフォルトの暗号スイートを更新します。暗号スイートは自動的に更新されません。以前のバージョンから AsyncOS 12.0 以降にアップグレードする場合は、暗号スイートを次のように更新することを推奨します。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

FALLBACK：SSL/TLS のフォールバック オプションを有効または無効にします。イネーブルの場合、リモート サーバーとの通信は、ハンドシェイクの失敗後、最も低く設定されているプロトコルにフォールバックします。

プロトコル バージョンがクライアントとサーバーの間でネゴシエートされると、実装の問題が原因でハンドシェイクが失敗する可能性があります。このオプションがイネーブルの場合、プロキシは現在設定されている TLS/SSL プロトコルの最も低いバージョンを使用して接続を試みます。

（注） AsyncOS 9.x の新規インストール時、フォールバックはデフォルトでディセーブルに設定されています。フォールバック オプションがある以前のバージョンからアップグレードする場合、現在の設定が保持されます。そうでない場合、つまりこのオプションがないバージョンからアップグレードする場合、フォールバックはデフォルトでイネーブルに設定されています。

ECDHE：LDAP での ECDHE 暗号の使用を有効または無効にします。

その後のリリースで追加の ECDH 暗号がサポートされていますが、追加の暗号とともに提供された特定の名前付き曲線が原因で、セキュア LDAP 認証と HTTPS トラフィック復号化の際中に、アプライアンスが接続をクローズする場合があります。追加の暗号の指定については、SSL の設定 を参照してください。

これらの問題がある場合は、このオプションを使用して、一方または両方の機能で ECDHE 暗号の使用をディセーブルにするか、またはイネーブルにします。

ssltool

アプライアンスの CLI から別の OPENSSL コマンドを実行し、SSL 接続のトラブルシューティングを行います。`ssltool` コマンドには、次のサブコマンドが用意されています。

- **sclient**：これは openssl s_client コマンドの CLI バージョンです。アプライアンスを使用せずに直接 SSL/TLS を使用してリモート ホストに接続します。
  - `COMMAND`：openssl s_client コマンドを実行します。次の openssl s_client コマンドがサポートされます。

```
-connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
 -showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
```

コマンドライン インターフェイス

```
-no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
-save, -noout
```

サポートされる openssl s_client コマンドの詳細については、インライン ヘルプを参照してください。

（注） command の実行後、-save オプションを使用して出力をファイルに保存できます。保存されたログ ファイルにアクセスすることはできません。これらのログ ファイルは、シスコ サポート チームによってデバッグに使用されます。

- HELP：ヘルプ情報を提供します。

- **CLEARLOGS**：ssltool によって生成されたすべてのログを削除します。

status

システム ステータスを表示します。

supportrequest

サポート要求の電子メールを Cisco カスタマー サポートに送信します。これには、システム情報およびプライマリ設定のコピーが含まれます。

（オプション）サービス要求番号を指定すると、システム情報と設定情報の大きなセットがサービス要求に自動的に追加されます。この情報は ZIP で圧縮され、FTP を使用してサービス要求にアップロードされます。

tail

ログ ファイルの末尾を表示します。コマンドは、ログ ファイル名をパラメータとして受け入れます。

例 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
…
…
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
“CTRL-C” + “q”
```

例 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
"CTRL-C" + "q"
```

tcpservices

開かれている TCP/IP サービスに関する情報を表示します。

techsupport

Cisco カスタマー サポートがシステムにアクセスしてトラブルシューティングを支援できるように、一時的な接続を提供します。

telnet

TELNET プロトコルを使用して別のホストと通信します。通常、接続の確認に使用されます。

testauthconfig

特定の認証レルムで定義された認証サーバーに対して、そのレルムの認証設定をテストします。

testauthconfig [-d level] [realm name]

オプションを指定せずにコマンドを実行すると、設定されている認証レルムのリストが表示されるので、そのリストから選択できます。

デバッグ フラグ（- d）によってデバッグ情報のレベルが制御されます。指定できるレベルの範囲は 0～10 です。指定しない場合は、レベル 0 が使用されます。レベル 0 の場合は、コマンドによって成功または失敗が返されます。テスト設定が失敗すると、失敗の原因が一覧表示されます。

（注） レベル 0 を使用することを推奨します。トラブルシューティングのためにさらに詳細な情報が必要な場合にのみ、別のデバッグ レベルを使用してください。

tuiconfig tuistatus

これらの 2 つのコマンドについては、CLI を使用した透過的ユーザー識別の詳細設定 で説明しています。

traceroute

ゲートウェイを通過し、宛先ホストまでのパスをたどって、IP パケットをトレースします。

trailblazerconfig

`trailblazerconfig` コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。

（注） デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。`help trailblazerconfig` コマンドを入力すると、インライン ヘルプを参照できます。

構文は次のようになります。

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

ここで、

`'enable'` は、デフォルトのポート（HTTPS: 4431 または HTTP: 801）で trailblazer を実行します。

`'disable'` は trailblazer を終了します

`'status'` は trailblazer のステータスをチェックします。

（注） アプライアンスで `trailblazerconfig` コマンドを有効にしている場合、リクエスト URL にはホスト名に付加された HTTP/HTTPS ポート番号が含まれます。

ブラウザの操作をシームレスにするために、以下のいずれかのステップを試行できます。

- Web インターフェイスで使用される証明書を承認し、新しいブラウザウィンドウで `https://hostname:<https_api_port>`（例：`https://some.example.com:6443`）の URL 構文を使用して証明書を承認します。ここで、`<https_api_port>` は [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] で設定されている AsyncOS API HTTPS ポートです。また、API ポート（HTTP/HTTPS）がファイアウォールで開かれていることを確認します。
- デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。HTTP または HTTPS ポートがファイアウォールで開かれていることを確認します。また、アプライアンスにアクセスするために指定したホスト名を DNS サーバーが解決できることを確認します。

  `trailblazerconfig` の CLI コマンドが無効になっている場合、CLI を使用して **trailblazerconfig** > **enable** コマンドを実行することにより、以下の問題を回避できます。

  - 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
  - スパム隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。

- Advanced Malware Protection レポートページのメトリックバーにデータが含まれない。

updateconfig

アップデートおよびアップグレードを設定します。

updatenow

すべてのコンポーネントを更新します。

upgrade

AsyncOS ソフトウェア アップグレードをインストールします。

`downloadinstall`：アップグレードパッケージをダウンロードし、即時にインストールします。

`download`：アップグレードパッケージをダウンロードし、後でインストールできるように保存します。

いずれかのコマンドを入力すると、この Web セキュリティアプライアンス に適用可能なアップグレードパッケージのリストが表示されます。使用するパッケージのエントリ番号を入力してそのパッケージを選択し、Enter キーを押します。ダウンロードがバックグラウンドで開始されます。ダウンロード中に、サブコマンド `downloadstatus` と `canceldownload` を使用できます。

最初に `downloadinstall` を入力した場合、ダウンロードが完了するとインストールが即時に開始されます。`download` を入力した場合は、ダウンロード完了時に 2 つのコマンド（`install` と `delete`）が使用可能になります。`install` と入力すると、以前にダウンロードしたパッケージのインストールが開始します。`delete` と入力すると、以前にダウンロードしたパッケージが Web セキュリティアプライアンス から削除されます。

userconfig

システム管理者を設定します。

version

一般的なシステム情報、インストールされているシステム ソフトウェアのバージョン、およびルールの定義を表示します。

wccpstat

`all`：すべての WCCP（Web Cache Communication Protocol）サービス グループの詳細を表示します。

`servicegroup`：特定の WCCP サービス グループの詳細を表示します。

webcache

プロキシキャッシュの内容を確認または変更したり、アプライアンスにキャッシュされないドメインとURLを設定します。管理者は特定のURLをプロキシキャッシュから削除したり、プロキシ キャッシュに保存しないドメインやURLを指定できます。

who

CLIおよびWebインターフェイス セッションの両方について、システムにログインしているユーザーを表示します。

（注） 各ユーザーは、最大10の同時セッションを持つことができます。

whoami

ユーザー情報を表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。