インストールおよびセットアップ

この章は、次のセクションで構成されています。

はじめに

Cisco Advanced Web Security Reporting アプリケーションに用意されているフィルタとダッシュボードは、複数の Web セキュリティアプライアンス、および Cisco Umbrella から送られる大量のデータを分析できるように設計されています。Cisco Advanced Web Security Reporting アプリケーションには、データ収集と表示アプリケーション、および Web セキュリティアプライアンス（WSA）と Umbrella ホストから収集したログデータを転送する関連サーバが含まれます。

Cisco Advanced Web Security Reporting アプリケーションはログデータを受信すると、データモジュールに保存します。これらのデータは、定義した検索または「フィルタ」を使用して表示できます。

最新情報

リリース 7.5.1 の新機能

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 7.3.5 にアップグレードされています。
Syslog パーサーの更新	Cisco Web セキュリティアプライアンス 12.0.1-334 の Syslog パーサーの更新。

リリース 7.5 の新機能

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 7.3.3 にアップグレードされています。
[ユーザのドリルダウン（Use Drilldown）] ページには、AD グループの詳細のレポートが表示されます。	**[ユーザ分析（User Analysis）]** > **[ユーザのドリルダウン（Use Drilldown）]**ページに、AD グループ名で検索するための新しいフィルタが追加されています。AD グループの詳細が検索結果に表示されます。[ADグループ（AD Group）]、[ユーザID（User ID）]、[宛先ドメイン（Destination Domain）]、[使用済み帯域幅（Bandwidth used）]、および[滞留時間（Time Spent）]の詳細が表示されます。

リリース 7.0 の新機能

機能	説明
AWSR プロキシサービスの検索結果に WBRS スコアのないイベントが表示される	WBRS スコアなしの新しいフィルタ（[WBRSの表示: スコアなし（Show WBRS: No Score）]）が**[Webトラッキング（Web Tracking）] > [プロキシサービス（Proxy Services）]**ダッシュボードに追加されました。このフィルタを使用すると、WBRS スコアのない AWSR プロキシサービスの検索結果を表示できます。
部門メンバーシップレポートに AD グループレポートの詳細な結果が表示される	AD グループレポートの次の結果を**[ユーザ分析（User Analysis）] > [概要（Overview）]**に表示できるようになりました。 • [ブロックされたトランザクション数の上位グループ（Top Groups by Transactions Blocked）] • [ブロックされたトランザクションのサマリー（Transactions Blocked Summary）] • [帯域幅使用量の上位グループ（Top Groups by Bandwidth Used）] • [使用帯域幅のサマリー（Bandwidth Used Summary）] • [ユーザ別の上位グループ（Top Groups by User）] • [使用帯域幅のサマリー（Bandwidth Used Summary）] • [ADグループサマリー（AD Group Summary）] • [ユーザごとのADグループの詳細（AD Group per User Details）]

リリース 6.6 の最新情報

機能	説明
カスタム ダッシュボードでの検索	カスタム ダッシュボードでの検索がサポートされています。 • [送信（Submit）] ボタンのある [メイン検索（Main Search）] フィールドを使用してデータを検索できます。 • 結果のペインで、セカンダリ [検索（search）] フィールドを使用して検索結果をフィルタリングできます。
任意のページからのエクスポート	データ（グラフィカルデータ以外）は、カンマ区切り値（csv）ファイル、XML ファイル、または JavaScript Object Notation（json）ファイルとして、任意のダッシュボードからエクスポートできます。ダウンロードするためにこのオプション  を表示するには、ダッシュボードデータの表示ペインの上にマウスカーソルを置く必要があります。

リリース 6.4 の最新情報

機能	説明
ダッシュボードの更新の Web トラッキング	• 新規フィルタ：**ユーザ、クライアント IP、WBRS** の最小および最大スコア範囲、および **SNI** が、**[Web トラッキング（Web Tracking）] > [プロキシ サービス（Proxy Services）]**ダッシュボードに追加されます。 • プロキシサービス ダッシュボードから、10,000 個のトランザクションを表示し、エクスポートすることができます。

リリース 6.3 の最新情報

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 6.6.6 にアップグレードされています。

リリース 6.2 の最新情報

機能	説明
Cisco Umbrella レポートのサポート	Cisco Advanced Web Security Reporting アプリケーションから Umbrella によって提供されるログを含むプライベート AWS S3 バケットをポイントできます。統合 Web セキュリティ レポート ダッシュボードで、レポートを表示できます。
Splunk エンジンのアップグレード	Splunk エンジンが最新バージョンにアップグレードされています。

（注） ロールベースのレポート機能は、高速化されないデータ モデルに対してのみ機能します。高速化を無効にするとレポートの読み込み時間が長くなるため、ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にしてください。「設定のベスト プラクティス」および「職務別の部門レポートへのアクセスの制限」を参照してください。

リリース 6.1 の最新情報

機能	説明
CEF エクストラクタ	共通イベント フォーマット（CEF）エクストラクタ サービスによって、1 つまたは複数の WSA から受信したアクセス ログを CEF 形式の出力データに変換できます。
Web セキュリティ アプライアンス AsyncOS 10.1 のサポート	Web セキュリティ アプライアンスのリリースの AsyncOS 10.1 に含まれている、アーカイブ スキャン アクセス ログの変更をサポートします。

リリース 6.0 の最新情報

機能	説明
カスタム フィルタ	「フィルタリング」と呼ばれるプロセスで、利用可能なアクセス ログ、SOCKS ログ、AMP ログのデータのカスタム検索を定義します。
Web セキュリティ アプライアンス AsyncOS 10.0 の変更	AMP の機能拡張と参照元のヘッダー関連のサポート。

サポートされる機能と、サポートされない機能

コンポーネント	サポート対象	サポート対象外
サーバ	単一サーバ展開	複数サーバ展開
送信方法	FTP（ファイルおよびディレクトリ） TCP（Syslog）	
PDF	統合 PDF 生成 スケジュール済 PDF レポート	
カスタム ダッシュボード	定義済みのレポートの場合は、それぞれに [ダッシュボードとして保存（Save As Dashboard）] を使用し、時間範囲、ソースタイプ、およびホスト（制限あり）を選択してカスタムダッシュボードを作成します。カスタムフィルタの場合は、それぞれに[ダッシュボードとして保存（Save As Dashboard）] を使用し、アクセスログ、SOCKS ログ、または AMP ログのフィルタフィールドを選択してカスタムダッシュボードを作成します。	

システム要件およびサイズ変更とスケーリングの推奨事項

システム要件およびサイズ変更とスケーリングの推奨事項については、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html から入手できる『*Cisco Advanced Web Security Reporting Release Notes*』で詳しく説明されています。

AWSR で使用される次のポートは開いている必要があります。これらのポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。

- 8887/TCP：Python ベースのアプリケーションサーバがリッスンするポート番号。このポートは、アプリケーション サーバ ポートと呼ばれます。
- 8888/TCP：Cisco Advanced Web Security Reporting の GUI にアクセスするためのポート。このポートは、Web ポートとも呼ばれます。

- 8889/TCP：Cisco Advanced Web Security Reporting がデーモンプロセスとの通信に使用するポート。このポートは管理ポートと呼ばれます。
- 8886/TCP - mongodb：デーモンが KV ストアサーバへの接続に使用するポート。
- 22/TCP：SSH/SCP/WGET
- 514/TCP：Syslog
- 21/TCP：FTP

（注） nmap/netstat/iptables を有効にして、システム構成と Windows の RDP を制御および検証することもできます。

セットアップの概要

- Cisco Advanced Web Security Reporting を初めてインストールします。
  - Cisco Advanced Web security Reporting 7.5.1 のインストール
  - ライセンスおよび移行
  - アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成
  - 履歴データのインポートおよびインデックス作成
  - 継続的なデータ転送の設定（Web セキュリティアプライアンスのセットアップを含む）
  - Umbrella のログの更新
- Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード

Cisco Advanced Web security Reporting 7.5.1 のインストール

（注） インストールまたはアップグレードする前に、ブラウザの Cookie とキャッシュをクリアしてください。

（注） AWSR 7.5.1 の場合、ログイン情報はインストール中に作成されます。インストール中に作成されたログイン情報には、「管理者」のロール、および機能/特権があります。

Cisco Advanced Web Security Reporting アプリケーションをインストールするには、この項の手順を実行します。

- Linux の場合
- Windows の場合

Linux の場合

次のタスクを順序どおりに実行してください。

ステップ 1 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 2 以下のコマンドを使用して、/opt にあるインストーラソフトウェアを抽出します。

tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.tgz -C /opt

ステップ 3 ディレクトリを `/cisco_wsa_reporting/` に変更してセットアップスクリプトを実行します。

```
cd /opt/cisco_wsa_reporting./setup.sh
```

- このコマンドの結果が次の場合には、以下の操作を行います。

```
./setup.sh: Permission denied
```

1. 次のコマンドを使用して、スクリプト `setup.sh` の権限レベルを変更します。

   ```
   chmod 777 setup.sh
   ```
2. スクリプトを再実行します。

セットアップ時に、進行状況およびマイルストーン ステートメントが表示されます。

ステップ 4 管理者のユーザ名とパスワードを作成し、パスワードを確認します。

```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/rtestuser/AWSR7.5/cisco_wsa_reporting/etc/openlda
```

ステップ 5 前の手順で作成したユーザ名とパスワードを入力してログインします。

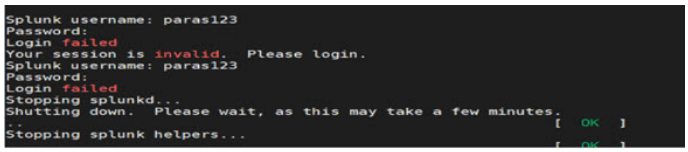
```
The Splunk web interface is at http://wsa061-client05.cs1:8888

Splunk username: admin
Password:
The licenses object has been added
```

ステップ 6 Cisco Advanced Web Security Reporting を起動し、インストール中に作成されたクレデンシャルを使用してログインします。

1. ブラウザウィンドウで `https://<hostname>:8888` にアクセスします。

（注） 以前のバージョンではポート 8000 が使用されていましたが、バージョン 4.0 以降で使用するポートは 8888 です。

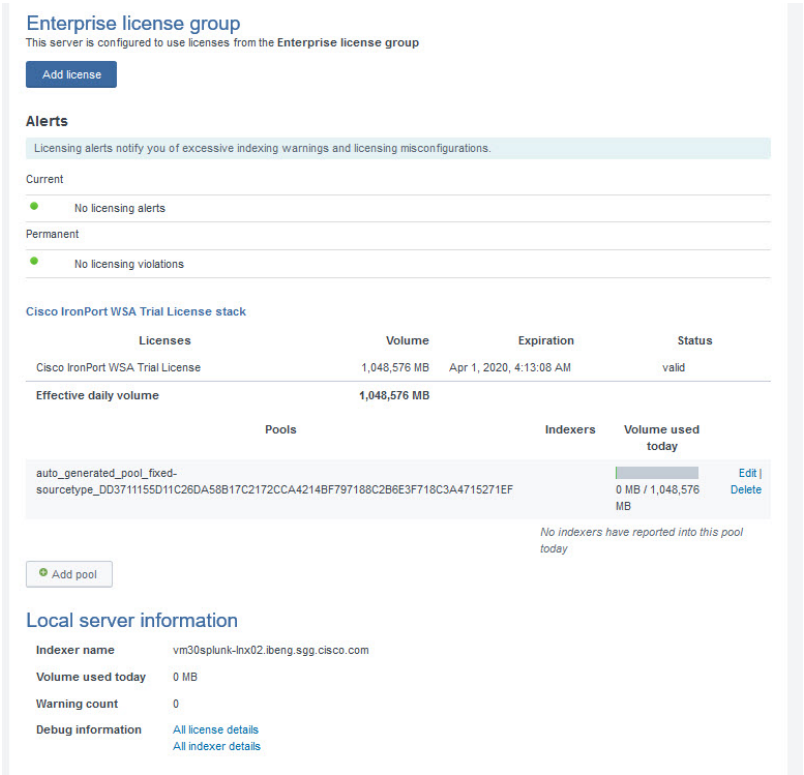
（注） Splunk へのログイン時にユーザ名とパスワードを誤って 2 回指定すると、**setup.sh** コマンドの実行中にライセンスは追加されません。



ライセンスファイルを手動で追加するには、次の手順に従います。

<INSTALL_HOME> ディレクトリ、たとえば /opt/cisco_wsa_reporting から次を実行します。

- ファイル「**Splunk-eval-120d-500GB.License**」の内容をコピーし、管理者として AWSR GUI にログインします。
- **[設定（Settings）] > [システム（SYSTEM）] > [ライセンス（Licensing）] > [ライセンスの追加（Add license）]**に移動して、**[ライセンスXMLディレクトリをコピーして直接貼り付ける（Copy & paste the license XML directly）]** をクリックし、**「Splunk-eval-120d-500GB.License」の内容の貼り付け > [インストール（Install）]**を実行して、再起動します。



- インストール後のタスク

- ライセンスおよび移行

Windows の場合

始める前に

Windows では、Advanced Web Security Reporting のインストールバージョンを 1 つだけ使用できます。以前のバージョンがインストールされている場合は、既存のデータをバックアップして以前のバージョンをアンインストールしてから、新しいバージョンをインストールする必要があります。

ステップ 1 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 2 インストーラを解凍します。7-Zip や WinZip などのアプリケーションを使用できます。

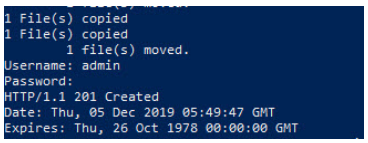
（注） デジタル署名に関連するファイルは、パッケージが抽出されたディレクトリにあります。たとえば、次のようになります。

```
C:\Users\<UserDirectory>\Downloads\CiscoAdvancedWebSecurityReporting-Windows_7-5-1-0-114.tgz
```

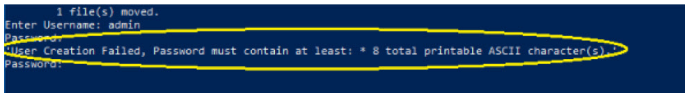
ステップ 3 コマンドライン シェル（PowerShell）を管理者として起動し、ディレクトリをインストーラの解凍先ディレクトリに変更します。

ステップ 4 インストールコマンド `./install.bat` を実行します。

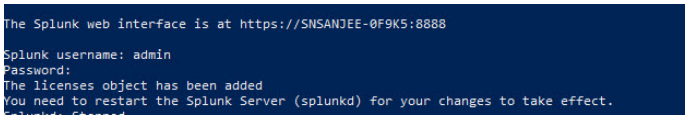
ステップ 5 管理者のユーザ名とパスワードを作成し、パスワードを確認します。



（注） パスワードの長さが無効な場合、「パスワードには少なくとも8文字の出力可能なASCII文字が含まれている必要があります（Password must contain at least 8 total printable ASCII character）」というエラーメッセージが表示される場合があります。ユーザを正常に作成するには、パスワードに少なくとも 8 文字の ASCII 文字を含めてください。



ステップ 6 前の手順で作成したユーザ名とパスワードを入力してログインします。



アプリケーションが `C:\Program Files\Cisco\CiscoWSAReporting` フォルダにインストールされます。

ステップ 7 Cisco Advanced Web Security Reporting サーバを再起動します。

ステップ 8 次の手順で Cisco Advanced Web Security Reporting アプリケーションを起動し、ログインします。

1. ブラウザウィンドウで `https://<hostname>:8888` にアクセスします。
2. インストール中に作成したユーザ名とパスワードでログインします。

（注） 以前のバージョンではポート 8000 が使用されていましたが、バージョン 4.0 以降で使用するポートは 8888 です。

次のタスク

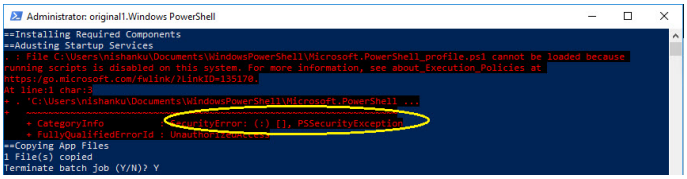
- インストール後のタスク
- ライセンスおよび移行

インストール中のエラーの処理

インストール中に次のエラーが表示される場合があります。このセクションでは、インストール中に発生する可能性のある一般的なエラーと、これらのエラーを解決するために実行する必要のある手順について説明します。

セキュリティエラー: PSSecurityException

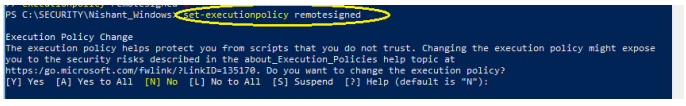
新しいアプライアンスに Cisco Advanced Web Security Reporting をインストールすると、PSSecurityException エラーが発生する場合があります。



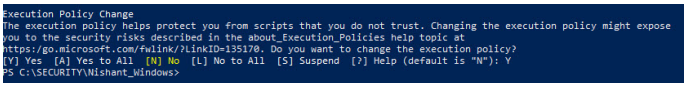
この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
set-executionpolicy remotesigned
```

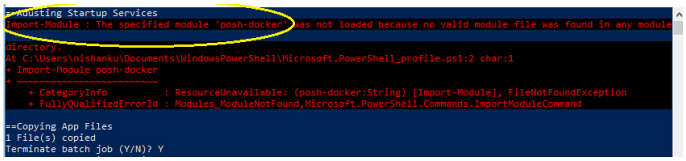


ステップ 2 表示されるプロンプトに対して [Y]（はい）を選択します。



ステップ 3 インストールコマンド `/install.bat` を再実行します。

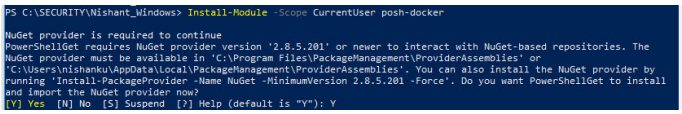
モジュールのインポートエラー：posh-docker



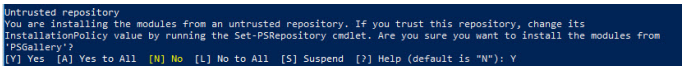
この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
Install-Module -Scope CurrentUser posh-docker
```

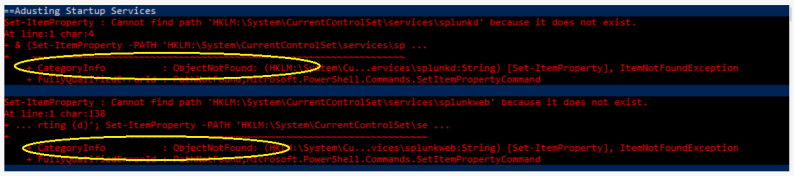


ステップ 2 表示されるプロンプトに対して **[Y]**（はい）を選択します。



ステップ 3 インストールコマンド `/install.bat` を再実行します。

ObjectNotFound：パスが見つからない



この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
New-Item -Path HKLM:\System\CurrentControlSet\services\splunkd -Force | Out-Null

New-Item -Path HKLM:\System\CurrentControlSet\services\splunkweb -Force | Out-Null
```

ステップ 2 インストールコマンド `/install.bat` を再実行します。

Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード

Linux の場合

次のタスクを順番どおりに実行してください。

ステップ 1 インストールされている Cisco Advanced Web Security Reporting の以前のバージョンのディレクトリに移動します。

ステップ 2 `chmod 777 ./shutdown` コマンドを使用して前のセッションをシャットダウンします。

ステップ 3 `https://<hostname>:8888` に移動して、AWSR が引き続きブラウザで実行されているかどうかを確認します。

ステップ 4 `/opt /` ディレクトリにあるバージョンの Cisco Advanced Web Security Reporting の新しいインストーラを次の場所からダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 5 ダウンロードしたインストーラ ファイルを cisco_wsa_reporting ディレクトリのベース ディレクトリにコピーします。

たとえば、 Cisco Advanced Web Security Reporting の以前のバージョンが `/opt/cisco_wsa_reporting/` にインストールされている場合は、ファイルを `/opt/` ディレクトリに置きます。

ステップ 6 ディレクトリをインストールのベース ディレクトリ（`/opt/` など）に変更します。

ステップ 7 次のコマンドを使用してインストーラを解凍します。適切なバージョン番号を使用します。

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.tgz
cisco_wsa_reporting/SeamlessUpgrade.sh; cp -f cisco_wsa_reporting/SeamlessUpgrade.sh./
```

ステップ 8 アップグレード スクリプトを実行します。適切なバージョン番号を使用します。

```
./SeamlessUpgrade.shCiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.tgz
```

- このコマンドの結果が次の場合には、以下の操作を行います。

  ```
  ./SeamlessUpgrade.sh: Permission denied
  ```

  1. 次のコマンドを実行して、スクリプト SeamlessUpgrade.sh の権限レベルを変更します。

     ```
     chmod 777 cisco_wsa_reporting/SeamlessUpgrade.sh
     ```

  2. スクリプトを再実行します。

ステップ 9 ブラウザで `https://<wsa_reporting_server_host_name>:8888` を開き、ユーザ名とパスワードを使用してログインします。

Windows の場合

次のタスクを順番どおりに実行してください。

ステップ 1 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 2 インストーラを解凍します。7-Zip や WinZip などのアプリケーションを使用できます。

ステップ 3 コマンドライン シェル（PowerShell）を管理者として起動し、ディレクトリをインストーラの解凍先ディレクトリに変更します。

ステップ 4 コマンド `.\WinSeamlessUpgrade.ps1` を使用して、Cisco Advanced Web Security Reporting をアップグレードします。

ステップ 5 ブラウザで `https://<wsa_reporting_server_host_name>:8888` を開き、ユーザ名とパスワードを使用してログインします。

ユーザ（Users）

Cisco Advanced Web Security Reporting アプリケーションは、2 人の管理者ユーザを提供します。さらにユーザを作成し、既存のロールを割り当てるか、新しいロールを作成することができます。「職務別の部門レポートへのアクセスの制限」を参照してください。

管理ユーザ（Administrative Users）

Cisco Advanced Web Security Reporting アプリケーションには、次の 2 つの管理ユーザが用意されています。

- 「デフォルトの管理者」（ユーザ名：`admin`、パスワード：`Cisco@dmin`）はすべての管理機能にアクセスできます。

  `admin` ユーザはライセンスをインストールして分散環境を設定できます。設定、テスト、トラブルシューティングを行うためにこのアカウントを使用します。

- 2 人目の管理ユーザ（名前：`wsa_admin`、パスワード：`Ironp0rt`）には管理機能のサブセットへのアクセス権があります。

インストール後すぐに両方のパスワードを変更することを推奨します（**[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access Controls）] > [ユーザ（Users）]**）。

新規ユーザーの作成

管理ユーザとは別に、新しいユーザを作成することもできます。

ステップ 1 **[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access controls）] > [ユーザ（Users）]**を選択します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 [ユーザ名（Username）] に名前を入力し、ロールを割り当てます。「職務別の部門レポートへのアクセスの制限」を参照してください。

ステップ 4 パスワードを設定します。

ステップ 5 [保存（Save）] をクリックします。

設定のベスト プラクティス

- Web セキュリティアプライアンスおよび Umbrella ホスト間で一貫性のあるタイムゾーンを設定します。

  検索結果に表示される時間は、Cisco Advanced Web Security Reporting インスタンスの「ローカルの」時間を表しています。デフォルトでは、アプライアン ログへの入力はすべて TZ = GMT に設定されます。

- ローカル `admin` アカウントのパスワードを記録します（選択した認証方法に関係なく）。
- ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にします。
  1. **[設定（Settings）] > [データ（Data）] > [データの高速化（Data Acceleration）]** を選択します。
  2. [編集（Edit）] をクリックします。
  3. [高速化の編集（Edit Acceleration）] を選択します。
  4. [高速化（Accelerate）] チェックボックスをオンにし、[サマリの範囲（Summary Range）] で [3ヵ月（3 months）] を選択します。
  5. [保存（Save）] をクリックします。

Cisco Advanced Web Security Reporting アプリケーションを起動および停止するコマンド

Linux の場合

Cisco Advanced Web Security Reporting アプリケーションを停止するには、次の手順に従います。

ディレクトリを /cisco_wsa_reporting/ に変更し、次のコマンドを実行します。

```
./shutdown.sh
```

Cisco Advanced Web Security Reporting アプリケーションを起動するには、次の手順に従います。

ディレクトリを /cisco_wsa_reporting/ に変更し、次のコマンドを実行します。

```
/startup.sh
```

Windows の場合

Cisco Advanced Web Security Reporting アプリケーションを停止するには、次の手順に従います。

ディレクトリを <install_home>\ に変更し、次のコマンドを実行します。

```
shutdown.bat
```

Cisco Advanced Web Security Reporting アプリケーションを起動するには、次の手順に従います。

ディレクトリを <install_home>\ に変更し、次のコマンドを実行します。

```
startup.bat
```

（注） Windows では、 <install_home>\ は C:\Program Files\Cisco\CiscoWSAReporting です。

インストール後のタスク

AWSR で HTTPS を有効にする

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、**[設定（Settings）]** > **[システム（System）]** > **[サーバ設定（Server Settings）]**を選択します。

ステップ 2 [全般設定（General Settings）] をクリックします。

ステップ 3 [Cisco Advanced Web Security ReportingアプリケーションでSSL（HTTPS）を有効にする（Enable SSL (HTTPS) in Cisco Advanced Web Security Reporting application）] で [はい（Yes）] をクリックします。

デフォルトでは、暗号化が有効になっている場合、AWSR の導入ではデフォルトの証明書を指します。証明書に署名については、「証明書の生成と署名」を参照してください。

ステップ 4 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 5 **web.conf** ファイルを編集し、エントリ enableSplunkWebSSL = 1 がそのファイルに存在することを確認します。

ステップ 6 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 7 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

ステップ 8 ここで、Cisco Advanced Web Security Reporting アプリケーションへのアクセスに使用する URL の前に `https://` を追加する必要があります。

クライアントが開始した再ネゴシエーションの無効化

ステップ 1 `root` ユーザとして CLI にログインし、`$AWSR_Home/etc/system/local/` に移動します。

ステップ 2 **web.conf** ファイルを開き、最後に `allowSslRenegotiation = false` というテキストを追加します。

ステップ 3 `$AWSR_HOME` ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

証明書の生成と署名

詳細については、「証明書の生成と署名」を参照してください。

Strict Transport Security ヘッダーの送信

ステップ 1 `root` ユーザとして CLI にログインし、`$AWSR_Home/etc/system/local/` に移動します。

ステップ 2 **server.conf** ファイルを開き、次のテキストを追加します。

```
[httpServer]
replyHeader.X-XSS-Protection= 1; mode=block
replyHeader.Content-Security-Policy = script-src 'self'; object-src 'self'
[sslConfig]
sendStrictTransportSecurityHeader = true
```

ステップ 3 **web.conf** ファイルを開き、次のテキストを追加します。

```
sendStrictTransportSecurityHeader = true
replyHeader.X-XSS-Protection= 1; mode=block
```

ステップ 4 `$AWSR_HOME` ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 5 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

パスワードの長さの制限

このトピックでは、パスワードを設定または変更するときに、許可する最小パスワードの長を文字数で設定する方法について説明します。

ステップ 1 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 2 **authentication.conf** ファイルを開き、最後に次のテキストを追加します。

```
[splunk_auth]
minPasswordLength = <positive integer>
```

ここで、positive integer には 12、127、256 などの正の数を指定できます。

（注） **authentication.conf** ファイルが $AWSR_HOME/etc/system/local パスに存在しない場合、$AWSR_HOME/etc/system/default パスから $AWSR_HOME/etc/system/local パスにファイルをコピーして、上記手順 2 で指定した変更を行います。

ステップ 3 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

圧縮アルゴリズムの無効化

次の手順では、SSL/TLS 圧縮アルゴリズムの情報漏えいに関する脆弱性に対処します。

ステップ 1 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 2 **server.conf** ファイルを開き、**[sslConfig]** セクションの下に allowSslCompression = false を追加します。

ステップ 3 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

ライセンスおよび移行

バージョン 4.5 で追加された 3 つの AMP レポートは、Web セキュリティ アプライアンス AMP ログでのみサポートされます。

バージョン 4.0 以降の Advanced Web Security Reporting アプリケーションは、WSA をサポートします。これは「ハイブリッドレポート」と呼ばれます。ハイブリッドレポートを使用するには、新しいライセンスをインストールする必要があります。既存のライセンスで Web セキュリティアプライアンス専用レポートを引き続き使用できます。次のようにライセンスと移行のさまざまな状況が考えられます。

- v3.0（Web セキュリティ アプライアンス）から v4.0（Web セキュリティ アプライアンスのみ）レポートへの移行
- v3.0（Web セキュリティ アプライアンス専用）から v4.0 ハイブリッド レポートへの移行
- 新しいハイブリッド レポート ライセンス

v3.0（Webセキュリティアプライアンス）からv4.0（Webセキュリティアプライアンスのみ）レポートへの移行

バージョン 4.0 以降のソフトウェアをインストールし、以前にインストール済みのライセンスで引き続き Web セキュリティ アプライアンス レポートを使用できます。さらに、バージョン 4.0 以降のソフトウェアには評価ライセンスが組み込まれています。このライセンスにはハイブリッド レポートを評価できるレポート ソース タイプが追加されています。

v3.0（Web セキュリティ アプライアンス専用）から v4.0 ハイブリッド レポートへの移行

前の項で説明したように、バージョン 4.0 以降のソフトウェアをインストールしても、以前にインストール済みのライセンスで引き続き Web セキュリティ アプライアンス レポートを使用できます。また、組み込みの評価ライセンスを使用してハイブリッド レポート機能を評価できます。

Web セキュリティアプライアンス専用レポートからハイブリッドレポートに移行するには、Cisco Technical Assistance Center（TAC）のサポートケースを開いて既存のライセンスを削除し、ソースタイプの完全なリストを含む（`ciscoumbrella` が https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case に含まれています）新しいハイブリッド レポート ライセンスをインストールする必要があります。

（注） バージョン 3.0 Web セキュリティアプライアンス専用レポートからバージョン 4.0 以降のハイブリッドレポートにアップグレードする場合にのみ TAC への連絡が必要です。

新しいハイブリッド レポート ライセンス

新規の Cisco Advanced Web Security Reporting ユーザとしてバージョン 4.0 以降のソフトウェアをインストールした後に、Web セキュリティアプライアンスおよびハイブリッド Web セキュリティレポートを利用する場合は、評価期間中に無制限で組み込みの評価ライセンスを使用できます。評価期間後も継続する場合や、評価の制限を超えてレポートを提供する場合は、マスター ハイブリッド ライセンスを取得する必要があります。新規インストールでは、注文時に提供される infodoc を使用して、ライセンスを要求します。

ハイブリッド レポート ライセンスの問題

ハイブリッド レポート ライセンスに関する問題が発生した場合は、シスコに問い合わせる前に、適切な Umbrella パッケージを購入していることを確認します。

また、レポートアプリケーション ライセンス（SMA-WSPL-LIC=、SMA-WSPL-LOW-LIC=、または SMA-WSPL-HIGH-LIC= を購入した場合に発行されます）に含まれているソースタイプ

が、wsa_trafmonlogs、wsa_accesslogs、wsa_w3clogs、wsa_syslog、および wsa_amplogs **のみ**であることを確認します。

シスコの Cisco Advanced Web Security Reporting アプリケーションを使用してこれ以外のソースタイプ（ps など）のログを処理すると、ライセンス違反エラーが発生します。このようなエラーは、別のソースタイプのログを生成する他のアプリケーションをインストールした場合に発生することがあります。

バージョン 4.0 以降のアップグレードに関するライセンスの考慮事項

履歴データ転送を処理するためには、最初に大量のデータに適した評価ライセンスが最低限必要になります。その後、Cisco Advanced Web Security Reporting のライセンスが必要になります。

1. 履歴データの初回アップロード時と毎日の継続的な運用時の両方でインデックスが作成されるデータ量を考慮します。
2. 履歴データ転送に十分な評価ライセンスを取得してアップロードします。
3. インデックスが作成される該当ソースタイプの予想データに対して十分な Cisco Advanced Web Security Reporting ライセンスを取得およびアップロードします。
4. ライセンスのタイプを、トライアルから評価または Cisco Advanced Web Security Reporting に変更します。
5. インデックスが正しいプールにレポートされることを確認します。
    1. **[設定（Settings）] > [システム（System）] > [ライセンス（Licensing）]**に移動して、該当するライセンススタックで [今日使用されたプールインデクサボリューム（Pools Indexers Volume used today）] 行を探します。
    2. [編集（Edit）] をクリックすると、必要に応じて日単位の最大ボリューム割り当ておよび割り当てられたインデクサを変更できます。
    3. 変更を行わなかった場合は [キャンセル（Cancel）]、変更した場合は [送信（Submit）] をクリックします。

ライセンスのインストール

ライセンスを取得するには、注文時に提供された情報を参照してください。次の手順に従って、Cisco Advanced Web Security Reportingライセンスをインストールします。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションを起動（ブラウザ ウィンドウで http://<hostname>:8888 と入力）して、デフォルト admin ユーザとしてログインします。

ステップ 2 **[設定（Settings）] > [システム（System）] > [ライセンス（Licensing）]**に移動します。

ステップ 3 [ライセンスの追加（Add License）] をクリックします。

ステップ 4 XML ライセンス ファイルを参照します。

ステップ 5 [インストール（Install）] をクリックします。

アクセスおよびトラフィックモニタログファイルのフォルダ構造の作成

ログ	デフォルト パス	変数
トラフィック モニタ	/$Input_base/wsa_hostname/trafmonlogs/	$Input_base=path of root FTP folder host_name=Web Security appliance
アクセス	/$Input_base/wsa_hostname/accesslogs/	$Input_base=deployment host_name=Web Security appliance
AMP	/$Input_base/wsa_hostname/amplogs/	$Input_base=deployment host_name=Web Security appliance

履歴データのインポートおよびインデックス作成

始める前に

- 「Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード」にリストされている構成タスクを実行します。
- フォルダ構造を理解します。「アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成」を参照してください。

ステップ 1 ログ ファイルのフォルダ構造に、履歴ログ ファイルをコピーします。

ステップ 2 Cisco Advanced Web Security Reporting アプリケーションで、`admin` としてログインします。

ステップ 3 データがインポートされていることを確認します。

1. **[設定（Settings）] > [データ（Data）] > [インデックス（Indexes）]**を選択します。
2. サマリー行までスクロールします。
3. [最も古いイベント（Earliest event）] および [最新のイベント（Latest event）] カラムに適切な日付が表示されることを確認します。履歴データのインポートを評価ライセンスで実行した場合は、アカウント用にダウンロードしたデフォルト ライセンスをインストールし、非プロダクション ライセンスをすべて削除してください。

ヒント チェックサムエラーにより、アプリケーションで設定された入力タイプのファイルにインデックスが生成されない場合は、`inputs.conf` ファイルの各入力スタンザに `crcSalt = <source>` 行を追加します（次のセクション「（任意）インデックス生成後にログ ファイルを削除するようアプリケーションを設定する」で、`inputs.conf` ファイルの編集について説明します）。

次のタスク

- Web セキュリティ アプライアンス ログのデータ入力の設定

（任意）インデックス生成後にログ ファイルを削除するようアプリケーションを設定する

始める前に

inputs.conf ファイルが `<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/` ディレクトリに存在しない場合は、入力コンフィギュレーション ファイル `<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf` を作成します。

ステップ 1 テキストエディタを使用して、以下のファイルを開きます。

```
<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf
```

ステップ 2 次のようにセグメントを追加します。

```
[batch:///home/logger/incoming/wsa176.wga/accesslogs/*]
host_segment = 4
disabled = false
sourcetype = wsa_accesslogs
move_policy = sinkhole
```

ここでの最初の行は、Web セキュリティ アプライアンス ログが送信される FTP ディレクトリ パスです。2 行目はホスト名を含む FTP パスの一部です。3 行目はこの FTP 入力を有効にします。4 行目でこの入力のソースを指定します。最後の行（`move_policy = sinkhole`）は、インデックス生成後の元のデータの削除を有効にします。

ステップ 3 inputs.conf ファイルを保存して、**[設定（Settings）]**>**[システム（System）]**>**[サーバコントロール（Server controls）]**に移動し、[リスタート（Restart）] をクリックして Cisco Advanced Web Security Reporting アプリケーションを再起動します。

継続的なデータ転送の設定

はじめる前に

- 履歴データのインポートおよびインデックス作成
- ログファイルへのパスを把握します（「アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成」）。
- Cisco Advanced Web Security Reporting アプリケーションに admin としてログインします。

Web セキュリティ アプライアンス ログのデータ入力の設定

（注） 複数のWSAからのデータ入力を設定するには、ホストごとに次の手順を繰り返してください。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、次の手順を実行します。

- **[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [ファイルとディレクトリ（Files & directories）]**を選択します。

ステップ 2 CiscoWSA とラベル付けされた入力をすべて無効にします。

ステップ 3 [新規（New）] をクリックします。

ステップ 4 Web セキュリティ アプライアンス ログを送信する FTP ディレクトリへのフル パスを入力します。

このパスと Web セキュリティ アプライアンスの [ログ設定（Log Subscription）] ページで指定した FTP パスが一致する必要があります。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [新規（New）] をクリックします。

ステップ 7 [ソースタイプ（Source Type）] にタイプを入力し、[ソースタイプのカテゴリ（Source Type Category）] でカテゴリを選択して、[ソースタイプの説明（Source Type Description）] に説明を入力します。

wsa_accesslogs：レイヤ 4 トラフィックモニタおよび高度なマルウェア防御レポートを除くすべてのレポートに使用します。

wsa_trafmonlogs：レイヤ 4 トラフィックモニタレポートで使用します。

wsa_amplogs：高度なマルウェア防御レポートで使用します。

ステップ 8 [アプリコンテキスト（App context）] ドロップダウン リストから [Advanced Web Security Reporting 6.2.0] を選択します。

ステップ 9 [定数値（Constant value）] をクリックし、[ホストフィールド値（Host field value）] フィールドに Web セキュリティアプライアンスのホスト名を入力します。

ステップ 10 宛先**インデックス**として [メイン（Main）] を選択します。

ステップ 11 [レビュー（Review）] をクリックして指定した値を確認します。

ステップ 12 [送信（Submit）] をクリックします。

（注） **[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [ファイルとディレクトリ（Files & directories）]**で、新しいデータ入力エントリを確認できます。

Web セキュリティ アプライアンス Syslog のデータ入力の設定

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、次の手順を実行します。

- **[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [TCP]**を選択します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 [TCP] ボタンをクリックして [ポート（Port）] フィールドに `514` と入力します。残りのフィールドは空白のままにします。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [新規（New）] をクリックします。

ステップ 6 [ソースタイプ（Source Type）] フィールドで `wsa_syslog` を入力します。

ステップ 7 [アプリコンテキスト（App Context）] で [Advanced Web Security 6.2.0] を選択します。

ステップ 8 [ホスト（Host）] セクションの [方法（Method）] で [カスタム（Custom）] をクリックし、[ホストフィールド値（Host field value）] に Web セキュリティ アプライアンスのホスト名を入力します。

ステップ 9 宛先インデックスとして [メイン（Main）] を選択します。

ステップ 10 [レビュー（Review）] をクリックして指定した値を確認します。

ステップ 11 [送信（Submit）] をクリックします。

ステップ 12 **[設定（Settings）] > [データ入力（Data inputs）] > [TCP]**に移動して新しい入力エントリを確認します。

（注） 複数アプライアンス設定を使用して、各アプライアンスの Cisco Advanced Web Security Reporting アプリケーションでこれらの手順を繰り返す必要があります。2 つの異なるデータ入力に同じポートを使用することはできません。ただし、`inputs.conf` ファイルを編集して複数のアプライアンスを設定することもできます。

Web セキュリティアプライアンスからのログ転送の確立

始める前に

- ログファイルへのパスを把握します（「アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成」）。
- 転送の頻度を決定します。60 分単位以下には設定できません。
- Cisco Web セキュリティアプライアンスの Web インターフェイスを開きます。

ステップ 1 Cisco Web セキュリティアプライアンスの Web インターフェイスで、**[システム管理（System Administration）] > [ログ設定（Log Subscription）]**に移動します。

ステップ 2 [ログ設定を追加（Add Log Subscription）] をクリックするか、既存のサブスクリプションの名前をクリックして編集します。

ステップ 3 サブスクリプションを設定します（この例では、アクセス、AMP エンジン、およびトラフィックモニタログを扱います）。

設定	ログ タイプ	値
ログ タイプ（Log Type）	アクセス（Access）	accesslogs
	トラフィックモニタ（Traffic Monitor）	trafmonlogs
	AMPエンジン（AMP Engine）	amp_logs
ログ名（Log Name）	いずれか	ログ ディレクトリの名前。
（AsyncOS のリリースによって異なります） **ファイルサイズ別ロールオーバー（Rollover by File Size）** **最大ファイル サイズ（Maximum File Size）**	いずれか	500 MB 以下を推奨します。
（このオプションを利用できるかどうかは AsyncOS のリリースによって異なります） 時刻によりロールオーバー（Rollover by Time）	いずれか	1 時間（1h）またはそれ以上頻繁なカスタム ロール オーバー間隔を推奨します。AMP ログの場合は 1 分（1m）を推奨します。
ログ スタイル（Log Style）	アクセス（Access）	**Squid**
	トラフィックモニタ（Traffic Monitor）	該当なし
	AMPエンジン（AMP Engine）	該当なし

設定	ログ タイプ	値
ログ レベル（Log Level）	アクセス（Access）	該当なし
	トラフィックモニタ（Traffic Monitor）	該当なし
	AMPエンジン（AMP Engine）	[デバッグ（Debug）] を選択します。 （注） AMP レポートの場合は、[ログレベル（Log Level）] を [デバッグ（Debug）]に変更しないと、情報がほとんどレポートされないので注意してください。
（任意）カスタム フィールド	アクセス（Access）のみ	%XK（ウエブ レピュテーション脅威の理由を追加します）。
取得方法（Retrieval Method） **リモート サーバ上の FTP（FTP on Remote Server）**	いずれか	[ホスト名（Hostname）] : Cisco Advanced Web Security Reporting ホストの IP アドレスまたはホスト名。 [ディレクトリ（Directory）] : Cisco Advanced Web Security Reporting インスタンスディレクトリの名前。 [ユーザ名/パスワード（Username/Password）] : アプリケーションにアクセスするための FTP ユーザ名とパスワード。 （注） Cisco Advanced Web Security Reporting と Web セキュリティアプライアンス間の接続が失われると、接続が復旧するまで、その期間のログは使用できません。

設定	ログ タイプ	値
取得方法（Retrieval Method） **Syslog 送信（Syslog Push）**	どちらか	[ホスト名（Hostname）]：Cisco Advanced Web Security Reporting ホストの IP アドレスまたはホスト名。 [プロトコル（Protocol）]：TCP。 [ファシリティ（Facility）]：[auth] を選択します。 （注） Cisco Advanced Web Security Reporting と Web セキュリティアプライアンス間の接続が失われると、接続が復旧するまで、その期間のログは使用できません。

（注） [ログ設定を追加（Add Log Subscription）] ページからオンラインヘルプにアクセスすると、すべての設定に関する詳細情報が表示されます。

Umbrella のログの更新

始める前に

- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。
- プライベート AWS S3 バケットが必要です。プライベート S3 バケットを設定するには、https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket を参照してください。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、次の手順を実行します。

[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [Cisco CWS/Umbrellaログ（Cisco CWS/Umbrella Logs）]を選択します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 このデータ入力の**名前**を入力します。

ステップ 4 Umbrella から提供された **client_id**、**s3_key**、および **s3_secret** を入力します。**client_id** は、Umbrella のAWS バケット名です。

ステップ 5 [詳細設定（More settings）] チェックボックスをオンにして、Umbrella ログを取得できる [間隔（Interval）] を秒単位で指定します。デフォルトは 3600 です。

ステップ 6 [sourcetypeの設定（Set sourcetype）] ドロップダウン リストで [手動（Manual）] を選択します。

ステップ 7 [ソースタイプ（Source Type）] を入力します。`ciscoumbrella`（Umbrella レポートの場合）を入力します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 成功したことを示す画面が表示されます。

（注） シスコが管理する AWS S3 バケットではサポートされていません。

部門メンバーシップ クエリーのセットアップ（任意）

次の条件で部門メンバーシップ要件のセットアップ手順を実行します。

- Cisco Advanced Web Security Reporting アプリケーションでロールにバンドルされた AD/LDAP グループを使用します。
- 組織の役割に基づくデータのレポートを実行する。

関連情報：

- 職務別の部門レポートへのアクセスの制限

部門メンバーシップ レポートのセットアップ

始める前に

- Linux ユーザ：次のコマンドを使用して、ldapsearch ツールをインストールします。

```
sudo yum install openldap-clients
```

ステップ 1 **[設定（Settings）]>[データ（Data）]>[データ入力（Data inputs）]>[AD/LDAPサーバの詳細（AD/LDAP Server Details）]** を選択します。

ステップ 2 [LDAP ADサーバの詳細（LDAP AD Server Details）] をクリックします。

ステップ 3 [LDAP ADサーバの詳細（LDAP AD Server Details）] ページで、次のサーバ情報を入力して [保存（Save）] をクリックします。

- [AD/LDAPサーバ名（AD/LDAP Server Name）]
- [AD/LDAPユーザ名（AD/LDAP User Name）]
- [AD/LDAPユーザパスワード（AD/LDAP User Password）] と [確認（Confirm）]
- [AD/LDAPグループ名（AD/LDAP Group Name）]（グループ DN を指定）

ステップ 4 **[設定（Settings）]** > **[データ（Data）]** > **[データ入力（Data inputs）]** > **[スクリプト（scripts）]**を選択して、メンバーシップのスクリプトを有効にします。

- Linux の場合、スクリプト名は `discovery.py` です。
- Windows の場合、スクリプト名は `discovery.vbs` です。

メンバーシップのスクリプトは、毎日実行するように初期設定されます。間隔は秒単位で設定されます。変更するには、**[設定（Settings）]**>**[データ（Data）]**>**[データ入力（Data inputs）]**>**[スクリプト（scripts）]**に移動して、`discovery` ファイル内の間隔を編集します。

`<install_home>/etc/apps/cisco_wsa_reporting/lookups/departments.csv` ファイルを調べることで、departments.csv ファイルにユーザデータを含むスクリプトが入力されていることを確認できます。

`departments.csv` ファイルはロールベースのレポート機能で使用されます。このファイルには、次の記述が含まれています。

- 最初の列に user（cs ユーザ名：認証されたユーザ名）。
- 後続の列に displayname、groupname（スクリプトを使用して Active Directory または LDAPサーバから取得）。アクセス ログ（user_id フィールド）に存在するユーザに対して、対応する表示名とグループが displayname と department フィールドに表示されます。

このファイルは、手動でも、ロールディスカバリ スクリプト（アプリケーションの `bin` フォルダで使用可能）をスクリプト入力として設定する方法でも編集できます。Linux と Windows 用のスクリプトがあります。

- ファイルがアプリケーションの参照フォルダにあることを確認します。
- Linux バージョンを使用している場合は、CLI コマンド **ldapsearch** がインストールされ、アプリケーション ユーザのパスにあることを確認します。
- Windows バージョンを使用している場合は、エラーの原因と発生場所についての特定情報を明示するため、「option explicit」がコメントアウトされる可能性があります。
- LDAP パスの構文が正しいことを確認します。
- バインド サービスのアカウント名が正しいことを確認します。
- 正しいバインド パスワードが入力されていることを確認します。
- ポート 389 経由でリモート マシンにテスト接続します。
- 正しい属性がメンバー名に設定されていることを確認します。
- 正しい属性がグループ メンバーシップに使用されたことを確認します。
- 正しい属性がグループ名に設定されていることを確認します。

（注） Windows では、この時点で `departments.csv` ファイルにデータが入力されていない場合、ディレクトリを `<install_home>\etc\apps\cisco_wsa_reporting\bin`（`<install_home>` は `C:\Program Files\Cisco\CiscoWSAReporting` です）に変更して、`cscript discovery.vbs` を実行します。

職務別の部門レポートへのアクセスの制限

始める前に

- ユーザのデータ閲覧が特定の部門またはグループからのデータに制限されている場合、レイヤ 4 トランスポート モニタ（L4TM）データを利用できるのは管理者のみに限られることを理解します。これは、L4TM データが部門または役割にリンクされていないためです。
- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

ステップ 1 **[設定（Settings）] > [ユーザと認証（Users and authentication）] > [アクセスコントロール（Access Controls）] > [役割（Roles）]**を選択します。

ステップ 2 [新規（New）] をクリックするか、既存の役割を編集します。

ステップ 3 役割の検索制限を定義します。

例：

営業部門データの閲覧だけに役割を限定する場合は、[検索条件の制限（Restrict search terms）] フィールドに `department=sales` と入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 **[設定（Settings）] > [データ（Data）] > [データの高速化（Data Acceleration）]** を選択します。

ステップ 6 [編集（Edit）] をクリックします。

ステップ 7 [高速化の編集（Edit Acceleration）] を選択します。

ステップ 8 [高速化（Accelerate）] チェック ボックスをオフにして、[保存（Save）] をクリックします。

新しい役割の検索の制限を確認するには、新しいユーザを作成して検索を実行します。「新規ユーザーの作成」を参照してください。手順 4 で作成した役割に割り当てられたユーザの検索結果には、役割で指定された検索文字列に一致するイベントのみが表示されます。

（注） ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にします。これにより、レポートのパフォーマンスが強化されます。「設定のベストプラクティス」を参照してください。

関連情報：

- ユーザ（Users）

部門メンバーシップ レポートのトラブルシューティング

ヒント

- Linux ユーザ：ldapsearch ツールが Cisco Advanced Web Security Reporting ユーザのパスにあることを確認します。
- departments.csv ファイルがアプリケーションの参照フォルダに存在することを確認します。
- Windows ユーザ：`option explicit` をコメントアウトし、エラーの発生と原因について、より具体的な情報を示します。
- LDAP パスの構文が正しいことを確認します。
- バインド サービスのアカウント名が正しいことを確認します。
- 正しいバインド パスワードが入力されていることを確認します。
- ポート 389 経由でリモート マシンにテスト接続します。
- 正しい属性がメンバー名に設定されていることを確認します。
- 正しい属性がグループ メンバーシップに使用されたことを確認します。
- 正しい属性がグループ名に設定されていることを確認します。

スケジュール済 PDF レポートのセットアップ（任意）

Cisco Advanced Web Security Reporting アプリケーションユーザは、ダッシュボード、ビュー、検索またはレポートからの PDF 出力の生成をスケジュールできます。次の設定手順に従って、スケジュール済 PDF レポートをセットアップします。

- 電子メール アラートの設定
- PDF レポート生成のスケジュール

電子メール アラートの設定

PDF レポートの生成後に電子メールアラートを送信するように Cisco Advanced Web Security Reporting アプリケーションを設定できます。

始める前に

- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、次の手順を実行します。

- **[設定（Settings）]** > **[システム（System）]** > **[サーバ設定（Server Settings）]** > **[電子メール設定（Email Settings）]**を選択します。

ステップ 2 電子メール アラートの送信に必要なメール サーバ設定を入力または更新します。

1. [メールホスト（Mail host）]：SMTP サーバのホスト名を入力します。
2. [Eメールセキュリティ（Email security）]（任意）：電子メールセキュリティオプションを選択します。アプリケーションでは SMTP サーバとの通信に SSL または TLS を使用できます。
3. [ユーザ名（Username）]：SMTP サーバ認証で使用する名前を入力します。
4. [パスワード（Password）]：指定したユーザ名に設定するパスワードです。
5. [パスワードの確認（Confirm password）]：パスワードを再入力します。

ステップ 3 必要な電子メールの形式情報を入力します。

1. [リンクのホスト名（Link hostname）]：出力結果の作成に使用するサーバのホスト名です。
2. [送信元（Send email as）]：電子メールの送信元として表示される送信者名です。
3. [電子メールのフッター（Email footer）]：送信電子メールのフッターに表示されるメモです。

ステップ 4 必要に応じて、[レポート用紙サイズ（Report Paper Size）] および [レポート用紙の向き（Report Paper Orientation）] を選択して、PDF レポート設定を変更します。

ステップ 5 [保存（Save）] をクリックします。

PDF レポート生成のスケジュール

カスタム ダッシュボードに対して PDF レポートの定期的な生成および電子メール送信をスケジュールできます。カスタムダッシュボードの作成については、「ダッシュボードとして保存」を参照してください。

始める前に

- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

ステップ 1 [カスタムダッシュボード（Custom Dashboards）] メニューから目的のダッシュボードを選択します。

ステップ 2 **[編集（Edit）]** > **[PDF配信のスケジュール（Schedule PDF Delivery）]**を選択します。

ステップ 3 [PDFスケジュールの編集（Edit PDF Schedule）] ダイアログボックスで、[PDFのスケジュール（Schedule PDF）] をオンにして、スケジュール、電子メール、およびページのオプションを指定します。

ステップ 4 （任意）[テストメールの送信（Send Test Email）] をクリックして、生成された PDF が指定した電子メール アドレスに添付ファイルとして送信されることを確認します。

ステップ 5 （任意）[PDFのプレビュー（Preview PDF）] をクリックして、生成された PDF をプレビューします。

ユーザの作成または変更

新規ユーザを作成します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access controls）] > [ユーザ（Users）] > [新規追加（Add New）]**を選択します。

ステップ 3 次の詳細を入力します。

1. [ユーザ名（Username）] : 一意のユーザ名を入力します（必須）。
2. [フルネーム（Full Name）] : 姓名を入力します。
3. [電子メールアドレス（Email Address）] : 電子メールアドレスを入力します。
4. [タイムゾーン（Time Zone）] : タイム ゾーンを選択します。
5. [デフォルトアプリ（Default app）] : **cisco_wsa_reporting**（Advanced Web Security Reporting 7.0）
6. [ロールに割り当てるまたはこのユーザのロールを作成する（Assign to roles or Create a role for this use）] : ユーザロールを新規作成するには、「ロールの作成または変更」を参照してください（必須）。
7. [パスワード（Password）]（必須） : パスワードを入力します。
8. [パスワードの確認（Confirm Password）]（必須） : パスワードを再入力します。

ステップ 4 [保存（Save）] をクリックします。

Delete Users

既存のユーザを削除するには、次の手順を実行します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access controls）] > [ユーザ（Users）]**を選択します。

ステップ 3 各ユーザーの横にある [削除（Delete）] をクリックして、そのユーザを削除します。

（注） admin ユーザは削除できません。

ロールの作成または変更

ユーザロールを作成または変更します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access controls）] > [ユーザ（Users）] > [新規追加（Add New）]**を選択します。

ステップ 3 次の詳細を入力して、新しいロールを作成します。

1. [ロール名（Role Name）]：ロールの一意の名前を入力します。
2. [デフォルトアプリ（Default app）]：cisco_wsa_reporting
3. [検索の制限（Search Restrictions）]：このロールによって実行される検索の範囲を制限します。このロールの検索結果には、この検索文字列に一致するイベントのみが表示されます。

   – [検索条件の制限（Restrict search terms）]（source、host、index（以下で設定可能）、eventtype、sourcetype、search フィールド、*、OR および AND を含めることができます）。たとえば、「host=web* OR source=/var/log/*」となります。

   –[検索時間範囲の制限（Restrict search time range）]（このロールの検索の最大時間枠（秒単位）を設定します。たとえば、これを「60」に設定すると、このロールの検索は、検索で指定された最新の時刻の 1 分前に制限されます。これを「0」に設定して時間枠を明示的に無限にすることも、「-1」に設定してこのロールの時間枠の設定を解除することもできます（インポートされたロールによってオーバーライドできます））。

   –[ユーザレベルの同時検索ジョブの制限（User-level concurrent search jobs limit）]（このロールの各ユーザの同時検索ジョブの最大数を入力します）。

   – [このロールの各ユーザーのリアルタイム検索ジョブ（Real-time search jobs for each user of this role）]（この数は、通常の検索ジョブの制限とは無関係です）。

   – [ロールレベルの同時検索ジョブの制限（Role-level concurrent search jobs limit）]（このロールの累積同時検索ジョブの最大数を入力します）。

   –[ロールレベルの同時リアルタイム検索ジョブの制限（Role-level concurrent real-time search jobs limit）]（このロールの累積同時リアルタイム検索ジョブの最大数を入力します。この数は、通常の検索ジョブの制限とは無関係です）。

   – [合計ジョブディスククォータの制限（Limit total jobs disk quota）]（ユーザの検索ジョブで使用できる合計ディスク容量を MB 単位で入力します。たとえば、「100」の場合はこのロールは合計 100 MB に制限されます）。

4. [継承（Inheritance）]：機能とインデックスを継承するロールを指定します。継承された機能とインデックスを無効にすることはできません。複数のロールが指定されている場合、このロールは最も範囲の広い権限を持つ親から機能を継承します。以下は、機能によって異なる事前定義ロールのリストです。

   – admin

   – can_delete

– power

– splunk_system_role

– user

– wsa_admin

5. [機能（Capabilities）]：使用可能な機能名のリストについては、以下の「機能のリスト」の表を参照してください。
6. [デフォルトで検索されるインデックス（Indexes searched by default）]：インデックスが指定されていない場合にデフォルトで検索されるインデックスを設定します。このロールを持つユーザは、index= を使用して他のインデックスを検索できます（たとえば「index=special_index」）。
7. [インデックス（Indexes）]：このロールの検索を指定されたインデックスに制限します。
8. [保存（Save）] をクリックします。

機能のリスト

機能名	実行できる機能
accelerate_datamodel	データモデルのアクセラレーションを有効または無効にします。このデータモデルの自動アクセラレーションを有効にするにはアクセラレーションを true に設定します。データ内のイベント、フィールド、および個別のフィールド値の数に応じて、追加のスペースが必要です。詳細については、『Knowledge Manager Manual』を参照してください。
accelerate_search	レポートのアクセラレーションを有効または無効にできます。ユーザには schedule_search 機能も割り当てる必要があります。変換コマンドを使用する検索で機能します。詳細については、『Knowledge Manager Manual』を参照してください。
admin_all_objects	オブジェクトに設定されている制限に関係なく、システム内の任意のオブジェクトにアクセスして変更できます。ユーザオブジェクト、検索ジョブ、レポート、ナレッジオブジェクトなどです。Linux 環境でのルートへのアクセスと同じように、ACL 制限をバイパスできます。
change_authentication	認証設定を変更し、認証をリロードできます。認証の詳細については、『Securing Splunk Enterprise Manual』を参照してください。

機能名	実行できる機能
change_own_password	自身のパスワードを変更できます。
delete_by_keyword	「delete」演算子を使用できます。「delete」コマンドは、検索によって返されたすべてのイベントを削除済みとしてマークします。これによりデータが検索結果に表示されないようにマスクされますが、実際にはディスク上のrawデータは削除されません。詳細については、『Search Manual』を参照してください。
dispatch_rest_to_indexers	REST検索コマンドをインデクサにディスパッチできます。
edit_deployment_client	導入クライアントの設定を変更できます。導入クライアントの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_deployment_server	導入サーバの設定を変更できます。フォワーダや他の導入クライアントにプッシュされるリモート入力を変更または作成できます。導入サーバの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_dist_peer	分散検索用のピアを追加および編集できます。詳細については、『Managing Indexers and Clusters of Indexers Manual』マニュアルを参照してください。
edit_forwarders	SSL、バックオフスキームなどの設定を含む、フォワーダ設定を変更できます。TCPおよびSyslog出力管理ハンドラでも使用されます。
edit_httpauths	httpauth-tokensエンドポイントを介してユーザセッションを編集および終了できます。
edit_indexer_cluster	インデクサクラスタを編集できます。インデクサの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_input_defaults	サーバ設定エンドポイントを使用して、入力データのデフォルトのホスト名を変更できます。
edit_monitor	ファイルのモニタリングに関する入力を追加し、設定を編集できます。標準入力エンドポイントおよびワンショット入力エンドポイントでも使用されます。

機能名	実行できる機能
edit_roles	ロールを編集し、ユーザ/ロールのマッピングを変更できます。ユーザとロールエンドポイントの両方で使用されます。
edit_roles_grantable	ロールを編集し、限られたロールセットのユーザ/ロールのマッピングを変更できます。他のユーザに任意のロールを割り当てることができます。この機能を制限するには、authorize.conf で grantableRoles を設定します。例：grantableRoles = role1;role2;role3
edit_scripted	スクリプト入力を作成および編集できます。
edit_search_head_clustering	検索ヘッドのクラスタリング設定を編集できます。
edit_search_schedule_priority	通常よりも高いスケジュール優先度を検索に割り当てることができます。検索スケジューラの詳細については、『Knowledge Manager Manual』を参照してください。
edit_search_schedule_window	スケジュールウィンドウをスケジュールされたレポートに割り当てることができます。schedule_search 機能が必要です。検索スケジューラの詳細については、『Knowledge Manager Manual』を参照してください。
edit_search_scheduler	検索スケジューラを有効または無効にできます。『Knowledge Manager Manual』を参照してください。
edit_search_server	タイムアウト、ハートビート、ブラックリストなどの一般的な分散検索設定を編集できます。
edit_server	サーバ名、ログレベルなどの一般的なサーバ設定を編集できます。
edit_server_crl	サーバ名、ログレベルなどの一般的なサーバ設定を編集できます。一般的なサーバとイントロスペクトの設定を読み取る機能を継承します。
edit_sourcetypes	ソースタイプを編集できます。ソースタイプの詳細については、『Knowledge Manager Manual』を参照してください。
edit_splunktcp	別の Splunk インスタンスから TCP 入力を受信するための設定を変更できます。
edit_splunktcp_ssl	Splunk TCP 入力の SSL 固有の設定を表示または編集できます。

機能名	実行できる機能
edit_splunktcp_token	Splunktcp トークンを編集できます。
edit_tcp	一般的な TCP 入力を受信するための設定を変更できます。
edit_tcp_token	TCP トークンを変更できます。これは管理機能であり、システム管理者にのみ割り当てる必要があります。
edit_telemetry_settings	製品インストルメンテーションをオプトインまたはオプトアウトします。
edit_token_http	HTTP トークン入力の設定を作成、編集、表示、および削除できます。HTTP イベントコレクタ機能も有効にします。
edit_udp	UDP 入力の設定を変更できます。
edit_user	ユーザを作成、編集、または削除できます。edit_user 機能を持つロールは、他のユーザに任意のロールを割り当てることができます。この機能を制限するには、authorize.conf で grantableRoles を設定します。たとえば、grantableRoles = role1;role2;role3 とします。また、分散検索用の証明書を管理できます。
edit_view_html	HTML ベースのビューを作成、編集、または変更できます。
edit_web_settings	システム設定エンドポイントを介して web.conf の設定を変更できます。
embed_report	レポートを埋め込んだり、埋め込まれたレポートの埋め込みを無効にできます。
export_results_is_visible	Splunk Web の [結果のエクスポート（Export Results）] ボタンを表示または非表示にできます。デフォルト値はボタンを表示することです。
extra_x509_validation	x509 検証を追加できます。
get_diag	/streams/diag エンドポイントを使用して Splunk インスタンスからリモート診断を取得できます。
get_metadata	「メタデータ」検索プロセッサを使用できます。
get_typeahead	エンドポイントと先行入力検索フィールドで先行入力を使用できます。

機能名	実行できる機能
indexs_edit	ファイルサイズやメモリ制限などのインデックス設定を変更できます。
input_file	inputcsv（dispatch=t モードを除く）および inputlookup を介してファイルを入力として追加できます。
license_edit	ライセンスを編集できます。
license_tab	ライセンスにアクセスして変更できます。この属性は非推奨です。
license_view_warnings	データ制限を超えている場合、またはライセンスの有効期限に達した場合に、警告メッセージを表示できます。これらの警告は、システムバナーに表示されます。
list_accelerate_search	アクセラレーションレポートを表示できます。ユーザはレポートを高速化できません。
list_deployment_client	導入クライアントの設定を表示できます。
list_deployment_server	導入サーバの設定を表示します。
list_forwarders	データ転送の設定を一覧表示して表示できます。TCP および Syslog 出力管理ハンドラーで使用できます。
list_httpauths	httpauth-tokens エンドポイントを介してユーザセッションを表示できます。
list_indexer_cluster	インデクサクラスタのリストと、バケット、ピアなどのインデクサクラスタオブジェクトを表示できます。
list_indexerdiscovery	インデクサ検出の設定を表示できます。インデクサ検出ハンドラでも使用されます。
list_inputs	ファイル、TCP、UDP、スクリプトなどからの入力を含む、さまざまな入力のリストを表示できます。
list_introspection	インデクサ、検索、プロセッサ、キューなどのイントロスペクション設定と統計を読み取ることができます。
list_search_head_clustering	アーティファクト、委任されたジョブ、メンバー、キャプテンなどの検索ヘッドクラスタリングオブジェクトを一覧表示して表示できます。
list_search_scheduler	検索スケジューラジョブのリストを表示できます。

機能名	実行できる機能
list_settings	サーバ名やログレベルなどのサーバとイントロスペクションの設定を一覧表示して表示できます。
list_storage_passwords	/storage/passwords エンドポイントを一覧表示して表示したり、GET を実行したりできます。/storage/passwords エンドポイントに対して POST を実行するには、admin_all_objects 機能をロールに追加する必要があります。
output_file	outputcsv（dispatch=t モードを除く）や outputlookup などのファイル出力を作成できます。
pattern_detect	[検索（Search）] ビューの [パターン（Patterns）] タブを表示して使用できます。
request_remote_tok	リモート認証トークンを取得できます。これにより、分散ピア管理を実行し、レプリケーションをバンドルして、古い 4.0.x Splunk インスタンスに検索を分散できます。
rest_apps_management	Python リモートアプリハンドラーのエントリとカテゴリの設定を編集できます。詳細については、restmap.conf を参照してください。
rest_apps_view	Python リモートアプリハンドラーでさまざまなプロパティを一覧表示して表示できます。詳細については、restmap.conf を参照してください。
rest_properties_get	サービス/プロパティエンドポイントから情報を取得できます。
rest_properties_set	サービス/プロパティエンドポイントを編集できます。
restart_splunkd	サーバ制御ハンドラを介して Splunk Enterprise を再起動できます。
rtsearch	リアルタイム検索を実行できます。
run_debug_commands	debug コマンドを実行できます。たとえば、「Summarize」を実行できます。
run_multi_phased_searches	redistribute コマンドを使用して検索を実行できます。このコマンドは、分散検索環境で並列削減検索処理を呼び出します。この機能は、デフォルトではどのロールにも割り当てられていません。

機能名	実行できる機能
schedule_search	保存された検索をスケジュールして、アラートを作成および更新し、トリガーされたアラート情報を確認できます。
search	検索を実行できます。詳細については、『Search Manual』を参照してください。
search_process_config_refresh	「refresh search-process-config」CLI コマンドを使用して、アイドル状態の検索プロセスを手動でフラッシュできます。
srchFilter	検索フィルタを管理できます。詳細については、『Search Manual』を参照してください。
srchIndexesAllowed	検索インデックスを実行できます。詳細については、『Search Manual』を参照してください。
srchIndexesDefault	デフォルトの検索インデックスを設定できます。
srchJobsQuota	検索ジョブのクォータを設定できます。
srchMaxTime	検索の最大時間を設定できます。
use_file_operator	「file」検索演算子を使用できます。「file」検索演算子は非推奨です。
web_debug	Web ファイルをデバッグできます。

表 *1 : Windows* 固有の機能

機能名	実行できる機能
edit_modinput_admon	admon.conf のモジュラ入力を編集します。
edit_modinput_perfmon	perfmon.conf でモジュラ入力を編集します。
edit_modinput_winhostmon	Windows ホストデータをモニタリングするための入力を追加および編集します。
edit_modinput_winnetmon	Windows ネットワークデータをモニタリングするための入力を追加および編集します。
edit_modinput_winprintmon	Windowsプリンタデータをモニタリングするための入力を追加および編集するために必要です。
edit_win_admon	（非推奨）

機能名	実行できる機能
edit_win_eventlogs	Windows のイベントログを編集します。
edit_win_perfmon	（非推奨）
edit_win_regmon	（非推奨）
edit_win_wmiconf	wmi.conf を編集します。
list_pdfserver	PDF サーバファイルを表示します。
list_win_localavailablelogs	すべてのローカル Windows イベントログを一覧表示します。
srchTimeWin	検索時間制限を設定します。
write_pdfserver	PDF サーバファイルに書き込みます。