CTA システムにログ ファイルを アップロードするための WSA の設定

最終更新日:2015 年 8 月 27 日

目次

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングと見なされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

メモ:*読者に留意していただきたいこと*を示します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意:**注意が必要なことを*示しています*。機器の損傷またはデータ損失を予防するための注意事項が記述されています。**

警告:**安全上の重要事項です。**

危険があることを示します。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国語版については、各警告文の末尾に提示されている番号をもとに、この機器に付属している各国語で記述された安全上の警告を参照してください。

これらの注意事項を保存しておいてください。

規制:追加情報および規制要件または顧客要件に準拠するために定められています。

はじめに

このドキュメントでは、Cisco Web Security Appliance（WSA）を設定し、そのログ ファイルを Cisco Cognitive Threat Analytics（CTA）システムにアップロードする方法について説明します。ログ ファイルがシステムにアップロードされると、CTA はデータを分析し、その結果を CTA ポータルに報告します。

前提条件

要件

Cisco ScanCenter は、Cisco Cloud Web Security の管理ポータルです。最初に、WSA 用に Cisco ScanCenter にデバイス アカウントを作成する必要があります。

- Cisco ScanCenter にログインします。
- [脅威（Threats）] タブをクリックします。
- ページの右上隅にあるグローバル設定メニューのアイコンをクリックします。
- [デバイス アカウント（Device Accounts）] をクリックします。
- アップロード方法として [自動（Automatic）] を選択します。

詳細については、『Cisco ScanCenter Administrator Guide（Cisco ScanCenter 管理ガイド）』の「Proxy Device Uploads（プロキシ デバイスのアップロード）」のセクションを参照してください。

デバイス アカウントを作成したら、Cisco ScanCenter の [デバイス アカウントの追加（Add Device Account）] ページから次の情報をコピーして WSA 設定に貼り付けます。

- SCP ホスト：`etr.cloudsec.sco.cisco.com`
- プロキシ デバイス用に生成されたユーザ名。大文字と小文字が区別され、プロキシ デバイスごとに異なります。

WSA には、次が必要です。

- WSA のホスト名または IP アドレス
- WSA の管理ユーザ パスワード（デフォルトのパスワードは `ironport`）
- WSA は、追加のプロキシ アップストリームを使用せずに、インターネットに直接接続する必要があります。
- WSA 管理インターフェイスと SCP ホスト `etr.cloudsec.sco.cisco.com` との間にポート `22` を使用したネットワーク接続が必要です。この接続を許可するには、ファイアウォールのルールの調整が必要になる場合があります。

注意：このドキュメントの情報は、ラボ環境にあるデバイスに基づいて作成されたものです。対象のネットワークが実稼働中である場合には、どのようなコンフィギュレーション コマンドについても、その潜在的な影響力を理解しておいてください。

注意：設定上の変更を確定すると、WSA が再起動します。そのため、プロキシ経由で接続しているユーザは一時的に接続を解除される場合があります。ロード バランサの背後で WSA が高可用性（HA）モードで動作していない場合は、営業時間外のメンテナンス時間帯に WSA を設定し、実稼働時間中にユーザに影響を与えないようにすることをお勧めします。

使用されるコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンでテストされています。

- WSA 8.5.1 GD
- WSA 8.0.8
- WSA 7.7.5

このドキュメントの情報は、次のハードウェアでテストされています。

- WSA S100V
- WSA S160
- WSA S300V

設定

プロキシの設定

1. Web ブラウザで次のように指定し、WSA に移動します。http://wsa_*hostname*:8080/
2. 必要に応じて、セキュアではない HTTPS 証明書を承認し、続行します。
3. admin としてログインします。
4. [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] に移動します。
5. [ログサブスクリプションを追加（Add Log Subscription）] をクリックします。
6. [ログタイプ（Log Type）] プルダウンで、[W3C ログ（W3C Logs）] を選択します。
7. [ログ名（Log Name）] フィールドに、ログ ディレクトリのわかりやすい名前を入力します。
8. [選択されたログフィールド（Selected Log Fields）] ボックスですべての項目を選択し、[削除（Remove）] をクリックして事前に選択されたログ フィールドを削除します。
9. [カスタムフィールド（Custom Fields）] ボックスに、次の項目を入力します。項目を区切るには改行を使用します。

```
timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
```

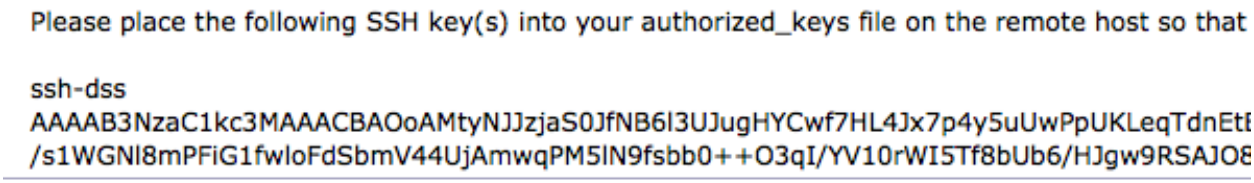
```
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

メモ: WSA バージョン 7.7.5 では AMP がサポートされていないため、4 つの「`x-amp`」フィールドは追加しないでください。

10. すべての項目を入力したら、[追加 >>(Add >>)] をクリックします。
11. [ファイル サイズによるロールオーバー(Rollover by File Size)] フィールドに `500M` と入力します。
12. [時刻によりロールオーバー(Rollover by Time)] プルダウンで、[カスタム時間間隔(Custom Time Interval)] を選択します。
13. [次の間隔でロールオーバー(Rollover every)] フィールドに、`55m` と入力します。

プロキシの背後のユーザ数	推奨アップロード期間
不明または 2000 未満	55 分
2000 ～ 4000	30 分
4000 ～ 6000	20 分
6000 超	10 分

14. [ファイル名(File Name)] フィールドに `w3c_log` と入力します。
15. [ログ圧縮(Log Compression)] をオンにし、圧縮を有効にします。
16. [検索方法(Retrieval Method)] として [リモートサーバでの SCP(SCP on Remote Server)] を選択します。
17. [SCP ホスト(SCP Host)] フィールドに、Cisco ScanCenter で指定した SCP ホストを入力します。次に例を示します。`etr.cloudsec.sco.cisco.com`
18. [SCP ポート(SCP Port)] フィールドに `22` と入力します。
19. [ディレクトリ(Directory)] フィールドに `/upload` と入力します。
20. [ユーザ名(Username)] フィールドに、Cisco ScanCenter のデバイス用に生成されたユーザ名を入力します。デバイス ユーザ名は大文字と小文字が区別され、プロキシ デバイスごとに異なります。
21. [ホスト キー チェックを有効にする(Enable Host Key Checking)] チェックボックスをオンにし、[自動スキャン(Automatically Scan)] オプション ボタンを選択します。
22. [送信(Submit)] をクリックします。
23. WSA 管理コンソールに公開 SSH キーが表示されます。このキーをコピーし、Cisco ScanCenter のデバイス アカウントに貼り付けます。プロキシ デバイスと CTA システム間の認証が成功すると、ログ ファイルをプロキシ デバイスから CTA システムにアップロードし、分析できるようになります。



24. [変更内容を確定(Commit Changes)] をクリックします。
    注意: 設定上の変更を確定すると、WSA が再起動します。そのため、プロキシ経由で接続しているユーザは一時的に接続を解除される場合があります。ロード バランサの背後で WSA が高可用性(HA)モードで動作していない場合は、営業時間外のメンテナンス時間帯に WSA を設定し、実稼働時間中にユーザに影響を与えないようにすることをお勧めします。

New Log Subscription

Log Subscription

Log Type: W3C Logs

Log Name: w3clogs

(will be used to name the log directory)

Log Fields:

Available Log Fields

CMF
DCF
bytes
c-ip
c-port
cs(Cookie)
cs(Referer)
cs(User-Agent)
cs(X-Forwarded-For)
cs-auth-group
cs-auth-mechanism
cs-bytes
cs-method
cs-mime-type
cs-uri
cs-url

Add >>

Selected Log Fields

timestamp
x-elapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
sc-body-size
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score

Custom Fields

(Use line breaks to separate multiple entries)

Rollover by File Size: 500M Maximum

(Add a trailing K or M to indicate size units)

Rollover by Time: Custom Time Interval

Rollover every: 55m

(Example: 120s, 5m 30s, 4h, 2d)

File Name: w3c_log

Log Compression: Enable

Log Exclusions (Optional):

(Enter the HTTP status codes of transactions that should not be included in the W3C Log)

Retrieval Method:

FTP on prg5-wsa-s160.cisco.com

Maximum Number of Files: 100

FTP on Remote Server

FTP Host:

Directory:

Username:

Password:

SCP on Remote Server

SCP Host: etr.cloudsec.sco.cisco.com SCP Port: 22

Directory: /upload

Username: d111...

Enable Host Key Checking

Automatically Scan

Enter Manually

ユーザ名を解決するための Active Directory への接続

ログ サブスクリプションを作成する場合は Active Directory のセットアップは必要ありません。すでに設定している場合は、影響を受けるデバイスの特定に役立ちます。CTA システムのユーザ名を確認するには、WSA ですべてのユーザを認証できるようにする必要があります。これを行うには、透過的ユーザ識別機能を使用します。詳細については、『Cisco Web Security Appliances User Guide（Cisco Web Security Appliance ユーザ ガイド）を参照してください。

1. [ネットワーク（Network）] > [認証（Authentication）] に移動します。
2. Active Directory に接続するレルムを追加します。
    a. [Active Directory サーバ（Active Directory Server）] は、ドメインの名前であり、ホスト名ではありません。
    b. [Active Directory ドメイン（Active Directory Domain）] は、大文字形式でのドメインの名前です。
    c. [ドメインの結合（Join Domain）] をクリックした後、ドメイン管理者権限を持つユーザのクレデンシャルを入力します。これにより、WSA が独自のユーザを Active Directory に作成します。
    d. [Active Directory Agent を使用して透過ユーザ識別を有効にする（Enable Transparent User Identification using Active Directory agent）] をオンにします。Cisco Active Directory Agent が稼動しており、Active Directory に接続できるようになっている必要があります。サーバ ホスト名と共有秘密を入力します。
3. [Web セキュリティ マネージャ（Web Security Manager）] > [アイデンティティ（Identities）] に移動します。
4. [グローバル アイデンティティ ポリシー（Global Identity Policy）] を編集します。[ユーザを透過的に識別する ID および認証（Identification and Authentication to Identify Users Transparently）] を設定し、前のステップで作成したレルムをピックします。
5. [ネットワーク認証グローバル認証の設定（Network Authentication Global Authentication Settings）] で [グローバル設定を編集（Edit Global Settings）] をクリックし、[認証サービスが使用できない場合のアクション（Action if Authentication Service Unavailable）] を [認証に失敗した場合にすべてのトラフィックをブロック（Block all traffic if authentication fails）] に設定します。これにより、非認証ユーザ用に追加される「*」が **userid access** ログ フィールドに追加されないようになります。

複数の WSA を設定するための SMA の使用

Cisco コンテンツ セキュリティ管理仮想アプライアンス（SMA）は複数の WSA にわたる管理機能を一元化します。ただし、SMA はログ アップロードのセットアップ時には役立ちません。構成時の設定は WSA ごとに異なるため、個別に WSA を設定する必要があります。

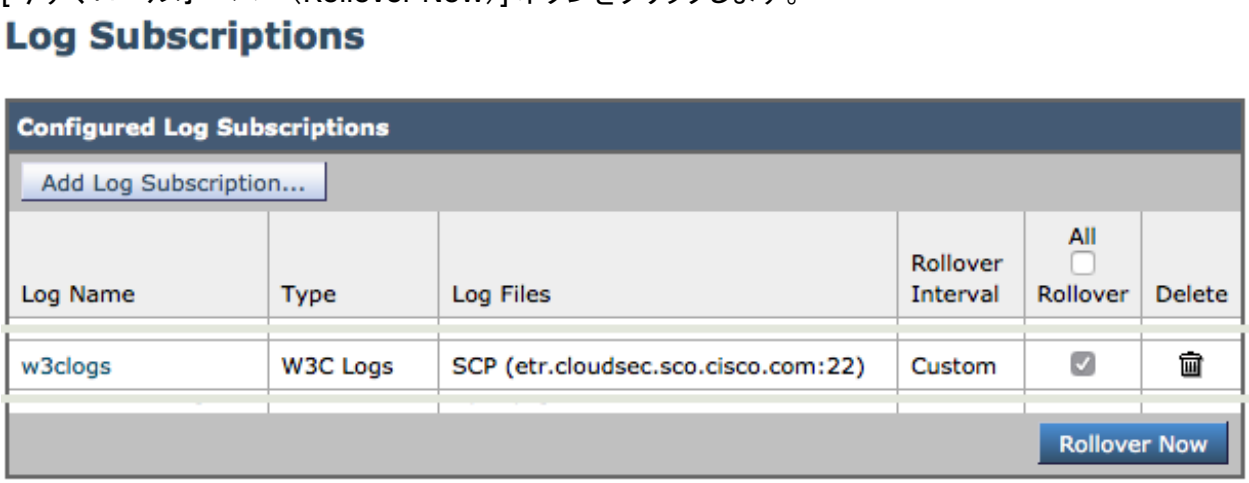
次のステップ

Cisco ScanCenter 内でデバイス アカウントを選択し、公開 SSH キーを入力します。詳細については、『Cisco ScanCenter Administrator Guide, Release 5.2（Cisco ScanCenter 管理ガイド、リリース 5.2）』の第 32 章「Proxy Device Uploads（プロキシ デバイスのアップロード）」のセクションを参照してください。

トラブルシューティング

接続をテストするには、WSA に即時アップロードを試行させます。

1. [ログ サブスクリプション（Log Subscriptions）] ページに移動します。
2. テストするサブスクリプションで、[ロールオーバー（Rollover）] チェックボックスをオンにします。
3. [今すぐロールオーバー（Rollover Now）] ボタンをクリックします。



マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用法、サービス要求の送信方法、および追加情報の収集方法については、「*What's New in Cisco Product Documentation*」（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

「*What's New in Cisco Product Documentation*」に配信登録すると、新しい（または改訂された）シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。