ASA 8.2： ASDM を使用した Syslog の設定

目次

概要

このドキュメントでは、Adaptive Security Device Manager（ASDM）の GUI を使用して Cisco 適応型セキュリティ アプライアンス（ASA）8.x の syslog の設定方法を説明します。 システム ログ メッセージは、構成の変更、ネットワーク設定の変更、デバイスのパフォーマンスの変更を管理者に通知するために Cisco ASA によって生成されるメッセージです。 システム ログ メッセージの分析により、管理者は根本原因分析を実行すれば簡単にエラーのトラブルシューティングを行うことができます。

syslog メッセージは主にその重大度に基づいて区別されます。

1. 重大度 0：緊急メッセージ：リソースが使用できない
2. 重大度 1：アラート メッセージ：緊急措置が必要
3. 重大度 2：クリティカル メッセージ：危険な状態

4. 重大度 3：エラー メッセージ：エラー状態
5. 重大度 4：警告メッセージ：警告状態
6. 重大度 5：通知メッセージ：正常だが重要な状態
7. 重大度 6：情報メッセージ：単なる情報メッセージ
8. 重大度 7：デバッグ メッセージ：デバッグ メッセージのみ**注:** 最も高い重大度レベルは緊急で、最も低い重大度はデバッグです。

Cisco ASA によって生成されたサンプルの syslog メッセージを次に示します。

- %ASA-6-106012： IP_address から IP_address への IP、16 進数の IP オプションを拒否
- %ASA-3-211001： メモリ割り当てエラー
- %ASA-5-335003： 適用されている NAC のデフォルト ACL、ACL： ACL 名：ホスト アドレス

数値は X は「%ASA-X-YYYYYY:」で指定され、 メッセージの重大度を示します。 たとえば、「%ASA-6-106012」は情報メッセージであり、「%ASA-5-335003」は、エラー メッセージです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA バージョン 8.2
- Cisco ASDM バージョン 6.2

このドキュメントの情報は、特定の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。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ASDM を使用した基本的な syslog 設定

Enable Logging

次の手順を実行します。

1. [Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択し、[Enable logging] オプションにチェック マークします。
2. バッファ サイズを指定して、内部バッファに syslog メッセージをログできます。[Configure Flash Usage] をクリックし、フラッシュ設定を定義することにより、フラッシュ メモリにバッファの内容を保存することも選択できます。

3. バッファに格納されているログ メッセージは上書きされる前に、FTP サーバに送信できます。 [Configure FTP Settings] をクリックし、次に示すように FTP サーバの詳細を指定します。

無効なロギング

要件に基づいて特定の syslog ID を無効にすることができます。

注: [Include timestamp in syslogs] オプションにチェック マークを選択することによって、syslog へのフィールドとして生成された日付と時刻を追加できます。

1. 無効にする syslog を選択して [Edit] をクリックします。
2. [Edit Syslog ID Settings] ウィンドウで、[Disable messages] オプションをチェック マークし [OK] をクリックします。
3. 無効になった syslog は、[Syslog ID Setup] ドロップダウン メニューから [Disabled syslog IDs] を選択することによって別のタブで確認できます。

電子メールへのロギング

電子メールで syslog を送信するには、ASDM を使用して次の手順を実行します。

1. [Configuration] > [Device Management] > [Logging] > [E-Mail Setup] を選択します。 [Source E-Mail Address] フィールドは、送信元として syslog に電子メール ID を割り当てるのに有効です。 送信元の電子メール アドレスを指定します。 ここで、電子メール受信者を追加するために [Add] をクリックします。
2. *宛先の電子メール アドレス*を指定し、*重大度*を選択します。 重大度に基づいて、異なる電子メール受信者を定義できます。 [E-Mail Setup] ペインに戻るには、[OK] をクリックします。これは、次の設定になります。
3. [Configuration] > [Device Setup] > [Logging] > [SMTP] の順に選択し、SMTP サーバを指定します。

syslog サーバへのロギング

専用 syslog サーバへすべての syslog メッセージを送信できます。 ASDM を使用して次の手順を実行します。

1. [Configuration] > [Device Management] > [Logging] > [Syslog Servers] を順に選択し、[Add] をクリックし syslog サーバを追加ます。[Add Syslog Server] ウィンドウが表示されます。
2. サーバが IP アドレスとともに関連付けられているインターフェイスを指定します。 ネットワークの設定に基づいて*プロトコル*と*ポートの詳細*を指定します。 次に、[OK] をクリックします。**注:** Cisco ASA から syslog サーバへの到達可能性を確認します。
3. 設定された syslog サーバは次に示すように表示されます。 修正はこのサーバを選択する際に行うことができ、その後 [Edit] をクリックします。**注:** [Allow user traffic to pass when TCP syslog server is down] オプションにチェック マークします。 そうしない場合は、新しいユーザ セッションは ASA 経由で拒否されます。 これは、ASA と syslog サーバ間のトランスポート プロトコルが TCP の場合だけ適用可能です。 デフォルトでは、なんらかの原因で syslog サーバがダウンした場合に新しいネットワーク アクセスのセッションは Cisco ASA によって拒否されます。syslog サーバに送信される syslog メッセージのタイプを定義

するためには、「ロギング フィルタ」セクションを参照してください。

ASDM を使用した詳細な syslog 設定

イベント リストの使用

イベント リストを使って、宛先に送信される syslog メッセージのグループを含むカスタマイズされたリストの作成が可能になります。 イベント リストには次の 3 通りの方法で作成できます。

- メッセージ ID またはメッセージ ID の範囲
- メッセージの重大度
- メッセージ クラス

メッセージ ID またはメッセージ ID の範囲

次の手順を実行します。

1. [Configuration] > [Device Management] > [Logging] > [Event Lists] を順に選択し、[Add] をクリックして新しいイベント リストを作成します。
2. [Name] フィールドに名前を指定します。 新しいイベント リストを作成するには、[Message ID Filters] ペインで [Add] をクリックします。
3. Syslog メッセージ ID の範囲を指定します。 たとえば、ここでは TCP syslog メッセージがを取得します。 [OK] をクリックして完了します。
4. [Event Lists] ウィンドウに戻るために、再度 [OK] をクリックします。

メッセージの重大度

1. また、イベント リストはメッセージの重大度に基づいても定義できます。 別のイベント リストを作成するために、[Add] をクリックします。
2. 名前を指定し、[Add] をクリックします。
3. 重大度をエラーとして選択します。
4. [OK] をクリックします。

メッセージ クラス

また、イベント リストはメッセージ クラスに基づいても設定されます。 メッセージ クラスとは、セキュリティ アプライアンスの機能に関連する syslog メッセージのグループです。メッセージ クラスを使用すると、メッセージごとに個別にクラスを指定するのではなく、メッセージのクラス全体を指定できます。 たとえば、auth クラスを使用すると、ユーザ認証に関連するすべての syslog メッセージを選択できます。 一部の使用可能なメッセージ クラスを次に示します。

- All：すべてのイベント クラス
- auth：ユーザ認証
- bridge：トランスペアレント ファイアウォール
- ca：PKI の証明機関
- config：コマンド インターフェイス
- ha：フェールオーバー
- ips：侵入からの保護サービス
- ip：IP スタック
- np：ネットワーク プロセッサ

- ospf：OSPF ルーティング
- rip：RIP ルーティング
- session：ユーザ セッション

vpnclient-errors エラー メッセージ クラスに基づいたイベント クラスを作成するには、次の手順を実行します。 メッセージ クラス *vpnc* は、vpnclient に関するすべての syslog メッセージを分類するために使用できます。 このメッセージ クラスの重大度は「エラー」として選択されます。

1. 新しいイベント リストを作成するには、[Add] をクリックします。
2. 作成するメッセージ クラスに関連する名前を指定し、[Add] をクリックします。
3. ドロップダウン リストから *vpnc* を選択します。
4. 重大度をエラーとして選択します。 この重大度は、このメッセージ クラスだけに対してログに記録されたメッセージに適用できます。 [Add Event List] ウィンドウに戻るには、[OK] をクリックします。
5. イベント クラス/重大度を次に示します。 「vpnclient-errors」イベント リストの設定を完了するには、[OK] をクリックします。また、新しいイベント リスト「user-auth-syslog」が、「auth」のメッセージ クラスと、この特定のメッセージ クラスに対する重大度「警告」で作成されたことが、次のスクリーンショットに表示されます。 これを設定するには、イベント リストは「auth」のメッセージ クラスに関連し、「警告」レベル**までの**重大度を持つすべての syslog メッセージを指定します。**注:** ここでは、用語「までの」が重要です。 重大度を示している場合、そのレベルまでのすべての syslog メッセージがログに記録されることに注意してください。**注:** イベント リストは複数のイベント クラスを含むことができます。 「vpnclient-errors」イベント リストは [Edit] をクリックして修正され、新しいイベント クラス「ssl/error」を定義しています。

ロギングのフィルタの使用

ロギング フィルタは、指定した宛先に syslog メッセージを送信するために使用されます。 これらの syslog メッセージは「重大度」または「イベント リスト」に基づくこともできます。

以下は、このようなフィルタが適用される宛先のタイプです。

- 内部バッファ
- SNMP トラップ
- E-Mail
- コンソール
- Telnetセッション
- ASDM
- syslog サーバ

次の手順を実行します。

1. [Configuration] > [Device Management] > [Logging] > [Logging Filters] の順に選択し、ロギング先を選択します。 次に、[Edit] をクリックして設定を変更ます。
2. 重大度に基づいて syslog にメッセージを送信できます。 ここでは、例として表示するために**緊急**が選択されています。
3. またイベント リストで、特定の宛先に送信されるメッセージのタイプを指定することもできます。 [OK] をクリックします。
4. 変更を確認します。

以下は、電子メール サーバにメッセージのグループ（重大度に基づいた）を送信する方法の手順

です。

1. [Logging Destination] フィールドで [E-mail] を選択します。 次に [Edit] をクリックします。
2. [Filter on severity] オプションを選択し、必要な重大度を選択します。ここでは、**アラート**が重大度として選ばれています。すべてのアラート syslog メッセージが設定された電子メールに送信されることを確認できます。

Rate Limit

これは、Cisco ASA が指定された期間に宛先に送信する syslog メッセージの数を指定します。通常は、重大度に対して定義されます。

1. [Configuration] > [Device Management] > [Logging] > [Rate Limit] の順に選択し、必要な重要度を選択します。 次に [Edit] をクリックします。
2. 時間間隔とともに送信するメッセージ数を指定します。 [OK] をクリックします。**注:** これらの数値は例として指定されます。 これらはネットワーク環境のタイプによって異なります。変更後の値を次に示します。

アクセス ルールのヒットのロギング

ASDM を使用してアクセス ルールの一致数のログを記録できます。 デフォルトのロギング動作では、すべての拒否されたパケットの syslog メッセージを送信します。 許可されたパケット用の syslog メッセージはなく、これらはログに記録されません。 ただし、このアクセス ルールに一致するパケットの数を追跡するためにアクセス ルールにカスタム ロギング重大度を定義できます。

次の手順を実行します。

1. 必要なアクセス ルールを選択し、[Edit] をクリックします。[Edit the Access Rule] ウィンドウが表示されます。**注:** このイメージでは、[Logging Level] フィールドの [Default] オプションは Cisco ASA のデフォルトのロギング動作を示します。 これについての詳細については、「ロギング アクセス リストの動作」セクションを参照してください。
2. [Enable logging] オプションにチェック マークし、必要な重大度を指定します。 次に、[OK] をクリックします。**注:** [More Options] ドロップダウン タブをクリックすると、[Logging Interval] オプションを確認できます。 このオプションは、上記の [Enable Logging] オプションにチェックがマークされている場合にだけ強調表示されます。 このタイマーのデフォルト値は 300 秒です。 この設定は、アクセス ルールに一致するエントリがない場合に削除されるフロー統計情報のタイムアウト値の指定に役立ちます。 一致がある場合、ASA は syslog のロギング インターバル時間まで待機し、その一致を syslog に送信します。
3. 変更を次に示します。 代わりに、特定のアクセス ルールの [Logging] フィールドをダブルクリックし、そこに重大度を設定することもできます。**注:** ダブル クリックして同じ [Access Rules] ペインの [Logging Level] を指定する代替手段は、手動で作成されたアクセス ルール エントリだけで機能し、暗黙のルールには機能しません。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

このドキュメントでは、次の設定を使用します。

CiscoASA

```
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors access-list inside_access_in extended permit
ip host 10.10.10.20 any access-list inside_access_in
extended deny ip 10.20.10.0 255.255.255.0 host
20.20.20.200 access-list inside_access_in extended
permit ip 10.78.177.0 255.255.255.192 any log
emergencies pager lines 24 logging enable logging list
user-auth-syslog level warnings class auth logging list
TCP-conn-syslog message 302013-302018 logging list
syslog-sev-error level errors logging list vpnclient-
errors level errors class vpnc logging list vpnclient-
errors level errors class ssl logging buffered user-
auth-syslog logging mail alerts logging from-address
test123@example.com logging recipient-address
monitorsyslog@example.com level errors logging queue
1024 logging host inside 172.16.11.100 logging ftp-
bufferwrap logging ftp-server 172.16.18.10 syslog
testuser **** logging permit-hostdown no logging message
302015 no logging message 302016 logging rate-limit 600
86400 level 7 mtu outside 1500 mtu inside 1500 icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-623.bin asdm history enable arp timeout
14400 ! !--- Output Suppressed ! timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
```

```
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout TCP-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!--- Output Suppressed ! ! telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list no threat-
detection statistics TCP-intercept ! !--- Output
Suppressed ! username test password /FzQ9W6s1KjC0YQ7
encrypted privilege 15 ! ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global
smtp-server 172.18.10.20 prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4 : end
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- ASDM から syslog を確認できます。 [Monitoring] > [Logging] > [Real Time Log Viewer] の順に選択します。 出力例を下記に示します。

トラブルシューティング

問題： 失われた接続 ---- 終了した syslog 接続 ----

このエラーは、いずれかのコンテキストに対するデバイス ダッシュボードで ASDM のロギングを有効にしようとすると表示されます。

" -- _syslog_ --"」

ASDM が管理コンテキストに直接接続するために使われ ADSM ロギングがそこで無効になっている場合、サブコンテキストに切り替えて ASDM ロギングを有効にします。 エラーを受信しますが、syslog メッセージは syslog サーバに正常に到達します。

解決策

これは Cisco ASDM の既知の動作で、Cisco Bug ID CSCsd10699（登録ユーザ専用）に記載されています。 回避策として、管理コンテキストにログインする際に asdm ロギングを有効にします。

Cisco ASDM でリアルタイム ログを表示できない

問題は、リアルタイムのログが ASDM に表示できないことです。 これはどのように設定できま

すか。

解決策

Cisco ASA で次の設定を実行します。

```
ciscoasa(config)#logging monitor 6 ciscoasa(config)#terminal monitor ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス サポート
- テクニカルサポートとドキュメント - Cisco Systems