ASA SNMP 機能拡張の実装

目次

概要

このドキュメントでは、ソフトウェア リリース 9.1.5 およびリリース 9.2.(1) 以降の Cisco 適応型セキュリティ アプライアンス（ASA）5500-X シリーズ ファイアウォールで使用できる新しい簡易ネットワーク管理プロトコル（SNMP）機能について説明します。

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、Cisco ASA® ソフトウェア リリース 9.1.5 およびリリース 9.2.(1) 以降が稼働する Cisco ASA 5500-X シリーズ ファイアウォールに基づくものです。

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。

背景説明

ASA バージョン 9.1.5 および 9.2.1 では、次の SNMP 拡張機能が導入されました。

- 128 個の SNMP ホストのサポートが追加されました。
- cpmCPUTotal5minRev SNMP のオブジェクト識別子（OID）のサポートが追加されました。
- 1,472 バイトの SNMP メッセージのサポートが追加されました。

128 個の SNMP ホストのサポート

この機能により、現在の 32 個を超える SNMP ホストを ASA でサポートできるようになります。

目的

現在、ASA には合計 32 個の SNMP ホストのハード制限があります。 これには、トラップ用とポーリング用に設定できるホストが含まれています。 以下の項では、この機能がシングルおよびマルチコンテキスト モードに与える影響について説明します。

シングルコンテキスト モード

- 設定できるエントリの数（合計ホスト数）が大幅に増えます（4,096 個以上）。 ただし、これらのエントリのうち、トラップに使用できるのは 128 個だけです。
- ポーリング設定のために、最大 4,096 個のポーリング ホストと 128 個のトラップ ホストを設定できます。 ただし、ホストの数が増えた場合のパフォーマンスへの影響が不明であり、サポートされないため、システムをポーリングするサーバの実際の数は 128 個未満に制限する必要があります。

マルチコンテキスト モード

- 設定のために、コンテキストごとに最大 4,000 個のホストを使用できます。システム全体の合計ホスト数は、64,000 個までに制限されています。
- 設定されたホストの合計数のうち、（コンテキストごとに）128 個だけをトラップに使用で

きます。マルチコンテキスト モードでのトラップは、システム全体で 32,000 個までに制限されています。

- コンテキストごとに最大で合計 4,000 個のホストを設定できますが、コンテキストをポーリングするサーバの実際の数は 128 個に制限する必要があります。

説明

SNMP ホストの大規模なプールからネットワーク デバイスを監視する必要がある場合があります。 理想的には、ネットワーク デバイスを監視できる IP アドレスの IP 範囲またはサブネット、あるいはその両方を指定する機能が必要です。 現在の ASA にはこのような柔軟性がなく、SNMP ホストの最大数は 32 個に制限されています。

この機能のサポートには、次の 2 つの側面があります。

- ASA が最大 128 個の SNMP ホストを処理できるようにします。

- 非常に多くのホスト（詳細については前の項を参照してください）を 1 つのコマンドで設定できるように、必要なコンフィギュレーション コマンドを提供します。

ASA の現在の設計では、CLI で個々のホストを設定できるようになっています。 この機能では、さらに次の設計要件が考慮されました。

- **snmp-server host** CLI コマンドを保持したまま **snmp-server host-group** CLI コマンドを導入すること。

- **snmp-server host-group** CLI コマンドと **snmp-server host** CLI コマンドの両方でエントリを入力できること。

- SNMP バージョン 3 では、**snmp-server user** CLI コマンドを保持したまま **snmp-server userlist** CLI コマンドを導入すること。

- 設定の重複もサポートする必要があります。 たとえば、ネットワーク オブジェクト内で重複するホストに関して複数の **host-group** コマンドを指定できます。 同様に、現在のホストまたはホスト グループと重複する IP アドレスを持つホストを指定できます。 これにより、グループ全体を再設定しなくても、グループ内の一部のホストに対するパラメータを上書きするために使用できるメカニズムが提供されます。

この機能に関連するソフトウェアの制限事項および注意事項を次に示します。

- **snmp-server host-group** コマンドの一部として **[trap|poll]** が指定されていない場合、デフォルトは poll です。 このコマンドでは、同じホスト グループに対してトラップとポーリングの両方をイネーブルにできないことにも注意してください。 これが必要な場合は、関連するホストに **snmp-server host** コマンドを使用することを推奨します。

- 複数の異なる **host-group** コマンドにネットワーク オブジェクトを重複して指定できます。異なるネットワーク オブジェクトに共通のホストに対しては、最後のホスト グループに指定した値が適用されます。

次に例を示します。

```
object network network1
```

```
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

ホスト エントリを表示するには、**show snmp-server host** コマンドを入力します。

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

この機能の使用に関する重要な注意点を次に示します。

- 他のホスト グループと重複するホストまたはホスト グループが削除された場合、設定済みのホスト グループで使用されている値を使用してホストが再設定されます。
- ホストに関連付けられる値またはパラメータは、コマンドの実行順序に依存します。
- 設定済みのユーザ リストが特定のホスト グループによって使用されている場合、そのユーザ リストは削除できません。
- SNMP ユーザが特定のユーザ リストで参照されている場合、そのユーザは削除できません。
- ネットワーク オブジェクトが **host-group** CLI コマンドで使用されている場合、そのオブジェクトは削除できません。

設定

この新機能を実装するには、この項に示す情報を使用して ASA を設定します。

> **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。

CLI コマンド

SNMP バージョン 3 の場合、管理者はさまざまなユーザを指定したホスト グループに関連付けることができます。 これは、管理者が一連のユーザに対し、ホスト グループから ASA にアクセスできるようにする必要がある場合に便利です。 複数のユーザを含むユーザ リストを設定するには、次の CLI コマンドを使用します。

```
ASA(config)# [no] snmp-server user-list <list_name> username <user_name>
```

ユーザ リストをホスト グループに関連付けるには、CLI に次のコマンドを入力します。

```
[no] snmp-server host-group <interface> <network-object> [trap|poll]
[community [enc_type] <text>] [version {1 | 2c | 3 [user name | user-list
<list-name>]}] [udp-port <port_number>]
```

この単一のコマンドで、追加する必要がある複数のホストを示すネットワーク オブジェクトを指定できます。 このネットワーク オブジェクトを使用して、追加する必要がある IP アドレスのサブネット マスクまたは範囲を 1 つのコマンドで指定できます。 ネットワーク オブジェクトの一部として示された IP アドレスのすべてが SNMP ホスト エントリとして追加されます。 同様に、ユーザ リストに指定されたユーザごとに別個の SNMP ホスト エントリがあります。

管理者が SNMP サーバの新しい設定オプションをクリアおよび表示できるようにするには、次の各コマンドを使用します。

- clear configure snmp-server user-list
- clear configure snmp-server host-group
- show running-config snmp-server user-list
- show running-config snmp-server host-group

設定例

新しい SNMP グループ オプションを使用して、バージョン 2c のポーリング用の SNMP サーバ ホスト グループを作成するには、次の手順を実行します。

1. ネットワーク オブジェクトを作成します。
   ```
   asa(config)# object network network1
   asa(config-network-object)# range 64.103.236.40 64.103.236.50
   ```
2. SNMP ホスト グループを定義します。
   ```
   asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
   ```
3. SNMP バージョン 3 グループを定義します。
   ```
   asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
   ```
4. これらのグループをユーザと結び付けます。
   ```
   asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
   asa(config)#snmp-server user-list SNMP-List username cisco1
   asa(config)#snmp-server host-group inside network1 poll version 3 user-list SNMP-List
   ```

次の図は、Cisco Adaptive Security Device Manager（ASDM）内で行われる変更を示しています。

cpmCPUTotal5minRev SNMP OID のサポート

この機能により、cpmCPUTotal5minRev SNMP OID を ASA でサポートできるようになります。

目的

この機能は、cpmCPUTotal5minRev および cpmCPUTotal1minRev OID のサポートを ASA に追加し、現在サポートされている cpmCPUTotal5min および cpmCPUTotal1min OID を廃止します。 これらの OID の目的は、CPU 使用率を監視することです。 現在サポートされている OID の範囲は 1 ~ 100 ですが、新しくサポートされた OID の範囲は 0 ~ 100 です。 このように、より広い範囲をカバーする新しい OID のサポートが追加されました。

廃止された OID（cpmCPUTotal5min および cpmCPUTotal1min）は ASA でサポートされなくなるため、ASA をアップグレードしてから廃止された OID をポーリングすると、ASA はこれらの OID の情報を返さないことに注意してください。 ASA をアップグレードした後は、cpmCPUTotal5minRev および cpmCPUTotal1minRev で CPU 使用率を監視できるようになります。

CLI コマンド

この新機能によって導入される CLI の変更はありません。

新しい OID

この機能によって追加される新しい OID を次に示します。

- 1.3.6.1.4.1.9.9.109.1.1.1.1.7. cpmCPUTotal1minRev
- 1.3.6.1.4.1.9.9.109.1.1.1.1.8. cpmCPUTotal5minRev

1,472 バイトの SNMP メッセージのサポート

ASA プラットフォームでは、SNMP 要求の最大パケット サイズが 512 バイトに制限されています。 単一の SNMP 要求内で多数の MIB OID の一括クエリーを実行すると、ASA で SNMP 接続がタイムアウトし、エラー syslog が生成されます。 RFC3417 では、SNMP 要求の最大パケット サイズを 1,472 バイトにするように推奨されています。 これは、パケットの SNMP ペイロードのサイズです。 パケットの合計サイズを計算するには、さらにイーサネット ヘッダーと IP ヘッダーのサイズを追加する必要があります。

> **注:** この機能では、シングルコンテキスト モードとマルチコンテキスト モードの両方がサポートされます。

トラブルシューティング

ここでは、ASA のシステムに関する問題のトラブルシューティングに役立つ情報を提供します。

show コマンド

次の show コマンドは、ASA に関する問題のトラブルシューティングを行うときに役立ちます。

- asa# show run snmp-server host-group
  snmp-server host-group inside network1 poll version 3 user-list SNMP-List

- asa# **show run snmp-server user-list**
  snmp-server user-list SNMP-List username cisco1

- asa# **show snmp-server host**

次の CLI コマンドは、SNMP サーバのアドレス テーブルにあるエントリを表示します。これには、ホストの設定とホスト グループの設定の両方が含まれています。

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
object network network3
range 64.103.236.60 64.103.236.70 ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

ここに示すように、これらのコマンドは **host-group** コマンドで設定されたすべてのホストを表示します。 このコマンドを使用して、すべてのエントリが使用可能であることを確認できます。また、重複するホスト グループの相互確認を行うこともできます。