SNMP

この章では、Simple Network Management Protocol（SNMP）に Cisco ASA をモニタさせるための設定方法について説明します。

SNMP の概要

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。ASAは SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワーク デバイスをモニタできます。ASAはGET要求の発行を通じてSNMP読み取り専用アクセスをサポートします。SNMP書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIBは定義の集合であり、ASAは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別するSNMP OIDが含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *1 : SNMP* の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバ。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニタすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIBは、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMP イベントのモニタやASAなどのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニタおよび表示される情報の源をユーザに示すシステム。
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバと SNMP エージェント間でデータをクリアテキストで転送します。SNMPバージョン3は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA およびASASMは、SNMP グループとユーザの作成、およびセキュア

なSNMP通信の転送の認証と暗号化をイネーブルにするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティモデルにまとめられます。セキュリティ モデルはユーザとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザ

SNMPユーザは、指定されたユーザ名、ユーザが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、およびAES（128、192、および256バージョンで使用可能）です。ユーザを作成した場合は、それをSNMP グループに関連付ける必要があります。その後、そのユーザはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザ名を設定する必要があります。SNMP ターゲット IP アドレスとターゲット パラメータ名は ASA および ASA サービス モジュールで固有である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザ クレデンシャルが ASA および ASASM のクレデンシャルと一致するように設定してください。

ASA、ASA サービス モジュール、Cisco IOS ソフトウェアの間の実装には、Cisco IOSソフトウェア サービス モジュール

ASA および ASASM での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装と次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカル エンジン ID は、ASA または ASASM が起動されたとき、あるいはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザとグループを作成する必要があります。
- 正しい順序でユーザ、グループ、およびホストを削除する必要があります。
- snmp-server host コマンドを使用すると、着信 SNMP トラフィックを許可する ASA、ASAv、または ASASM のルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、『syslog メッセージ ガイド』を参照してください。

（注） SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMP を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーのガイドライン

各 ASA、ASAv または ASASM の SNMP クライアントは、それぞれのピアとエンジン データを共有します。エンジン データには、SNMP-FRAMEWORK-MIB の engineID、engineBoots、および engineTime オブジェクトが含まれます。エンジン データは flash:/snmp/*contextname* にバイナリ ファイルとして書き込まれます。

IPv6 のガイドライン

SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリを実行でき、IPv6 ソフトウェアを実行するデバイスから SNMP 通知を受信できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

（注） ユーザ リストの 1 人のユーザまたはユーザ グループをネットワーク オブジェクトに関連付けるためのコマンド **snmp-server host-group** は、IPv6 をサポートしていません。

その他のガイドライン

- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。
- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。

- 結果としてSNMP機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザ、ホストの順に行う必要があります。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザが削除されていることを確認する必要があります。
- ユーザを削除する前に、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。
- 特定のセキュリティモデルを使用して特定のグループに属するようにユーザが設定されている場合にそのグループのセキュリティ レベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザを追加します。
- MIB オブジェクトのサブセットへのユーザ アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザ コンテキストで設定された SNMP サーバ ホストが少なくとも 1 つ必要です。
- ASA 5585 SSP-40（NPE）のシャーシ温度を問い合わせることはできません。
- NMS が正常にオブジェクトを要求できない場合、またはASA からの着信トラップを適切に処理していない場合は、パケット キャプチャの実行が問題を判別する最も有効な方法となります。[Wizards] > [Packet Capture Wizard] を選択して、画面に表示される指示に従います。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの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。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。

- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- SNMPv3 エンジン ID はクラスタのメンバー間で同期されません。そのため、SNMPv3 については、クラスタの各ユニットでそれぞれ設定する必要があります。
- バージョン 9.4(1) では、ASA がサポートするコンテキストあたりの SNMP サーバのトラップ ホスト数に制限はありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

SNMP を設定します。

ここでは、SNMP の設定方法について説明します。

手順

ステップ 1 ASA から要求を受信するように SNMP 管理ステーションを設定します。

ステップ 2 SNMP トラップを設定します。

ステップ 3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP 管理ステーションの設定

SNMP 管理ステーションを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。デフォルトでは、SNMP サーバはイネーブルになっています。

ステップ 2 [SNMP Management Stations] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ホストが存在するインターフェイスを選択します。

ステップ 4 SNMP ホストの IP アドレスを入力します。

ステップ 5 SNMP ホストの UDP ポートを入力します。デフォルトのポート 162 をそのまま使用することもできます。

ステップ 6 SNMP ホストのコミュニティ ストリングを追加します。管理ステーションに対してコミュニティ ストリングが指定されていない場合は、[SNMP Management Stations] ペインの [Community String (default)] フィールドに設定されている値が使用されます。

ステップ 7 SNMP ホストで使用される SNMP のバージョンを選択します。

ステップ 8 前の手順で SNMP バージョン 3 を選択した場合は、設定済みユーザの名前を選択します。

ステップ 9 [Poll] チェックボックスまたは [Trap] チェックボックスのいずれかをオンにして、NMS との通信に使用する方式を指定します。

ステップ 10 [OK] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

NMS が設定され、その変更内容が実行コンフィギュレーションに保存されます。SNMP バージョン 3 の NMS ツールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

Configure SNMP Traps

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [Configure Traps] をクリックします。

[SNMP Trap Configuration] ダイアログボックスが表示されます。

ステップ 3 [SNMP Server Traps Configuration] チェックボックスをオンにします。

トラップは、[standard]、[IKEv2]、[entity MIB]、[IPsec]、[remote access]、[resource]、[NAT]、[syslog]、[CPU utilization]、[CPU utilization and monitoring interval]、および [SNMP interface threshold and interval] のカテゴリに分類されます。SNMP トラップを介して通知を発行するための SNMP イベントを指定するため、目的のチェックボックスをオンにします。デフォルトの設定では、すべての SNMP 標準トラップがイネーブルです。トラップ タイプを指定しない場合、デフォルトで **syslog** トラップに設定されます。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。デフォルトでは他のトラップはすべてディセーブルです。トラップをディセーブルにするには、該当するチェックボックスをオフにします。**syslog** トラップの重大度レベルを設定するには、**[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Filters]** の順に選択します。

ステップ 4 [OK] をクリックして、[SNMP Trap Configuration] ダイアログボックスを閉じます。

ステップ 5 [Apply] をクリックします。

SNMP トラップが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 SNMP バージョン 1 または 2c を使用する場合は、[Community String (default)] フィールドにデフォルトのコミュニティ ストリングを入力します。要求を ASA に送信するときに SNMP NMS で使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP NMS と管理対象のネットワーク ノード間の共有秘密です。ASA では、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは、大文字と小文字が区別される、最大 32 文字の英数字です。スペースは使用できません。デフォルトは public です。SNMP バージョン 2c では、NMS ごとに、別々のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの NMS にも設定されていない場合、ここで設定した値がデフォルトとして使用されます。

ステップ 3 ASA システム管理者の名前を入力します。テキストは、大文字と小文字が区別される、最大 127 文字の英数字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4 SNMP で管理している ASA の場所を入力します。テキストは、大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5 NMS からの SNMP 要求をリッスンする ASA ポートの番号を入力します。デフォルトのポート番号 161 をそのまま使用することもできます。

ステップ 6 [SNMP Host Access List] ペインで [Add] をクリックします。

[Add SNMP Host Access Entry] ダイアログボックスが表示されます。

ステップ 7 トラップの送信元となるインターフェイスの名前をドロップダウン リストから選択します。

ステップ 8 ASA に接続できる NMS または SNMP マネージャの IP アドレスを入力します。

ステップ 9 UDP のポート番号を入力します。デフォルトは 162 です。

ステップ 10 使用する SNMP のバージョンをドロップダウン リストから選択します。バージョン 1 または 2c を選択した場合は、コミュニティ ストリングを入力する必要があります。バージョン 3 を選択した場合は、ドロップダウン リストからユーザ名を選択する必要があります。

ステップ 11 要求の送信（ポーリング）だけに NMS を制限する場合は、[Server Poll/Trap Specification] 領域の [Poll] チェックボックスをオンにします。トラップの受信だけに NMS を制限する場合は、[Trap] チェックボックスをオンにします。両方のチェックボックスをオンにすると、SNMP ホストの両方の機能が実行されます。

ステップ 12 [OK] をクリックして、[Add SNMP Host Access Entry] ダイアログボックスを閉じます。

新しいホストが [SNMP Host Access List] ペインに表示されます。

ステップ 13 **Apply** をクリックします。

SNMP バージョン 1、2c、または 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User]** の順にクリックして、設定済みのユーザまたは新規ユーザをグループに追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。

（注） ユーザが作成された後は、そのユーザが属するグループは変更できません。

[Add SNMP User Entry] ダイアログボックスが表示されます。

ステップ 3 SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザには、認証も暗号化も設定されません。

（注） グループ名は変更できません。

ステップ 4 ユーザ セキュリティ モデル（USM）グループを使用する場合は、[USM Model]]タブをクリックします。

ステップ 5 [Add] をクリックします。

[Add SNMP USM Entry] ダイアログボックスが表示されます。

ステップ 6 グループ名を入力します。

ステップ 7 ドロップダウン リストからセキュリティ レベルを選択します。設定済みの USM グループをセキュリティ レベルとして SNMPv3 ユーザに割り当てることができます。

ステップ 8 設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバ グループ内で一意であることが必要です。

ステップ 9 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 10 [MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。

ステップ 11 認証に使用するパスワードを入力します。

ステップ 12 [DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 AES 暗号化を選択した場合は、使用する AES 暗号化のレベルとして、128、192、256 のいずれかを選択します。

ステップ 14 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 15 [OK] をクリックすると、グループが作成され（指定したユーザがそのグループに属する最初のユーザである場合）、[Group Name] ドロップダウン リストにそのグループが表示されます。またそのグループ内にユーザが作成されます。

[Add SNMP User Entry] ダイアログボックスが閉じます。

ステップ 16 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

ユーザのグループの設定

指定したユーザのグループからなる SNMP ユーザ リストを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMPv3 Users] ペインの [SNMPv3 User/Group] タブで **[Add]** > **[SNMP User Group]** の順にクリックし、設定済みのユーザ グループまたは新規ユーザ グループを追加します。グループ内に残る最後のユーザを削除すると、そのグループは ASDM により削除されます。

[Add SNMP User Group] ダイアログボックスが表示されます。

ステップ 3 ユーザ グループ名を入力します。

ステップ 4 既存のユーザまたはユーザ グループを選択する場合は、[Existing User/User Group] オプション ボタンをクリックします。

ステップ 5 新規ユーザを作成する場合は、[Create new user] オプション ボタンをクリックします。

ステップ 6 SNMP ユーザが属するグループを選択します。選択できるグループは次のとおりです。

- [Auth&Encryption]：このグループに属するユーザには、認証と暗号化が設定されます。
- [Authentication_Only]：このグループに属するユーザには、認証だけ設定されます。
- [No_Authentication]：このグループに属するユーザには、認証も暗号化も設定されません。

ステップ 7 設定済みユーザまたは新規ユーザの名前を入力します。ユーザ名は、選択した SNMP サーバグループ内で一意であることが必要です。

ステップ 8 [Encrypted] と [Clear Text] のいずれかのオプション ボタンをクリックして、使用するパスワードのタイプを指定します。

ステップ 9 [MD5] と [SHA] のいずれかのオプション ボタンをクリックして、使用する認証のタイプを指定します。

ステップ 10 認証に使用するパスワードを入力します。

ステップ 11 認証に使用するパスワードを確認のためにもう一度入力します。

ステップ 12 [DES]、[3DES]、[AES] の中からいずれかのオプション ボタンをクリックして、使用する暗号化のタイプを指定します。

ステップ 13 暗号化に使用するパスワードを入力します。パスワードの長さは、英数字で最大 64 文字です。

ステップ 14 暗号化に使用するパスワードを確認のためにもう一度入力します。

ステップ 15 [Members in Group] ペインの指定したユーザ グループに新規ユーザを追加するには、[Add] をクリックします。[Members in Group] ペインから既存のユーザを削除するには、[Remove] をクリックします。

ステップ 16 [OK] をクリックすると、指定したユーザ グループに新規ユーザが作成されます。

[Add SNMP User Group] ダイアログボックスが閉じます。

ステップ 17 [Apply] をクリックします。

SNMP バージョン 3 のパラメータが設定され、その変更内容が実行コンフィギュレーションに保存されます。

SNMP モニタリング

次の SNMP モニタリング用のコマンドを参照してください。**[Tools] > [Command Line Interface]** を使用して次のコマンドを入力できます。

- **show running-config snmp-server** [**default**]

  すべての SNMP サーバのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

  リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

SNMP ユーザベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザ リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは2つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMPサーバの設定済み特性を表示します。すべてのSNMPカウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザの設定済み特性を表示します。

SNMP の履歴

表 *2 : SNMP* の履歴

機能名	プラットフォーム リリース	説明
SNMP バージョン 1 および 2c	7.0(1)	クリア テキスト コミュニティ文字列を使用してSNMPサーバとSNMPエージェントの間でデータを送信することによって、ASA、ASAv、および ASASM のネットワーク モニタリングとイベント情報を提供します。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。

機能名	プラットフォーム リリース	説明
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザ、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。

機能名	プラットフォーム リリース	説明
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。
IF-MIB ifAlias OID のサポート	8.2(5)/8.4(2)	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。

機能名	プラットフォーム リリース	説明
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。

機能名	プラットフォーム リリース	説明
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザ リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP]。

機能名	プラットフォーム リリース	説明
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB および OID	9.2(1)	ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASAv が追加されました。 新しい ASAv プラットフォームをサポートするよう、CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 VPN 共有ライセンスの使用状況をモニタするための新しい SNMP MIB が追加されました。
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。

機能名	プラットフォーム リリース	説明
SNMP の MIB およびトラップ	9.3(2)	ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次の画面が変更されました。[Configuration] > [Device Management] > [Management Access] > [SNMP] > [Configure Traps] > [SNMP Trap Configuration]。
SNMP の MIB およびトラップ	9.4(1)	SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。

機能名	プラットフォーム リリース	説明
コンテキストごとに無制限の SNMP サーバ トラップ ホスト	9.4(1)	ASA は、コンテキストごとに無制限の SNMP サーバ トラップ ホストをサポートします。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 変更された ASDM 画面はありません。
ISA 3000 のサポートが追加されました。	9.4(1.225)	ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。**snmp-server enable traps entity** コマンドが変更され、新しい変数 *l1-bypass-status* が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。 変更された ASDM 画面はありません。
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。
Precision Time Protocol（PTP）の E2E トランスペアレント クロック モード MIB のサポート	9.7(1)	E2E トランスペアレント クロック モードに対応する MIB がサポートされます。 （注） SNMP の bulkget、getnext、walk 機能のみがサポートされています。

機能名	プラットフォーム リリース	説明
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更された画面：**[Configuration]** > **[Device Management]** > **[Management Access]** > **[SNMP]**