



概要

SNMPバージョン3では、User-based Security Model (USM; ユーザーベースセキュリティモデル) および View-based Access Control Model (VACM; ビューベースアクセスコントロールモデル) による認証オプションやプライバシー オプションを使用することにより、SNMP エージェントによる SNMP トランザクションのセキュアな通信が実現されます。SNMPバージョン1 および SNMPバージョン2c では、MIB のアクセス コントロールを行う場合ユーザは認識されないため、暗号化されたプライバシー オプションを使用して認証を行うことはできません。VACM のサポートは、次リリース以降に先送りされました。

この章では、ASA ソフトウェアバージョン 8.2(1) 以降が稼働しているデバイス上で、SNMPバージョン3 を介して ASA と通信可能な CiscoWorks およびいくつかのサードパーティ製ツールをインストールする方法、設定する方法、および使用する方法について説明します。

この章は、次の項目を取り上げます。

- [ネットワーク管理ツール\(1-1 ページ\)](#)
- [ネットワーク トポロジ\(1-2 ページ\)](#)
- [ASA 設定\(1-2 ページ\)](#)

ネットワーク管理ツール

このマニュアルでは、次のネットワーク管理ツールについて説明します。

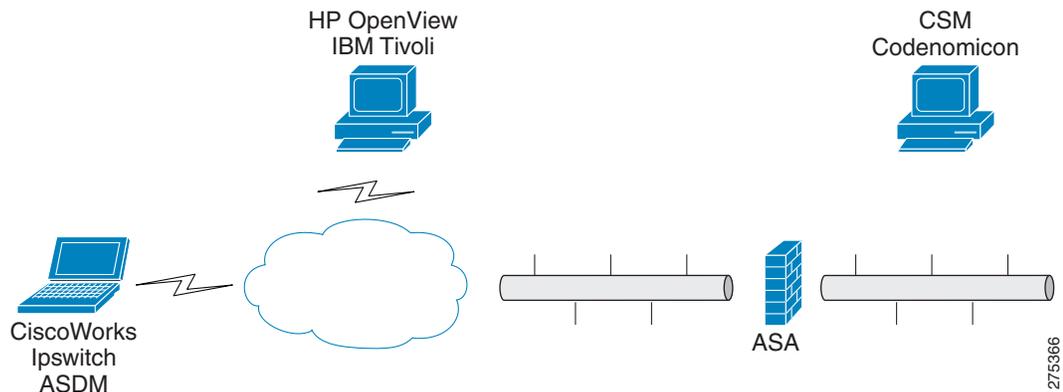
- Net-SNMP (CLI アプリケーション)
- IWL SilverCreek (SNMP テストスイート)
- Ipswitch WhatsUp Gold
- HP OpenView NNM
- CiscoWorks for Windows LMS

シスコでは、これらのツールに対して、NMS および ASA との間の相互運用性試験をすでに実施しています。

ネットワーク トポロジ

図 1-1 は、SNMP バージョン 3 を実装するためのネットワーク トポロジを示したものです。

図 1-1 SNMP バージョン 3 を実装するためのネットワーク トポロジ



ASA 設定

ASA を使用するためには、SNMP サーバグループ、そのグループに関連付けられた SNMP サーバユーザ、および SNMP トラップの受信ユーザを指定するための SNMP サーバホストを設定する必要があります。

SNMP バージョン 3 の動作を設定する際に必要となるコマンドは次のとおりです。

- **snmp-server group**
- **snmp-server user**
- **snmp-server host**

ASA の構成例を以下に示します。

```

ciscoasa# snmp-server group authPriv v3 priv
ciscoasa# snmp-server group authNoPriv v3 auth
ciscoasa# snmp-server group noAuthNoPriv v3 noauth

ciscoasa# snmp-server user md5des authPriv v3 auth md5 mysecretpass priv des passphrase
ciscoasa# snmp-server user md5user authNoPriv v3 auth md5 mysecretpass
ciscoasa# snmp-server user noauthuser noAuthNoPriv v3

ciscoasa# snmp-server host mgmt 10.0.0.1 version 3 md5des
ciscoasa# snmp-server host mgmt 10.0.0.2 version 3 md5des
ciscoasa# snmp-server host mgmt 10.0.0.3 version 3 md5des

ciscoasa# snmp-server location Anywhere, USA
ciscoasa# snmp-server contact admin@example.com
ciscoasa# snmp-server enable traps snmp authentication linkup linkdown coldstart
ciscoasa# snmp-server enable traps syslog
ciscoasa# snmp-server enable traps ipsec start stop
ciscoasa# snmp-server enable traps entity config-change fru-insert fru-remove
ciscoasa# snmp-server enable traps remote-access session-threshold-exceeded

```