RV160およびRV260ルータでのSNMPの設定

目的

この記事の目的は、RV160およびRV260ルータでSimple Network Management Protocol(SNMP)を設定する方法を示すことです。

概要

SNMPは、IPネットワーク上の管理対象デバイスのデータを収集および整理するためのイン ターネット標準プロトコルです。ネットワーク管理者は、ネットワーク上で発生した重要な イベントの通知を管理、監視、受信し、トラブルシューティングすることができます。

SNMPフレームワークは、次の3つの要素で構成されています。SNMPマネージャ、 SNMPエージェント、および管理情報ベース(MIB)。 SNMPマネージャの機能は、SNMPを 使用するネットワークホストのアクティビティを制御および監視することです。SNMPエー ジェントはデバイスのソフトウェア内にあり、システムを管理するためにデータのメンテナ ンスを支援します。最後に、MIBはネットワーク管理情報の仮想ストレージエリアです。こ れら3つを組み合わせて、ネットワーク内のデバイスを監視および管理します。

RV160/260デバイスは、SNMPバージョンv1、v2c、およびv3をサポートしています。これ らは、SNMPネットワーク管理システムからのSNMPコマンドに応答するSNMPエージェン トとして機能します。サポートされているコマンドは、標準のSNMPコマンドget/next/setで す。また、デバイスは、アラーム状態が発生したときにSNMPマネージャに通知するトラッ プメッセージを生成します。たとえば、リブート、電源サイクル、WANリンクイベントな どがあります。

該当するデバイス

- RV160
- RV260

[Software Version]

• 1.0.00.13

SNMPの設定

ルータのSNMPを設定するには、次の手順を実行します。

ステップ1:ルータのWeb設定ページにログインします。

cisco
Router
cisco 1
English -
Login
©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademar of Cisco Systems, Inc. and/or its affiliates in the United States and certain other

注:この記事では、RV260Wを使用してSNMPを設定します。設定は、使用しているモデル によって異なります。

ステップ2:[System Configuration] > [SNMP]に移動します。

System Configuration
Initial Router Setup 1
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP (2)

ステップ3:SNMPを有効にするには、[SNMP Enable]チェックボックスをオンにします。



ステップ4:(オプション)[Allow user access from Internet]チェックボックスをオンにして、Cisco FindIT Network Managementなどの管理アプリケーションを使用して、許可されたユーザがネットワークの外部にアクセスできるようにします。

SNMP	
SNMP Enable:	
Allow user access from Internet:	

ステップ5:(オプション)[Allow user access from VPN]チェックボックスをオン**にし**て、バ ーチャルプライベートネットワーク(VPN)からの許可されたアクセスを許可します。

SNMP

SNMP Enable:	
Allow user access from Internet:	

Allow user access from VPN:

ステップ6:[Version] ドロップダウンメニューから、ネットワークで使用するSNMPバージョ ンを選択します。次のオプションがあります。

- v1:最もセキュアでないオプション。コミュニティストリングにプレーンテキストを使用します。
- v2c:SNMPv2cでサポートされる改善されたエラー処理には、さまざまなタイプのエラ ーを区別する拡張エラーコードが含まれます。すべてのタイプのエラーは、SNMPv1の 単一のエラーコードで報告されます。
- v3:SNMPv3は、ネットワーク上のデータパケットを認証および暗号化することによって、デバイスへのセキュアなアクセスを提供します。認証アルゴリズムには、メッセージダイジェストアルゴリズム(MD5)およびセキュアハッシュアルゴリズム(SHA)が含まれます。暗号化方式には、Data Encryption Standard (DES;データ暗号規格)や Advanced Encryption Standard (AES;高度暗号化規格)などがあります。

SNMPv3の詳細については、ここをクリックし<u>てください</u>。

SNMP	
SNMP Enable:	
Allow user access from Internet:	
Allow user access from VPN:	
Version:	v2c ~

この例では、v2cがバージョンとして選択されました。

ステップ7:次のフィールドを入力します

- System Name:ネットワーク管理アプリケーションで識別しやすいように、ルータの 名前を入力します。
- ・システム接続:緊急時にルータと識別する個人または管理者の名前を入力します。
- System Location: ルータの場所を入力します。これにより、管理者は問題を簡単に見つけることができます。
- Get Community:[Get Community]フィールドにSNMPコミュニティ名を入力します。
 SNMPエージェントの情報にアクセスして取得するために使用される読み取り専用コミュニティが作成されます。
- Set Community:[Set Community]フィールドに、SNMPコミュニティ名を入力します。 SNMPエージェントの情報へのアクセスと変更に使用される読み取り/書き込みコミュニ ティを作成します。このコミュニティ名で自身を識別するデバイスからの要求のみが受 け入れられます。これはユーザが作成した名前です。デフォルトはprivateです。

System Name:	RV260W	1
System Contact:	Admin	2
System Location:	San Jose	3
Get Community:	cisco	4

トラップの設定

トラップ設定を使用すると、発信インターフェイスに関係なく、ルータから送信されるすべてのSNMPトラップパケットの送信元アドレスを1つのアドレスに設定できます。

ステップ8:SNMPトラップを設定するには、次の情報を入力します。

trap comm	unity		
IP		IP	
Trap Configuration			
Trap Community:	Cisco	0	
Trap Receiver IP Address:	192.168.1.40	2	
Trap Receiver Port:	162	3	

注:通常、SNMPはトランスポートプロトコルとしてユーザデータグラムプロトコル (UDP)を使用し、SNMPトラフィックのデフォルトUDPポートは161(SNMP)および 162(SNMPトラップ)です。

ステップ9:[Apply]をクリ**ックします**。

SNMP								Apply	
SNMP Enable:		3							
Allow user access	from Internet	J							
Allow user access	from VPN:	D							
Version:		v2c ~							
System Name:	RV260W								
System Contact:	Admin								
System Location:	San Jose								
Get Community:	cisco								
Set Community:	private								
Trap Configura	ation								
Trap Community:	Cisc)							
Trap Receiver IP Ad	idress: 192.	168.1.40							
Trap Receiver Port:	162								

これで、RV160/RV260ルータでSNMPが正常にイネーブルおよび設定されたはずです。