

RV34xシリーズルータでのSimple Network Management Protocol(SNMP)の設定

目的

Simple Network Management Protocol(SNMP)は、ネットワーク管理、トラブルシューティング、およびメンテナンスに使用されます。SNMPは、次の2つの主要ソフトウェアを使用して情報を記録、保存、および共有します。マネージャデバイス上で実行されるネットワーク管理システム(NMS)、および管理対象デバイス上で実行されるエージェント。RV34xシリーズルータは、SNMPバージョン1、2、および3をサポートしています。

SNMP v1は、特定の機能を持たず、TCP/IPネットワークでのみ動作するSNMPのオリジナルバージョンです。一方、SNMP v2はv1の改良版です。SNMP v1とv2cは、SNMPv1またはSNMPv2cを使用するネットワークでのみ選択してください。SNMP v3はSNMPの最新の標準であり、SNMP v1およびv2cの問題の多くに対処します。特に、v1およびv2cのセキュリティ脆弱性の多くに対処します。SNMP v3では、管理者は1つの共通のSNMP標準に移行することもできます。

この記事では、RV34xシリーズルータでSNMPを設定する方法について説明します。

該当するデバイス

- RV34xシリーズ

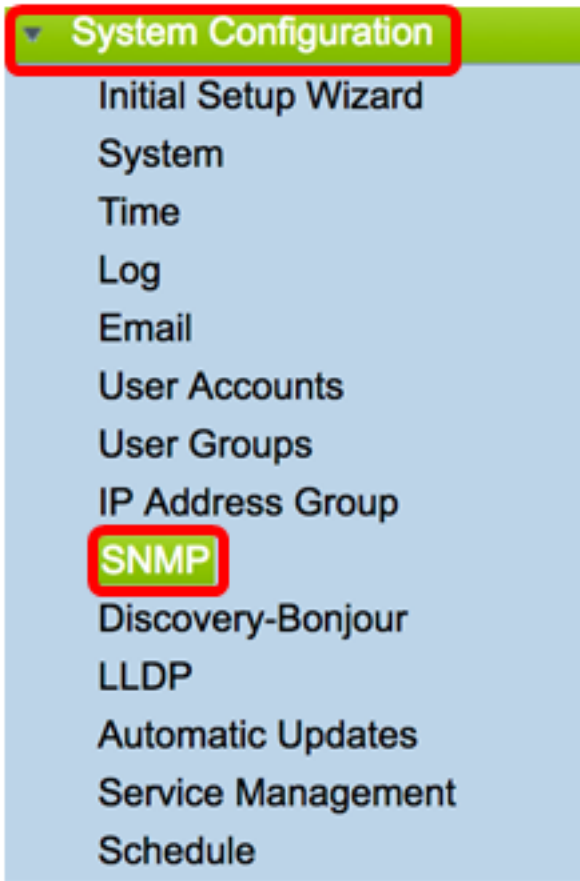
[Software Version]

- 1.0.1.16

RV34xシリーズルータのSNMP設定

SNMPの設定

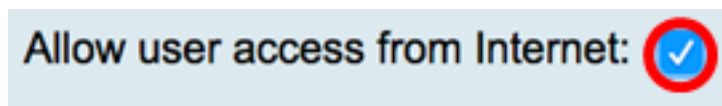
ステップ1：ルータのWebベースのユーティリティにログインし、[System Configuration] > [SNMP]を選択します。



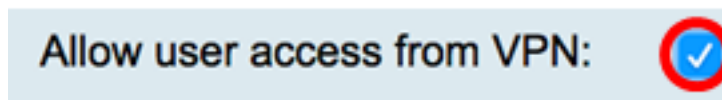
ステップ2:SNMPを有効にするには、[SNMP Enable]チェックボックスをオンにします。



ステップ3: (オプション) [Enable 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外にアクセスできるようにします。



ステップ4: (オプション) VPNからの許可されたアクセスを許可するには、[Allow user access from VPN]チェックボックスをオンにします。

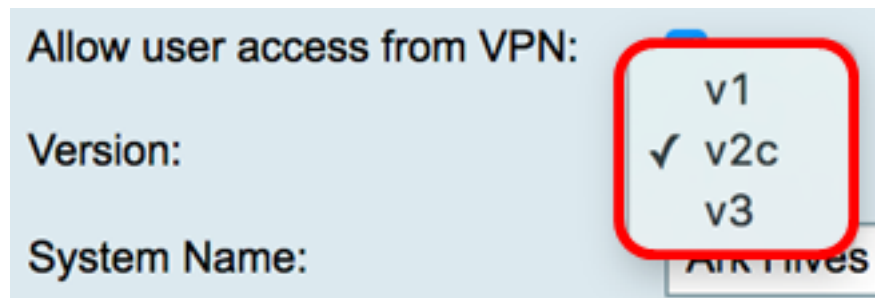


ステップ5:[Version]ドロップダウンメニューから、ネットワークで使用するSNMPバージョンを選択します。次のオプションがあります。

- v1 : 最もセキュリティが低いオプション。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によって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、ユーザとユーザが存在するグループに対して認証戦略を設定するセキュリティ

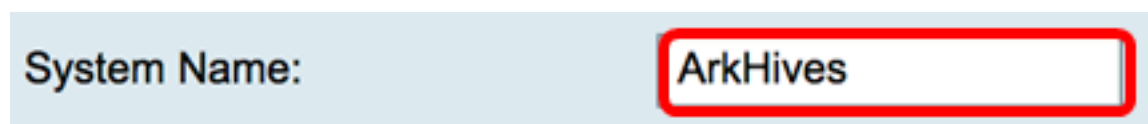
イモデルです。セキュリティレベルは、セキュリティモデル内で許可されるセキュリティレベルです。セキュリティモデルとセキュリティレベルの組み合わせによって、SNMPパケットを処理するときに使用されるセキュリティメカニズムが決まります。

注：この例では、v2cが選択されています。



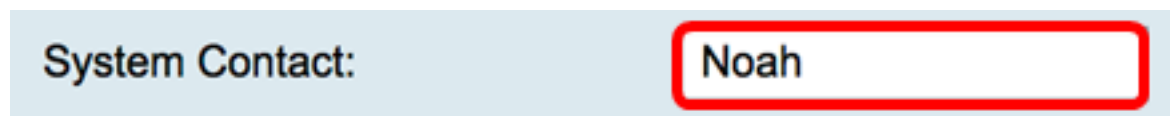
ステップ6:[System Name]フィールドに、ネットワーク管理アプリケーションで識別しやすいようにルータの名前を入力します。

注：この例では、システム名としてArkHivesが使用されています。



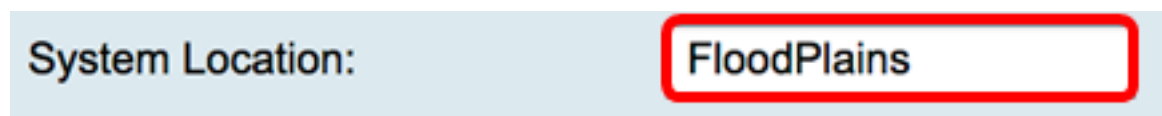
ステップ7:[System Contact]フィールドに、緊急時にルータと識別する個人または管理者の名前を入力します。

注：この例では、システム接点としてNoahが使用されます。



ステップ8:[System Location]フィールドに、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。

注：この例では、FloodPlainsがシステムロケーションとして使用されます。



設定を続行するには、ステップ5で選択したSNMPバージョンをクリックします。

- [SNMP 1またはv2cの設定](#)
- [SNMP v3の設定](#)

[SNMP 1またはv2cの設定](#)

ステップ1：ステップ5でSNMP v2cを選択した場合は、[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へのアクセス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。送信者が送信した要求パケットで送信されるコミュニティストリングは、エージェントデバイスのコミュニティストリングと一致する必要があります。読み取り専用のデフォルト文字列はpublicです。

注：読み取り専用パスワードは、情報を取得する権限だけを与えます。この例では、pblickが使用されています。

Get Community:

pblick

ステップ2:[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に使用される読み取り/書き込みコミュニティが作成されます。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。

注：外部からのセキュリティ攻撃を避けるために、両方のパスワードをよりカスタマイズされたものに変更することを推奨します。この例では、pribadoを使用します。

Set Community:

pribado

これで、SNMP v1またはv2の設定が正常に設定されました。「トラップの設定」[領域に進みます](#)。

SNMP v3の設定

ステップ1:SNMP v3が選択されている場合は、[Username]領域のオプションボタンをクリックしてアクセス権限を選択します。次のオプションがあります。

- guest：読み取り専用権限
- admin：読み取り/書き込み権限

注：この例では、guestが選択されています。

[Access Privilege]領域には、クリックしたオプションボタンに応じて特権のタイプが表示されます。

Username:

guest admin

Access Privilege:

Read

ステップ2:[Authentication Algorithm]領域のオプションボタンをクリックして、SNMPエージェントが認証に使用する方法を選択します。次のオプションがあります。

- None：ユーザ認証は使用されません。
- MD5:Message-Digest Algorithm 5では、認証に128ビットのハッシュ値を使用します。ユーザ名とパスワードが必要です。
- SHA1：セキュアハッシュアルゴリズム(SHA-1)は、160ビットのダイジェストを生成する一方方向ハッシュアルゴリズムです。SHA-1はMD5よりも低速を計算しますが、MD5よりも安全です。

注：この例では、MD5が選択されています。

Authentication Algorithm: None MD5 SHA1

Authentication Password:

注：[なし]を選択した場合は、[トラップの設定]領域にスキップします。

ステップ3:[Authentication Password]フィールドにパスワードを入力します。

Authentication Algorithm: None MD5 SHA1

Authentication Password:

ステップ4: (オプション) [Encryption Algorithm (暗号化アルゴリズム)]領域で、オプションボタンをクリックして、SNMP情報の暗号化方法を選択します。次のオプションがあります。

- None：暗号化は使用されません。この手順を選択した場合は、[トラップの設定]領域に移動します。
- DES:Data Encryption Standard (DES ; データ暗号規格) は56ビットの暗号化方式で、安全性は低いものの、後方互換性のために必要になる場合があります。
- AES：高度暗号化規格(AES)。これを選択した場合、暗号化パスワードが必要です。

注：この例では、DESが選択されています。

Encryption Algorithm: None DES AES

Encryption Password:

ステップ5: (オプション) DESまたはAESを選択した場合は、[Encryption Password]フィールドに暗号化パスワードを入力します。

Encryption Algorithm: None DES AES

Encryption Password:

これで、SNMP v3の設定が正常に完了したはずですが、ここで、[トラップの設定]領域に進みます。

トラップの設定

ステップ1:[Trap Receiver IP Address] フィールドに、SNMPトラップを受信するIPv4またはIPv6 IPアドレスを入力します。

注：この例では、192.168.2.202が使用されています。

Trap Configuration

Trap Receiver IP Address

(Hint: 1.2.3.4 or fc02::0)

ステップ2:[Trap Receiver Port]フィールドにユーザデータグラムプロトコル(UDP)ポート番号を入力します。SNMPエージェントは、このポートでアクセス要求をチェックします。

注：この例では、161が使用されています。

Trap Receiver Port

ステップ3:[Apply]をクリックします。

Trap Configuration

Trap Receiver IP Address

Trap Receiver Port

SNMP



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

SNMP Enable:	<input checked="" type="checkbox"/>
Allow user access from Internet:	<input checked="" type="checkbox"/>
Allow user access from VPN:	<input checked="" type="checkbox"/>
Version:	v3
System Name:	Ark Hives
System Contact:	Noah
System Location:	FloodPlains
Username:	<input checked="" type="radio"/> guest <input type="radio"/> admin
Access Privilege:	Read
Authentication Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA1
Authentication Password:
Encryption Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> DES <input type="radio"/> AES
Encryption Password:

Trap Configuration

Trap Receiver IP Address	192.168.2.100	(Hint: 1.2.3.4 or fc02::0)
Trap Receiver Port	161	

Apply

Cancel

ステップ4: (オプション) 構成を永続的に保存するには、[構成のコピー/保存(Copy/Save Configuration)]ページに移動するか、ページの上にあるアイコンをクリックします。

 Save

これで、RV34xシリーズルータでSNMP設定が正常に行われたはずです。