

Configurar o Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) em um roteador RV34x Series

Objetivo

O SNMP (Simple Network Management Protocol) é usado para gerenciamento de rede, solução de problemas e manutenção. O SNMP grava, armazena e compartilha informações com a ajuda de dois softwares principais: um sistema de gerenciamento de rede (NMS) que é executado em dispositivos gerenciadores e em um agente que é executado em dispositivos gerenciados. O RV34x Series Router suporta SNMP versões 1, 2 e 3.

O SNMP v1 é a versão original do SNMP que não tem certas funcionalidades e só funciona em redes TCP/IP, enquanto o SNMP v2 é uma iteração melhorada de v1. SNMP v1 e v2c devem ser escolhidos somente para redes que utilizam SNMPv1 ou SNMPv2c. O SNMP v3 é o mais novo padrão de SNMP e aborda muitos dos problemas de SNMP v1 e v2c. Em particular, ele lida com muitas das vulnerabilidades de segurança de v1 e v2c. O SNMP v3 também permite que os administradores mudem para um padrão SNMP comum.

Este artigo explica como configurar as configurações SNMP no RV34x Series Router.

Dispositivos aplicáveis

- Série RV34x

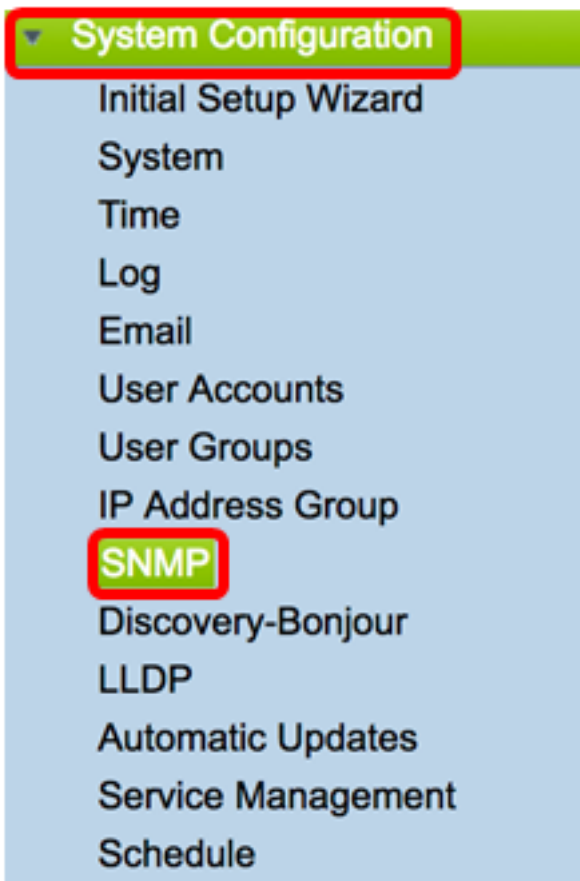
Versão de software

- 1.0.1.16

Configurar as configurações SNMP no roteador RV34x Series

Definir configurações SNMP

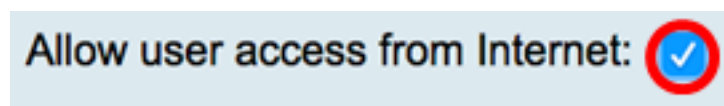
Etapa 1. Faça login no utilitário baseado na Web do roteador e escolha **Configuração do sistema > SNMP**.



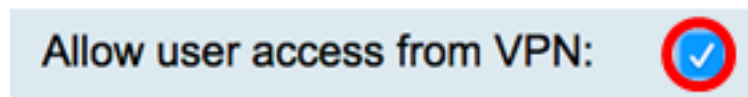
Etapa 2. Marque a caixa de seleção **SNMP Enable** para ativar o SNMP.



Etapa 3. (Opcional) Marque a caixa de seleção **Enable Allow user access from Internet** para permitir o acesso autorizado do usuário fora da rede por meio de aplicativos de gerenciamento, como o Cisco FindIT Network Management.



Etapa 4. (Opcional) Marque a caixa de seleção **Permitir acesso de usuário da VPN** para permitir acesso autorizado de uma VPN.

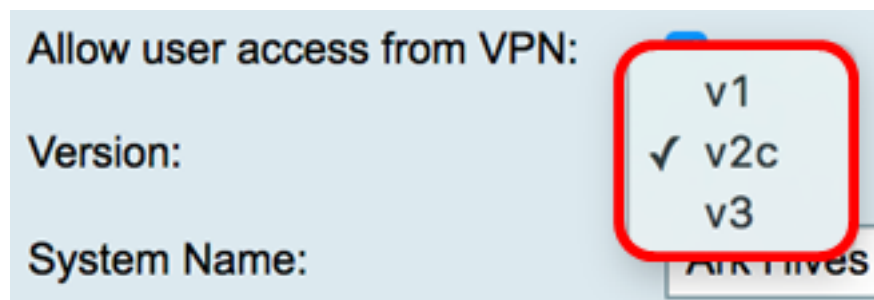


Etapa 5. No menu suspenso **Version (Versão)**, escolha uma versão SNMP para usar na rede. As opções são:

- v1 — opção menos segura. Usa texto simples para community strings.
- v2c — o melhor suporte para tratamento de erros fornecido pelo SNMPv2c inclui códigos de erro expandidos que distinguem diferentes tipos de erros; todos os tipos de erros são relatados por meio de um único código de erro em SNMPv1.
- v3 — SNMPv3 é um modelo de segurança no qual uma estratégia de autenticação é configurada para um usuário e o grupo no qual o usuário reside. O nível de segurança é o

nível de segurança permitido em um modelo de segurança. Uma combinação de um modelo de segurança e um nível de segurança determina qual mecanismo de segurança é usado ao tratar um pacote SNMP.

Note: Neste exemplo, v2c é escolhido.



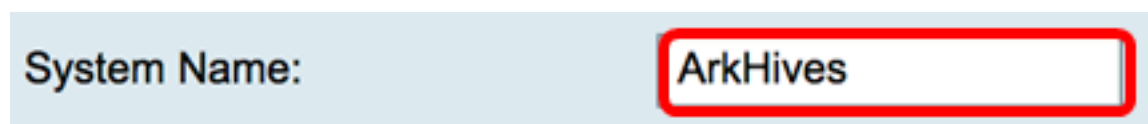
Allow user access from VPN:

Version: v1
✓ v2c
v3

System Name: ArkHives

Etapa 6. No campo *System Name*, insira um nome para o roteador para facilitar a identificação em aplicativos de gerenciamento de rede.

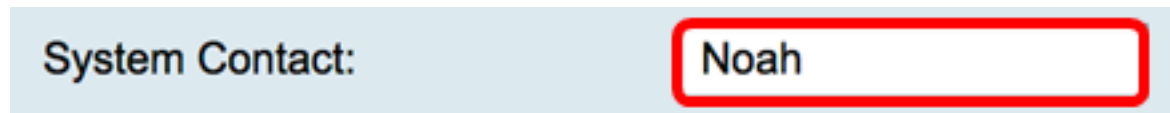
Note: Neste exemplo, ArkHives é usado como o Nome do sistema.



System Name: ArkHives

Passo 7. No campo *System Contact*, insira um nome de um indivíduo ou administrador para se identificar com o roteador em caso de emergência.

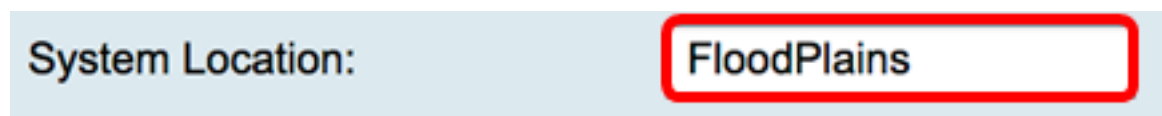
Note: Para este exemplo, Noah é usado como o Contato do sistema.



System Contact: Noah

Etapa 8. No campo *System Location*, insira um local do roteador. Isso torna a localização de um problema muito mais fácil para um administrador.

Note: Para este exemplo, FloodPlains é usado como a Localização do sistema.



System Location: FloodPlains

Para prosseguir com a configuração, clique na versão SNMP escolhida na Etapa 5.

- [Configurar SNMP 1 ou v2c](#)
- [Configurar SNMP v3](#)

[Configurar SNMP 1 ou v2c](#)

Etapa 1. Se o SNMP v2c foi escolhido na Etapa 5, insira o nome da comunidade SNMP no campo *Get Community*. Cria uma comunidade somente leitura que é usada para acessar as informações do agente SNMP. A string de comunidade enviada no pacote de solicitação enviado pelo remetente deve corresponder à string de comunidade no dispositivo do agente. A string padrão para somente leitura é pública.

Note: A senha somente leitura dá autoridade para recuperar somente informações. Neste exemplo, é usado o pblick.

Get Community:

pblick

Etapa 2. No campo *Set Community*, insira um nome de comunidade SNMP. Ele cria uma comunidade de leitura e gravação que é usada para acessar as informações do agente SNMP. Somente as solicitações dos dispositivos que se identificam com esse nome de comunidade são aceitas. Este é um nome criado pelo usuário. O padrão é privado.

Note: É aconselhável alterar ambas as senhas para algo mais personalizado para evitar ataques à segurança de terceiros. Nesse exemplo, é usado o privado.

Set Community:

privado

Agora você deve ter configurado com êxito as configurações de SNMP v1 ou v2. Vá para a área [Configuração de interceptação](#).

Configurar SNMP v3

Etapa 1. Se o SNMP v3 tiver sido escolhido, clique em um botão de opção na área Nome de usuário para escolher um privilégio de acesso. As opções são:

- convidado — Privilégios somente leitura
- admin — privilégios de leitura e gravação

Note: Para este exemplo, o convidado é escolhido.

A área Privilégio de acesso mostra o tipo de privilégio dependendo do botão de opção clicado.

Username:

guest admin

Access Privilege:

Read

Etapa 2. Clique em um botão de opção na área Authentication Algorithm para escolher um método que o agente SNMP usará para autenticar. As opções são:

- Nenhum — Nenhuma autenticação de usuário é usada.
- MD5 — O Message-Digest Algorithm 5 usa um valor de hash de 128 bits para a autenticação. Requer nome de usuário e senha.
- SHA1 — O Secure Hash Algorithm (SHA-1) é um algoritmo de hash unidirecional que produz um resumo de 160 bits. O SHA-1 computa mais lentamente que o MD5, mas é mais seguro que o MD5.

Note: Para este exemplo, MD5 é escolhido.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Note: Se você escolheu Nenhum, pule para a área [Configuração de interceptação](#).

Etapa 3. No campo *Authentication Password*, digite uma senha.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Etapa 4. (Opcional) Na área Encryption Algorithm (Algoritmo de criptografia), clique em um botão de opção para escolher como as informações de SNMP serão criptografadas. As opções são:

- Nenhum — Nenhuma criptografia é usada. Se esta etapa for escolhida, vá para a área [Configuração de interceptação](#).
- DES — Data Encryption Standard (DES) é um método de criptografia de 56 bits que não é muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.
- AES — Advanced Encryption Standard (AES). Se esta opção for escolhida, será necessária uma senha de criptografia.

Note: Para este exemplo, DES é escolhido.

Encryption Algorithm: None DES AES

Encryption Password:

Etapa 5. (Opcional) Se DES ou AES tiver sido escolhido, insira uma senha de criptografia no campo *Senha de criptografia*.

Encryption Algorithm: None DES AES

Encryption Password:

Agora você deve ter configurado com êxito as configurações de SNMP v3. Prossiga agora para a área [Configuração de interceptação](#).

[Configuração de armadilha](#)

Etapa 1. No campo *Trap Receiver IP Address*, insira um endereço IPv4 ou IPv6 que receberá as interceptações SNMP.

Note: Para este exemplo, 192.168.2.202 é usado.

Trap Configuration

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

Etapa 2. Insira um número de porta UDP (User Datagram Protocol) no campo *Trap Receiver Port* (*Porta do receptor de interceptação*). O agente SNMP verifica se há solicitações de acesso nesta porta.

Note: Para este exemplo, 161 é usado.

Trap Receiver Port

Etapa 3. Clique em Apply.

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

Etapa 4. (Opcional) Para salvar a configuração permanentemente, vá para a página

Copiar/Salvar configuração ou clique no  ícone na parte superior da página.

Agora você deve ter configurado com êxito as configurações de SNMP em um RV34x Series Router.