

Configuración de los parámetros del protocolo simple de administración de red (SNMP) en un router serie RV34x

Objetivo

El protocolo simple de administración de red (SNMP) se utiliza para la gestión de redes, la resolución de problemas y el mantenimiento. SNMP registra, almacena y comparte información con la ayuda de dos software clave: un sistema de administración de redes (NMS) que se ejecuta en dispositivos de administrador y un agente que se ejecuta en dispositivos administrados. El router serie RV34x admite las versiones 1, 2 y 3 de SNMP.

SNMP v1 es la versión original de SNMP que carece de cierta funcionalidad y sólo funciona en redes TCP/IP, mientras que SNMP v2 es una iteración mejorada de v1. SNMP v1 y v2c sólo deben elegirse para redes que utilizan SNMPv1 o SNMPv2c. SNMP v3 es el estándar más reciente de SNMP y aborda muchos de los problemas de SNMP v1 y v2c. En particular, aborda muchas de las vulnerabilidades de seguridad de v1 y v2c. SNMP v3 también permite a los administradores pasar a un estándar SNMP común.

En este artículo se explica cómo configurar los parámetros SNMP en el router serie RV34x.

Dispositivos aplicables

- Serie RV34x

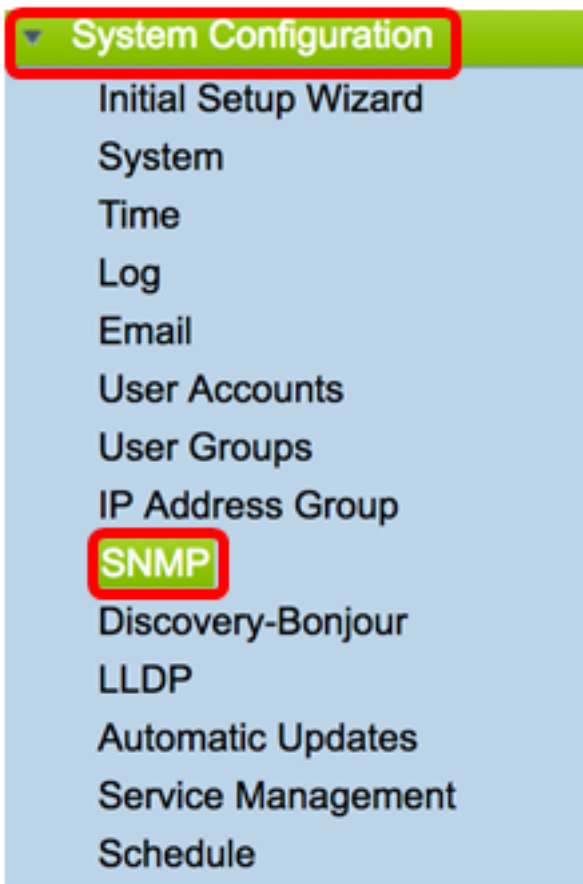
Versión del software

- 1.0.1.16

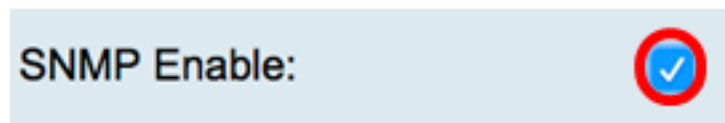
Configuración de los parámetros SNMP en el router serie RV34x

Configuración de los parámetros de SNMP

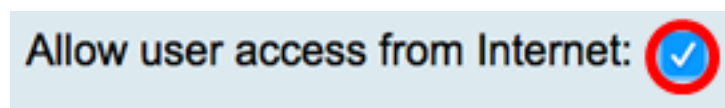
Paso 1. Inicie sesión en la utilidad basada en web del router y elija **Configuración del sistema > SNMP**.



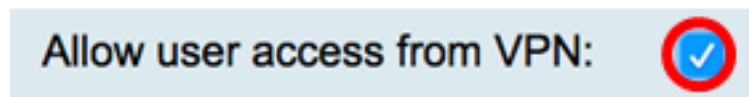
Paso 2. Marque la casilla de verificación **SNMP Enable** para habilitar SNMP.



Paso 3. (Opcional) Marque la casilla de verificación **Enable User Access from Internet** para permitir el acceso de usuarios autorizados fuera de la red a través de aplicaciones de administración como Cisco FindIT Network Management.



Paso 4. (Opcional) Marque la casilla de verificación **Allow user access from VPN** para permitir el acceso autorizado desde una VPN.

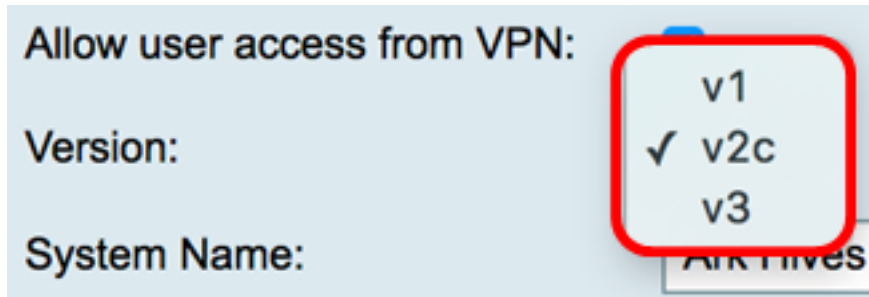


Paso 5. En el menú desplegable Versión, elija una versión SNMP para utilizar en la red. Las opciones son:

- v1: opción menos segura. Utiliza texto sin formato para cadenas de comunidad.
- v2c: el soporte mejorado de manejo de errores proporcionado por SNMPv2c incluye códigos de error expandidos que distinguen diferentes tipos de errores; todos los tipos de errores se informan a través de un solo código de error en SNMPv1.
- v3: SNMPv3 es un modelo de seguridad en el que se configura una estrategia de autenticación para un usuario y el grupo en el que reside el usuario. El nivel de seguridad es

el nivel de seguridad permitido dentro de un modelo de seguridad. Una combinación de un modelo de seguridad y un nivel de seguridad determina qué mecanismo de seguridad se utiliza al gestionar un paquete SNMP.

Nota: En este ejemplo, se elige v2c.



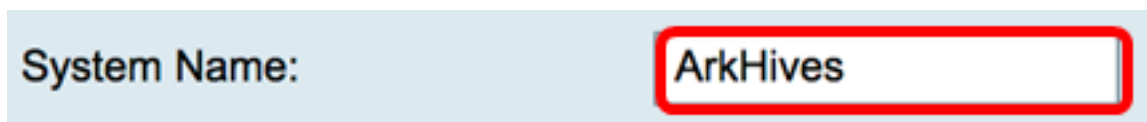
Allow user access from VPN:

Version: v1
✓ v2c
v3

System Name: ArkHives

Paso 6. En el campo *Nombre del sistema*, introduzca un nombre para el router para facilitar la identificación en las aplicaciones de administración de red.

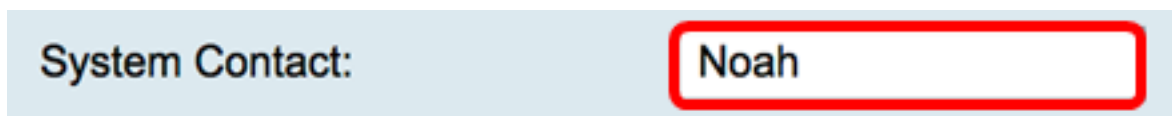
Nota: En este ejemplo, ArkHives se utiliza como Nombre del sistema.



System Name: ArkHives

Paso 7. En el campo *Contacto del sistema*, ingrese un nombre de una persona o administrador para identificarlo con el router en caso de emergencia.

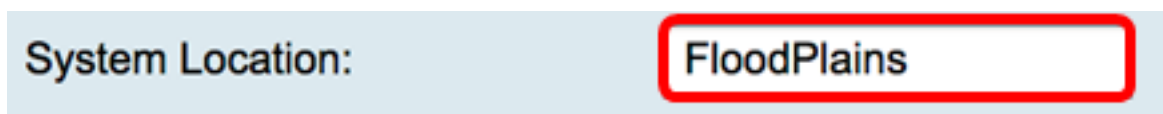
Nota: Para este ejemplo, Noah se utiliza como contacto del sistema.



System Contact: Noah

Paso 8. En el campo *System Location*, ingrese una ubicación del router. Esto facilita la localización de un problema para un administrador.

Nota: Para este ejemplo, FloodPlains se utiliza como ubicación del sistema.



System Location: FloodPlains

Para continuar con la configuración, haga clic en la versión SNMP elegida en el Paso 5.

- [Configuración de SNMP 1 o v2c](#)
- [Configuración de SNMP v3](#)

[Configuración de SNMP 1 o v2c](#)

Paso 1. Si se eligió SNMP v2c en el Paso 5, ingrese el nombre de la comunidad SNMP en el campo *Get Community*. Crea una comunidad de sólo lectura que se utiliza para acceder a la información del agente SNMP. La cadena de comunidad enviada en el paquete de solicitud enviado por el remitente debe coincidir con la cadena de comunidad en el dispositivo agente. La cadena predeterminada para sólo lectura es pública.

Nota: La contraseña de sólo lectura otorga autoridad para recuperar sólo información. En este ejemplo, se utiliza pblick.

Get Community:

Paso 2. En el campo *Establecer comunidad*, ingrese un nombre de comunidad SNMP. Crea una comunidad de lectura y escritura que se utiliza para acceder a la información del agente SNMP. Solo se aceptan las solicitudes de los dispositivos que se identifican con este nombre de comunidad. Este es un nombre creado por el usuario. El valor predeterminado es private (privado).

Nota: Se recomienda cambiar ambas contraseñas por algo más personalizado para evitar ataques de seguridad de los foráneos. En este ejemplo, se utiliza el privado.

Set Community:

Ahora debería haber configurado correctamente los parámetros SNMP v1 o v2. Vaya al área [Configuración de trampa](#).

Configuración de SNMP v3

Paso 1. Si se seleccionó SNMP v3, haga clic en un botón de opción en el área Nombre de usuario para elegir un privilegio de acceso. Las opciones son:

- invitado: privilegios de sólo lectura
- admin: privilegios de lectura y escritura

Nota: Para este ejemplo, se elige invitado.

El área Privilegio de acceso muestra el tipo de privilegio en función del botón de opción que se haya hecho clic.

Username: guest admin
Access Privilege: Read

Paso 2. Haga clic en un botón de opción del área Algoritmo de autenticación para elegir un método que el agente SNMP utilizará para autenticar. Las opciones son:

- Ninguno: no se utiliza autenticación de usuario.
- MD5: el algoritmo Message-Digest 5 utiliza un valor hash de 128 bits para la autenticación. Requiere nombre de usuario y contraseña.
- SHA1: el algoritmo hash seguro (SHA-1) es un algoritmo de hash unidireccional que produce un resumen de 160 bits. SHA-1 se calcula más lentamente que MD5, pero es más seguro que MD5.

Nota: Para este ejemplo, se elige MD5.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Nota: Si ha seleccionado Ninguno, vaya al área [Configuración de trampa](#).

Paso 3. En el campo *Authentication Password*, ingrese una contraseña.

Authentication Algorithm: None MD5 SHA1

Authentication Password:

Paso 4. (Opcional) En el área Algoritmo de cifrado, haga clic en un botón de opción para elegir cómo se cifrará la información SNMP. Las opciones son:

- Ninguno: no se utiliza ninguna encriptación. Si se elige este paso, vaya directamente al área [Configuración de trampa](#).
- DES: el estándar de cifrado de datos (DES) es un método de encriptación de 56 bits que no es muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.
- AES: estándar de cifrado avanzado (AES). Si se selecciona esta opción, se requiere una contraseña de cifrado.

Nota: Para este ejemplo, se elige DES.

Encryption Algorithm: None DES AES

Encryption Password:

Paso 5. (Opcional) Si se eligió DES o AES, introduzca una contraseña de cifrado en el campo *Encryption Password* (Contraseña de cifrado).

Encryption Algorithm: None DES AES

Encryption Password:

Ahora debería haber configurado correctamente los parámetros de SNMP v3. Proceda ahora al área [Configuración de trampa](#).

[Configuración de trampa](#)

Paso 1. En el campo *Trap Receiver IP Address*, ingrese una dirección IPv4 o IPv6 que recibirá las trampas SNMP.

Nota: Para este ejemplo, se utiliza 192.168.2.202.

Trap Configuration

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

Paso 2. Introduzca un número de puerto de protocolo de datagramas de usuario (UDP) en el campo *Puerto del receptor de capturas*. El agente SNMP verifica este puerto en busca de solicitudes de acceso.

Nota: Para este ejemplo, se utiliza 161.

Trap Receiver Port

Paso 3. Haga clic en Apply (Aplicar).

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

Paso 4. (Opcional) Para guardar la configuración de forma permanente, vaya a la página Copiar/Guardar configuración o haga clic en el  Save icono situado en la parte superior de la página.

Ahora debería haber configurado correctamente los parámetros SNMP en un router serie RV34x.