

# Configurazione SNMP sul router VPN RV315W

## Obiettivo

Il protocollo SNMP (Simple Network Management Protocol) è un protocollo TCP/IP per la gestione della rete. L'SNMP consente agli amministratori di monitorare le prestazioni e le percentuali di errore della rete. L'SNMP può anche mappare la disponibilità della rete. Il quadro SNMP è costituito da tre elementi: un manager SNMP, un agente SNMP e un MIB. La funzione di SNMP Manager è quella di controllare e monitorare le attività degli host di rete che utilizzano SNMP. L'agente SNMP è incluso nel software del dispositivo e contribuisce alla manutenzione dei dati per consentire la gestione del sistema. Infine, il MIB (Management Information Base) è un'area di storage virtuale per le informazioni di gestione della rete. Questi tre dispositivi si combinano per monitorare e gestire i dispositivi in una rete.

Questo articolo spiega come configurare il protocollo SNMP sul router VPN RV315W.

## Dispositivo applicabile

RV315W

## Versione del software

•1.01.03

## Configurazione di SNMP

SNMP v1 è la versione originale di SNMP, che non dispone di alcune funzionalità e funziona solo su reti TCP/IP, SNMP v2 è un'iterazione migliorata di v1. SNMP v1 e v2 deve essere scelto solo per le reti che utilizzano SNMPv1 o SNMPv2. SNMP v3 è lo standard più recente di SNMP e risolve molti dei problemi di SNMP v1 e v2. In particolare, risolve molte delle vulnerabilità della sicurezza di v1 e v2. SNMP v3 consente inoltre agli amministratori di passare a uno standard SNMP comune.

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Gestione sistema > SNMP**. Viene visualizzata la pagina *SNMP*:

SNMP:  Enable  Disable

SNMP Version:  SNMP v1&v2  SNMP v3

System Contact:  (1-200 characters)

System Name:  \*(1-30 characters)

System Location:  \*(1-200 characters)

Security Username:  (1-32 characters)

Authentication Password:  (8-64 characters)

Authentication Method:  HMAC-MD5  HMAC-SHA

Encrypted Password:  (8-64 characters)

Encryption Method:  None  CBC-DES

SNMP Read-Only Community:  \*(1-32 characters)

SNMP Read-Write Community:  \*(1-32 characters)

Trap Community:  \*(1-32 characters)

SNMP Trusted Host:

Trap Receiver Host:  \*

\* indicates a mandatory option.

Save Cancel

Passaggio 2. Fare clic sul pulsante di opzione **Enable** per abilitare il protocollo SNMP.

Passaggio 3. Fare clic sul pulsante di opzione versione SNMP desiderata.

- SNMP v1&v2 — SNMP v1 è l'iterazione originale di SNMP e non dispone di determinate funzionalità, SNMP v2 è la versione più recente che migliora le funzionalità, ma questa opzione deve essere scelta solo per le reti che eseguono SNMP v1 o SNMP v2.

- SNMP v3: SNMP 3 è la versione più recente, che consente agli amministratori di utilizzare uno standard. È consigliabile scegliere questa opzione, in quanto consente di correggere molti difetti di protezione all'interno di v1 e v2.

## Configura SNMP per SNMP v1&v2

SNMP:  Enable  Disable

SNMP Version:  SNMP v1&v2  SNMP v3

System Contact:  (1-200 characters)

System Name:  \*(1-30 characters)

System Location:  \*(1-200 characters)

Security Username:  (1-32 characters)

Authentication Password:  (8-64 characters)

Authentication Method:  HMAC-MD5  HMAC-SHA

Encrypted Password:  (8-64 characters)

Encryption Method:  None  CBC-DES

SNMP Read-Only Community:  \*(1-32 characters)

SNMP Read-Write Community:  \*(1-32 characters)

Trap Community:  \*(1-32 characters)

SNMP Trusted Host:

Trap Receiver Host:  \*

\* indicates a mandatory option.

Save Cancel

Passaggio 4. (Facoltativo) Inserire le informazioni sul contatto nel campo Contatto di sistema. Persona da contattare per richiedere assistenza alla rete.

Passaggio 5. Inserire un nome nel campo Nome sistema. Questo è il nome assegnato alla configurazione SNMP.

Passaggio 6. Inserire un'ubicazione nel campo Ubicazione di sistema. Qui è dove si trova il sistema.

Passaggio 7. Inserire una community nel campo Community di sola lettura SNMP. Questo è

il parametro client per l'accesso in sola lettura del programma di installazione di SNMP.

Passaggio 8. Immettere una community nel campo Community di lettura/scrittura SNMP. Questo è il parametro client per l'accesso in lettura e scrittura del programma di installazione di SNMP.

Passaggio 9. Inserire una comunità nel campo Trap Community. Questa è la comunità che può utilizzare le trap SNMP. I trap sono notifiche dirette inviate all'amministratore. I trap consentono all'amministratore di gestire ogni dispositivo consentendo all'utente di inviarne notifica tramite una trap.

Passaggio 10. Immettere un host nel campo Host trusted SNMP. Questo è l'indirizzo IP dell'host di trust per l'installazione di SNMP.

Passaggio 11. Inserire un host nel campo Host ricevitore trap. Indirizzo IP dell'amministratore a cui inviare i trap.

Passaggio 12. Fare clic su **Save** per applicare le impostazioni.

## Configurare SNMP per SNMP v3

Passaggio 4. (Facoltativo) Inserire le informazioni sul contatto nel campo Contatto di sistema. Persona da contattare per richiedere assistenza alla rete.

Passaggio 5. Inserire un nome nel campo Nome sistema. Questo è il nome assegnato alla configurazione SNMP.

Passaggio 6. Inserire un'ubicazione nel campo Ubicazione di sistema. Qui è dove si trova il sistema.

The screenshot shows the SNMP configuration window with the following settings:

- SNMP:  Enable  Disable
- SNMP Version:  SNMP v1&v2  SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W \*(1-30 characters)
- System Location: Office \*(1-200 characters)
- Security Username: Profile1 (1-32 characters)
- Authentication Password: \*\*\*\*\* (8-64 characters)
- Authentication Method:  HMAC-MD5  HMAC-SHA
- Encrypted Password: (8-64 characters)
- Encryption Method:  None  CBC-DES
- SNMP Read-Only Community: public \*(1-32 characters)
- SNMP Read-Write Community: private \*(1-32 characters)
- Trap Community: public \*(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 \*

\* indicates a mandatory option.

Buttons: Save, Cancel

Passaggio 7. (Facoltativo) Immettere un nome utente nel campo Nome utente protezione. Questo è il nome utente usato per accedere alla configurazione SNMP.

Passaggio 8. (Facoltativo) Immettere una password nel campo Password di autenticazione. Questa è la password usata per accedere alla configurazione SNMP.

Passaggio 9. Fare clic sul pulsante di opzione HMAC-MD5 o HMAC-SHA nel campo Metodo di autenticazione. Il codice HMAC (Hash-based message authentication code) è un codice crittografato che combina un codice di autenticazione con una chiave di crittografia segreta. Lo scopo principale di HMAC è la sicurezza dei messaggi. Un HMAC autenticerà i dati in

base alle chiavi segrete prodotte.

·HMAC MD5 — Questo algoritmo hash presenta diversi difetti di sicurezza e i dati possono essere compromessi. HMAC MD5 è un meccanismo di autenticazione dei messaggi che utilizza funzioni di hash crittografiche. MD5 è utilizzato in situazioni in cui prestazioni superiori sono fondamentali per un sistema, anche se meno sicuro.

·HMAC SHA: questo algoritmo hash è molto più sicuro in quanto il metodo di crittografia è superiore. Si tratta di un meccanismo più sicuro per l'autenticazione dei messaggi che utilizza funzioni di hash crittografiche. HMAC SHA deve essere utilizzato quando la sicurezza è di importanza vitale.

SNMP configuration interface showing fields for System Name, System Location, Security Username, Authentication Password, Authentication Method (HMAC-MD5, HMAC-SHA), Encrypted Password, Encryption Method (None, CBC-DES), and various community and host settings.

Passaggio 10. Immettere una password nel campo Password crittografata.

Passaggio 11. Fare clic sul pulsante di opzione CBC-DES nel campo Metodo di crittografia. CBC e DES sono standard di crittografia che si combinano per proteggere i dati trasferiti.

Passaggio 12. Immettere una community nel campo Community di sola lettura SNMP. Questo è il parametro client per l'accesso in sola lettura del programma di installazione di SNMP.

Passaggio 13. Immettere una community nel campo Community di lettura/scrittura SNMP. Questo è il parametro client per l'accesso in lettura e scrittura del programma di installazione di SNMP.

Passaggio 14. Inserire una comunità nel campo Comunità trap. Questa è la comunità che può utilizzare le trap SNMP. Le trap sono notifiche dirette inviate all'amministratore. I trap consentono all'amministratore di gestire ogni dispositivo consentendo all'utente di inviarne notifica tramite una trap.

Passaggio 15. Inserire un host nel campo Host trusted SNMP. Questo è l'indirizzo IP dell'host di trust per l'installazione di SNMP.

Passaggio 16. Inserire un host nel campo Host ricevitore trap. Indirizzo IP dell'amministratore a cui inviare i trap.

Passaggio 17. Fare clic su **Save** per applicare le impostazioni.