Команда snmpd (SNMP daemon)

Содержание

Описание

Модуль поддержки сетевого протокола SNMP версии 1, 2c и 3.

Поддержка протокола SNMP является важной составляющей любого коммуникационного устройства, поскольку позволяет администратору сети использовать единую систему и механизмы контроля всей сети в целом и каждой её компоненты в отдельности.

Хотя в версиях SNMP v1 и 2c уделено недостаточно внимания вопросам безопасности самого протокола, что делает весьма проблематичным его использование для управления сетью, они широко используются для контроля и анализа функционирования сети.

Модуль SNMP также поддерживает версия SNMP v3 с моделью доступа USM (User-based Security Model) с аутентификацией MD5 и обеспечением конфиденциальности. Для организации доступа создаются пользователи с указанием имени, паролями и минимальными уровнями доступа (с аутентификацией и обеспечением конфиденциальности или без них).

Участниками SNMP являются агент и менеджер. Взаимодействие по протоколу происходит несимметрично, агент SNMP отправляет уведомления (traps) и отвечает на запросы, поступающие от менеджера SNMP. Менеджер SNMP собирает данные со всех агентов сети, получает уведомления и отправляет агенту запросы. Информация передается через запросы и ответы с использованием информационной базы управления (MIB).

Данная реализация поддерживает MIB-II, а также частные MIB.

Синтаксис:

```
user NAME (add|set) [pass PASSWORD] [sec[urity] (noAuthNoPriv|authNoPriv|authPriv)]
            [acc[essRights] (readOnly|readWrite)] [cla[ss] (guest|admin)]
            [privpass PRIVPASS]
user NAME del[ete]
comm[unity] NAME
(nodebug|debug  [prox] [trap] [stat] [mibs] [user] [cryp] [time] [flow])
(v1disable|v1enable) # SNMPv1 and SNMPv2c disable/enable
(start|stop)
clear
```

Параметры

Параметр	Описание
user NAME (add|set)	Добавляет/устанавливает имя пользователя.
[pass PASSWORD]	Назначает пароль пользователя SNMP.
[privpass PRIVPASS]	В данном параметре указывается пароль "privacy", если обеспечение конфиденциальности является требованием выбранного уровня защиты.
[sec[urity] (noAuthNoPriv|authNoPriv|authPriv)]	Устанавливает уровень безопасности: • *"noAuthNoPriv"* – самый низкий уровень: сообщения SNMP посылаются без аутентификации и без обеспечения конфиденциальности, требуется установить только имя пользователя. • "*authNoPriv"* – средний уровень: сообщения SNMP посылаются с аутентификацией, но без обеспечения конфиденциальности, требуется установить имя пользователя и пароль. • "*authPriv"* – самый высокий уровень: сообщения SNMP посылаются с аутентификацией и обеспечением конфиденциальности, требуется установить имя пользователя, пароль и пароль "privacy".

[acc [essRights] (readOnly|readWrite)]	Параметр используется для предоставления прав доступа к ресурсам: • *"readOnly"* – только чтение. • "readWrite" – чтение/изменение некоторых переменных, установлен по умолчанию.
[cla[ss] (guest|admin)]	Данный параметр предоставляет доступ: • *"guest"* – ограниченный, установлен по умолчанию. • *"admin"* – полный доступ ко всем переменным.
user NAME del[ete]	Удаляет указанное имя пользователя.
comm[unity] NAME	Позволяет изменить групповое имя при использовании SNMP версии 1 и 2c, по умолчанию имя группы "*public*". Агент SNMP может быть настроен таким образом, чтобы отвечать только на запросы, приходящие от менеджера, групповое имя которого соответствует заданному. Таким образом, прежде чем ответить на запрос менеджера, агент проверяет, относится ли тот к группе SNMP с правами доступа к запрошенной информации. Однако данная система безопасности несовершенна, так как имя группы передаётся с пакетом данных открытым текстом, что позволяет всем желающим его узнать и использовать.
(v1disable|v1enable)	Включает/отключает поддержку SNMPv1 и SNMPv2c. Отключение поддержки данных версий немного ускоряет обработку входящих SNMP-запросов.
(nodebug|debug [prox] [trap] [stat] [mibs] [user] [pack] [time] [flow])	Отключает/включает запись отладочной информации модуля SNMP в системный журнал. Позволяет вести записи по следующим параметрам: • *"[prox]"* – перенаправление SNMP-запросов из IP-сети в сеть MINT и SNMP-ответов в обратную сторону (устройства R5000 имеют встроенную функцию SNMP-прокси). • *"[trap]"* – пересылка и перекодировка уведомлений (traps) (подмножество функционала 'flow'). • *"[stat]"* – накопленная статистика по времени обработки SNMP-запросов (время ответа на этот запрос, на самый долгий запрос и среднее время ответа). • *"[mibs]"* – нахождение SNMP-значений в MIB-дереве устройства и подстановка значений в ответную датаграмму. • *"[user]"* – аутентификация и причины отсутствия ответов на некорректные SNMP-запросы в версии протокола SNMPv3. • *"[time]"* – запись точного времени приема и отправки пакетов SNMP. • *"[flow]"* – запись приема, подтверждения и разбора принятых SNMP-запросов, составления и отправки ответов, пересылки и перекодирования уведомлений (когда, что, откуда пришло, почему решили не отвечать, кому и почему решили переслать, что ответили).
(start|stop)	Включает/отключает модуль поддержки протокола SNMP.
clear	Удаляет конфигурацию SNMP на устройстве.

Примеры

Для пользователя с именем "*john*" назначим пароль "*mypassword*" и установим средний уровень безопасности с аутентификацией, но без обеспечения конфиденциальности.

```
snmpd user john add pass mypassword security authNoPriv
```