

Routerus

РОУТЕРЫ ▾

СЕТИ ▾

КОМПЬЮТЕРЫ

ИНТЕРНЕТ

LINUX ▾

Искать на сайте

Найти

- (разархивировать) файл tar.xz
- Команда tail в Linux
- Как смонтировать общий ресурс NFS в Linux
- Команда Basename в Linux
- Как удалить строки в Vim / Vi
- Команда Rsync в Linux с примерами
- Как удалить файлы и каталоги с помощью командной строки Linux
- Как сохранить файл в Vim / Vi и выйти из редактора
- Команда перезагрузки (перезагрузки) Linux
- Команда Stat в Linux
- Как монтировать и размонтировать файловые системы в Linux
- Как использовать sed для поиска и замены строки в файлах

Команда Netcat (nc) с примерами

26.12.2020 Linux, Команды Комментариев нет

Реклама от RtbSape

Netcat (или nc) — это утилита командной строки, которая считывает и записывает данные через сетевые соединения с использованием протоколов TCP или UDP. Это один из самых мощных инструментов в арсенале сетевых и системных администраторов, который считается швейцарским армейским ножом сетевых инструментов.

Netcat является кроссплатформенным и доступен для Linux, macOS, Windows и BSD. Вы можете использовать Netcat для отладки и мониторинга сетевых подключений, сканирования открытых портов, передачи данных в качестве прокси-сервера и многого другого.

Пакет Netcat предварительно установлен в macOS и популярных дистрибутивах Linux, таких как Ubuntu, Debian или CentOS.

Содержание

- Синтаксис Netcat
- Сканирование портов
- Отправка файлов через Netcat
- Создание простого чат-сервера
- Выполнение HTTP-запроса

Синтаксис Netcat

Самый простой синтаксис утилиты Netcat имеет следующий вид:

```
nc [options] host port
```

В Ubuntu вы можете использовать netcat или nc. Оба они являются символическими ссылками на версию Netcat для openBSD.

По умолчанию Netcat пытается запустить TCP-соединение с указанным хостом и портом. Если вы хотите установить UDP-соединение, используйте параметр -u:

```
nc -u host port
```

Сканирование портов

Сканирование портов — одно из самых распространенных применений Netcat. Вы можете сканировать один порт или диапазон портов.

Например, чтобы сканировать открытые порты в диапазоне 20-80, вы должны использовать следующую команду:

```
$ nc -z -v 10.10.8.8 20-80
```

Похожие статьи

В этой рубрике

- Как проверить (сканировать) на наличие открытых портов в Linux
- Команда wall в Linux
- Команды Pushd и Popd в Linux
- Как распаковать Popd в Linux (разархивировать) файл tar.xz
- Как распаковать Команда tail в Linux (разархивировать) файл tar.xz
- Как смонтировать общий ресурс NFS в Linux
- Как смонтировать общий ресурс Команда Basename в Linux
- Как удалять строки в Vim / Vi
- Команда Rsync в Linux
- Команда Rsync в Linux с примерами
- Как удалить файлы и каталоги с помощью командной строки Linux
- Как увеличивать и уменьшать размер экрана в Vim (Ctrl-U) и выйти из редактора
- Как удалить файлы и каталоги с помощью командной строки Linux (перезагрузки) Linux
- Как сохранить файл в Vim / Vi и выйти из редактора
- Команда Stat в Linux
- Как монтировать и размонтировать файловые системы в Linux
- Команда Stat в Linux
- Как использовать sed для поиска и замены строки в файлах

Похожие статьи

- Как проверить (сканировать) на наличие открытых портов в Linux
- Команда wall в Linux
- Команды Pushd и Popd в Linux
- Как распаковать (разархивировать) файл tar.xz
- Команда tail в Linux
- Как смонтировать общий ресурс NFS в Linux
- Команда Basename в Linux
- Как удалить строки в Vim / Vi
- Команда Rsync в Linux с примерами
- Как удалить файлы и каталоги с помощью командной строки Linux
- Как сохранить файл в Vim / Vi и выйти из редактора
- Команда перезагрузки (перезагрузки) Linux
- Команда Stat в Linux
- Как монтировать и размонтировать файловые системы в Linux
- Как использовать sed для поиска и замены строки в файлах

```
nc: connect to 10.10.8.8 port 20 (tcp) failed: Connection refused
nc: connect to 10.10.8.8 port 21 (tcp) failed: Connection refused
Connection to 10.10.8.8 22 port [tcp/ssh] succeeded!
nc: connect to 10.10.8.8 port 23 (tcp) failed: Connection refused
...
nc: connect to 10.10.8.8 port 79 (tcp) failed: Connection refused
Connection to 10.10.8.8 80 port [tcp/http] succeeded!
```

</>

Если вы хотите распечатать только строки с открытыми портами, вы можете отфильтровать результаты с помощью команды `grep`.

```
$ nc -z -v 10.10.8.8 20-80 2>&1 | grep succeeded
```

</>

```
Connection to 10.10.8.8 22 port [tcp/ssh] succeeded!
Connection to 10.10.8.8 80 port [tcp/http] succeeded!
```

</>

Вы также можете использовать Netcat для поиска серверного программного обеспечения и его версии. Например, если вы отправляете команду «EXIT» на сервер через [SSH-порт 22](#) по умолчанию:

```
$ echo "EXIT" | nc 10.10.8.8 22
```

</>

Результат будет выглядеть примерно так:

```
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4
Protocol mismatch.
```

</>

Чтобы сканировать порты UDP, просто добавьте к команде параметр `-u` как показано ниже:

```
$ nc -z -v -u 10.10.8.8 20-80
```

</>

Как правило, [Nmap](#) — лучший инструмент, чем Netcat для комплексного сканирования портов.

Отправка файлов через Netcat

Netcat можно использовать для передачи данных с одного хоста на другой путем создания базовой модели клиент / сервер.

Это работает путем настройки Netcat для прослушивания определенного порта (с использованием параметра `-l`) на принимающем хосте, а затем установления обычного TCP-соединения с другим хостом и отправки файла через него.

При получении выполните следующую команду, которая откроет порт 5555 для входящего соединения и перенаправит вывод в файл:

```
$ nc -l 5555 > file_name
```

</>

От отправляющего хоста подключитесь к принимающему хосту и отправьте файл:

```
$ nc receiving.host.com 5555 < file_name
```

</>

Чтобы передать каталог, вы можете использовать `tar` для архивации каталога на исходном хосте и для извлечения архива на целевом хосте.

На принимающем хосте настройте инструмент Netcat для прослушивания входящего соединения через порт 5555. Входящие данные передаются команде `tar`, которая распаковывает архив:

```
$ nc -l 5555 | tar xzvf -
```

</>



```
$ tar czvf - /path/to/dir | nc receiving.host.com 5555
```

Вы можете наблюдать за процессом передачи на обоих концах. По завершении CTRL+C чтобы закрыть соединение.

Создание простого чат-сервера

Процедура создания онлайн-чата между двумя и более хостами такая же, как и при передаче файлов.

На первом хосте запустите процесс Netcat для прослушивания порта 5555:



```
$ nc -l 5555
```

Со второго хоста выполните следующую команду для подключения к слушающему порту:



```
$ nc first.host.com 5555
```

Теперь, если вы наберете сообщение и нажмете ENTER оно будет отображаться на обоих хостах.

Чтобы закрыть соединение, введите CTRL+C

Выполнение HTTP-запроса

Хотя есть гораздо лучшие инструменты для HTTP-запросов, такие как curl, вы также можете использовать Netcat для отправки различных запросов на удаленные серверы.

Например, чтобы получить справочную страницу Netcat с веб-сайта OpenBSD, вы должны ввести:



```
$ printf "GET /nc.1 HTTP/1.1\r\nHost: man.openbsd.org\r\n\r\n" | nc man.openbsd.org 80
```

Полный ответ, включая заголовки HTTP и HTML-код, будет напечатан в терминале.

Выводы

В этом руководстве вы узнали, как использовать утилиту Netcat для установления и тестирования соединений TCP и UDP.

Для получения дополнительной информации посетите страницу руководства Netcat и прочтите обо всех других мощных параметрах команды Netcat.

Если у вас есть вопросы или замечания, пожалуйста, оставьте комментарий ниже.

Похожие статьи

- Как проверить (сканировать) на наличие открытых портов в Linux
- Команда wall в Linux
- Команды Pushd и Popd в Linux
- Как распаковать (разархивировать) файл tar.xz
- Команда tail в Linux
- Как смонтировать общий ресурс NFS в Linux
- Команда Basename в Linux
- Как удалить строки в Vim / Vi
- Команда Rsync в Linux с примерами
- Как удалить файлы и каталоги с помощью командной строки Linux
- Как сохранить файл в Vim / Vi и выйти из редактора
- Команда перезагрузки (перезагрузки) Linux
- Команда Stat в Linux
- Как монтировать и размонтировать файловые системы в Linux
- Как использовать sed для поиска и замены строки в файлах

Похожие статьи



Оставьте комментарий

Имя

Отправить

Похожие статьи

- [Как проверить \(сканировать\) на наличие открытых портов в Linux](#)
- [Команда wall в Linux](#)
- [Команды Pushd и Popd в Linux](#)
- [Как распаковать \(разархивировать\) файл tar.xz](#)
- [Команда tail в Linux](#)
- [Как смонтировать общий ресурс NFS в Linux](#)
- [Команда Basename в Linux](#)
- [Как удалить строки в Vim / Vi](#)
- [Команда Rsync в Linux с примерами](#)
- [Как удалить файлы и каталоги с помощью командной строки Linux](#)
- [Как сохранить файл в Vim / Vi и выйти из редактора](#)
- [Команда перезагрузки \(перезагрузки\) Linux](#)
- [Команда Stat в Linux](#)

[Вернуться на верх](#)

[размонтировать файловые системы в Linux](#)

- [Как использовать sed для поиска и замены строки в файлах](#)