Настройка SSH

Введение

SSH (Secure Shell) — это протокол для удаленного управления и передачи файлов, обеспечивающий безопасность благодаря шифрованию. В НАЙС ОС SSH используется для безопасного доступа к серверам, выполнения удаленных команд и передачи данных между машинами. В этой документации мы рассмотрим, как установить, настроить и обезопасить SSH-сервер в НАЙС ОС.

Установка OpenSSH

OpenSSH — это наиболее распространенная реализация SSH, которая включает сервер и клиентские утилиты. Для установки OpenSSH используйте `dnf`:

```
sudo dnf install openssh-server openssh-clients
```

Запуск и управление службой SSH

Запустите и настройте автозапуск службы SSH:

```
sudo systemctl start sshd
sudo systemctl enable sshd
```

Проверка состояния службы

Убедитесь, что служба SSH работает корректно:

```
sudo systemctl status sshd
```

Основные команды SSH

Для работы с SSH используются несколько основных команд:

Подключение к удаленному серверу

Используйте команду `ssh` для подключения к удаленному серверу:

```
ssh user@remote_host
```

Копирование файлов с использованием SCP

Команда `scp` используется для копирования файлов между локальной и удаленной машинами:

```
scp /path/to/local/file user@remote_host:/path/to/remote/destination
```

Использование SFTP для передачи файлов

Команда `sftp` предоставляет интерфейс для передачи файлов по SSH:

```
sftp user@remote_host
```

Настройка SSH-сервера

Конфигурационный файл SSH-сервера находится по пути `/etc/ssh/sshd_config`. Измените настройки по умолчанию для повышения безопасности и настройки специфичных параметров.

Ограничение доступа по IP-адресу

Для ограничения доступа к SSH-серверу с определенных IP-адресов используйте директивы `AllowUsers` и `DenyUsers`:

```
sudo nano /etc/ssh/sshd_config
```

Добавьте следующие строки:

```
AllowUsers user1@192.168.1.100
DenyUsers user2@192.168.1.101
```

Изменение порта SSH

Для повышения безопасности измените порт по умолчанию (22) на нестандартный порт:

```
sudo nano /etc/ssh/sshd_config
```

Измените строку:

```
Port 2222
```

Отключение входа под пользователем root

Для повышения безопасности отключите вход под пользователем root:

```
sudo nano /etc/ssh/sshd_config
```

Измените строку:

```
PermitRootLogin no
```

Ограничение аутентификации по паролю

Для повышения безопасности используйте аутентификацию по ключам вместо паролей:

```
sudo nano /etc/ssh/sshd_config
```

Измените строку:

```
PasswordAuthentication no
```

Перезагрузка службы SSH

После внесения изменений перезагрузите службу SSH для применения новых настроек:

```
sudo systemctl restart sshd
```

Аутентификация по ключам SSH

Аутентификация по ключам SSH обеспечивает более высокий уровень безопасности по сравнению с паролями.

Создание ключей SSH

Используйте команду `ssh-keygen` для создания пары ключей (публичного и приватного):

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

Следуйте инструкциям на экране для сохранения ключей.

Копирование публичного ключа на удаленный сервер

Используйте команду `ssh-copy-id` для копирования публичного ключа на удаленный сервер:

```
ssh-copy-id user@remote_host
```

Теперь вы можете подключаться к удаленному серверу без пароля:

```
ssh user@remote_host
```

Дополнительные настройки безопасности SSH

Для дополнительной защиты SSH-сервера можно использовать следующие настройки и методы:

Настройка двухфакторной аутентификации

Для настройки двухфакторной аутентификации используйте Google Authenticator:

```
sudo dnf install google-authenticator
google-authenticator
```

Следуйте инструкциям на экране для настройки двухфакторной аутентификации.

Использование Fail2ban для защиты от брутфорс-атак

Fail2ban автоматически блокирует IP-адреса после нескольких неудачных попыток входа:

```
sudo dnf install fail2ban
sudo systemctl start fail2ban
sudo systemctl enable fail2ban
```

Создайте конфигурационный файл для SSH:

```
sudo nano /etc/fail2ban/jail.local
```

Добавьте следующие строки:

```
[sshd]
enabled = true
port = 2222
logpath = /var/log/secure
maxretry = 3
```

Перезапустите Fail2ban для применения изменений:

```
sudo systemctl restart fail2ban
```

Использование SSH-туннелей

SSH-туннели позволяют передавать данные через защищенное соединение, обеспечивая безопасную передачу информации между клиентом и сервером.

Создание локального SSH-туннеля

Локальный SSH-туннель перенаправляет локальный порт на удаленный сервер:

```
ssh -L local_port:remote_host:remote_port user@remote_host
```

Например, для перенаправления локального порта 8080 на удаленный сервер с портом 80:

```
ssh -L 8080:localhost:80 user@remote_host
```

Создание удаленного SSH-туннеля

Удаленный SSH-туннель перенаправляет удаленный порт на локальный сервер:

```
ssh -R remote_port:localhost:local_port user@remote_host
```

Например, для перенаправления удаленного порта 8080 на локальный сервер с портом 80:

```
ssh -R 8080:localhost:80 user@remote_host
```

Создание динамического SSH-туннеля

Динамический SSH-туннель работает как SOCKS-прокси, позволяя перенаправлять трафик через SSH-соединение:

```
ssh -D local_port user@remote_host
```

Например, для создания SOCKS-прокси на локальном порту 1080:

```
ssh -D 1080 user@remote_host
```

Использование SSH-агента

SSH-агент позволяет управлять ключами SSH и облегчает аутентификацию при множественных подключениях.

Запуск SSH-агента

Запустите SSH-агент и добавьте свой ключ:

```
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_rsa
```

Просмотр добавленных ключей

Для просмотра списка добавленных ключей используйте команду `ssh-add -l`:

```
ssh-add -l
```

Удаление ключа из SSH-агента

Для удаления ключа из агента используйте команду `ssh-add -d`:

```
ssh-add -d ~/.ssh/id_rsa
```

Журналирование и аудит SSH

Журналирование действий SSH помогает отслеживать подключение и выявлять потенциальные угрозы безопасности.

Просмотр журналов SSH

Журналы SSH можно просмотреть с помощью команды `tail`:

```
sudo tail -f /var/log/secure
```

Настройка подробного журналирования

Для настройки более подробного журналирования измените конфигурацию SSH:

```
sudo nano /etc/ssh/sshd_config
```

Добавьте или измените строки:

```
LogLevel VERBOSE
```

Перезагрузите службу SSH для применения изменений:

```
sudo systemctl restart sshd
```

Заключение

Настройка SSH в НАЙС ОС является важным аспектом обеспечения безопасности и управления удаленным доступом. Используя рассмотренные методы и инструменты, вы сможете настроить SSH-сервер, обеспечить безопасность соединений, использовать аутентификацию по ключам, настраивать туннели и журналирование. Следование приведенным рекомендациям поможет защитить вашу систему и обеспечить надежный удаленный доступ.