Для эксплуатации сайтов на Bitrix я чаще всего использую BitrixEnv. Это удобный инструмент с консольным управлением, основанном на рецептах ansible. В типовых случаях это сильно упрощает разворачивание и управление окружением. При этом сделано все в целом качественно и удобно, всегда можно все поправить руками, если понимаешь, что и как делать. Но вот если нужно сделать что-то не типовое, возникают закономерные сложности.

Содержание

Введение

Ранее я уже рассказывал, как делать тонкую настройку сервера под bitrix на основе bitrixenv. Сейчас продолжу эту тему и расскажу, как добавить еще одного пользователя в систему, чтобы он мог спокойно работать над сайтом. Напомню, что по умолчанию bitrixenv создает системного пользователя bitrix с доступом по ssh к серверу. От этого пользователя работают многие службы, так же для него выставлены полные права на исходники сайта.

Если над проектом работает один программист, то нет никаких проблем. Ему выдается пользователь bitrix, который не имеет полных прав на сервере, но при этом может работать с исходниками сайта. И все в порядке. А вот если надо организовать одновременную работу нескольких разработчиков, которым нужен прямой доступ к исходникам сайта, то придется что-то придумывать. Давать им всем одного и того же пользователя неудобно. Нужно каждому свой. Я покажу далее, как это сделать.

Напомню, что по-хорошему, вести разработку сайта необходимо с использованием git. Ранее я показывал пример, как можно деплоить bitrix сайт из репозитория. На практике, над небольшими проектами работают по старинке, правя напрямую исходники сайта. Зачастую даже без dev окружения. Я с этим постоянно сталкиваюсь, когда соприкасаюсь с небольшими интернет магазинами. Думаю, для микро проектов это приемлемо, так как отслеживать

изменения по репозиторию банально некому.

В общем, если вам нужна дополнительная учетная запись для работы с bitrix, рассказываю, как это сделать. Причем доступ у этой учетки будет только к папке с исходниками сайта. Первое, что приходит на ум, это создать отдельного пользователя с шелом */sbin/nologin* и настроить ему chroot по sftp в настройках ssh. Это первое, что я попробовал. Подробно об этом я рассказываю в отдельной статье про доступ к сайту через sftp. Но в данном случае это не прокатывает. При подключении вы будете получать ошибку в */var/log/secure*:

```
Aug 10 16:11:08 bitrix-dev sshd[3819]: pam_unix(sshd:session): session opened for user devbitrix01 by (uid=0)
Aug 10 16:11:08 bitrix-dev sshd[3819]: fatal: bad ownership or modes for chroot directory component "/home/bitrix/"
[postauth]
Aug 10 16:11:08 bitrix-dev sshd[3819]: pam_unix(sshd:session): session closed for user devbitrix01
```

Суть ошибки в том, что на всем пути до chroot директории, владельцем каталогов с правами на запись может быть только root. Нам это никак не подходит, так как у домашнего каталога */home/bitrix* владельцем должен быть пользователь bitrix.

Добавление sftp пользователя в bitrixenv

Рассказываю дальше, как все сделать правильно. Настроим все сразу для группы, чтобы потом можно было добавлять неограниченное количество пользователей для работы с файлами сайта.

Добавляем в систему группу dev-group.

```
# groupadd dev-group
```

Настроим chroot для всех пользователей этой группы, чтобы они не могли выйти за пределы каталога с сайтами при подключении к исходникам по sftp. Для этого редактируем файл */etc/ssh/sshd_config*. Комментируем существующий параметр и добавляем новые.

```
#Subsystem      sftp        /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
```

```
Match Group dev-group
ChrootDirectory /home/dev-group/
```

Для применения настроек перезапускаем sshd.

```
# systemctl restart sshd
```

Теперь создаем нового пользователя, который будет работать с сайтом.

```
# adduser devbitrix01 -g600 -o -u600 -s /sbin/nologin -d /home/dev-group/
```

devbitrix01	имя нового пользователя
-g600	принадлежность к группе с id 600, дефолтный id для группы bitrix в bitrixenv
-o	ключ, позволяющий создать пользователя с неуникальным id
-u600	задаем id пользователя 600 как у пользователя bitrix в bitrixenv
-s /sbin/nologin	указываем shell, данном случае его отсутствие
-d /home/dev-group	домашний каталог для пользователя

Если пользователю нужен будет доступ к консоли по ssh, то вместо /sbin/nologin укажите /bin/bash. Устанавливаем пароль для пользователя:

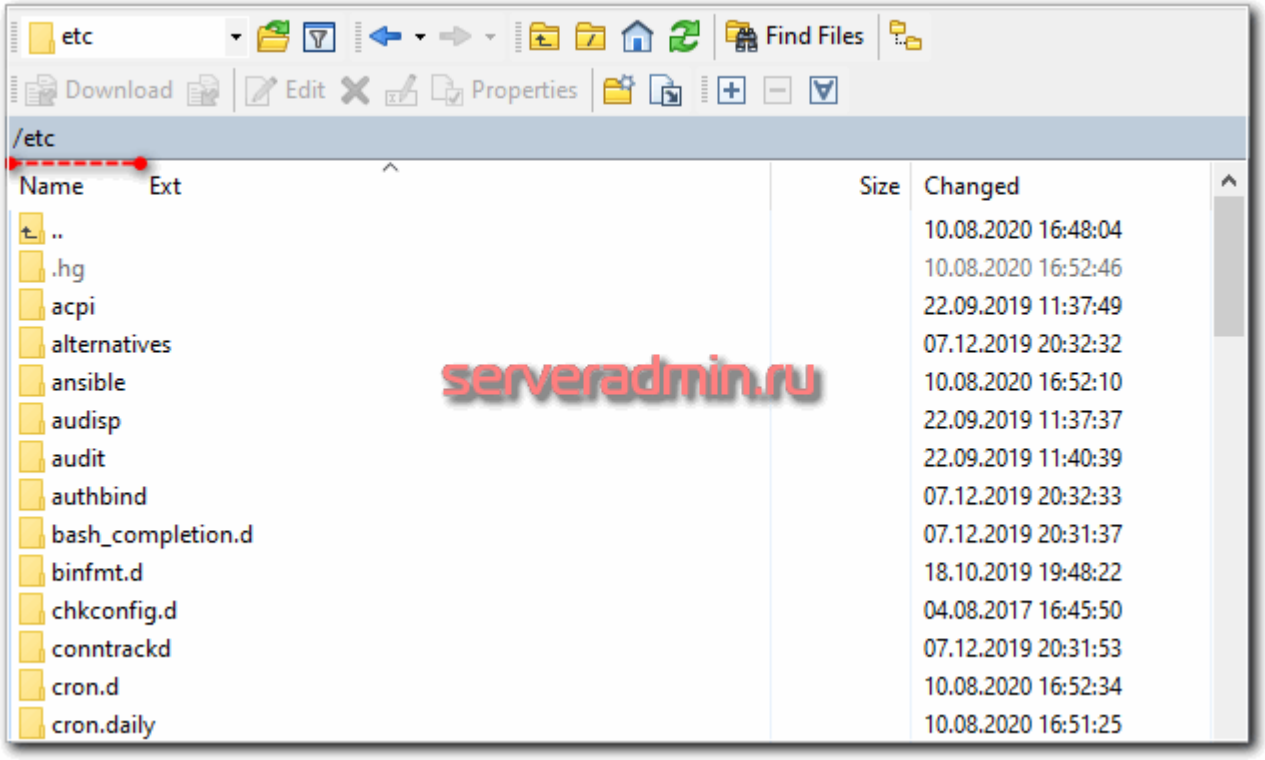
```
# passwd devbitrix01
```

Теперь для того, чтобы заработал chroot по sftp, выставляем необходимые права доступа на домашний каталог пользователя:

```
# chown root:bitrix /home/dev-group/
```

```
# chmod 750 /home/dev-group/
```

Уже сейчас вы можете подключиться по sftp пользователем и проверить доступ. Удивитесь, когда обнаружите, что пользователь может перемещаться по всем директориям сервера.



Все правильно, я еще не добавил его в группу dev-group, для которой назначен chroot. Делаем это.

```
# usermod -aG dev-group devbitrix01
```

Отключитесь и подключитесь заново. Пользователь будет сразу попадать в свой домашний каталог, выхода из которого у него теперь нет. Дальше нам осталось добавить в этот каталог исходники сайта.

Доступ к bitrix сайтам разным пользователям по sftp

Делается это с помощью **mount --bind**. Если у вас несколько сайтов, то имеет смысл для каждого сайта делать отдельный каталог и моунтить туда нужный сайт.

```
# mkdir /home/dev-group/site1.ru
# chown bitrix. /home/dev-group/site1.ru
# chmod 750 /home/dev-group/site1.ru
# mount --bind /home/bitrix/ext_www/site1.ru /home/dev-group/site1.ru
```

Подключитесь еще раз по sftp и попробуйте отредактировать или создать файл в каталоге с сайтом. Его владельцем будет пользователь bitrix, что нам и нужно для корректной работы с сайтом.

При необходимости, можете добавить монтирование каталога с сайтом в автозагрузку, чтобы не пришлось это делать еще раз после перезагрузки сервера. Для этого в /etc/fstab добавьте в самый конец строку.

```
/home/bitrix/ext_www/site1.ru /home/dev-group/site1.ru none bind 0 0
```

Обязательно убедитесь, что файл fstab оканчивается **переходом на новую строку**. Это важно. Перезагрузите сервер, чтобы убедиться в том, что все корректно настроили.

Если вам нужно добавить еще одного пользователя для работы над такими же сайтами, то просто добавляйте его в систему по аналогии с первым.

```
# adduser devbitrix02 -g600 -o -u600 -s /sbin/nologin -d /home/dev-group/
# passwd devbitrix02
# usermod -aG dev-group devbitrix02
```

В том случае, когда список сайтов для разных пользователей будет разный, добавляйте новую группу в другую домашнюю директорию и биндите туда другой набор сайтов. Если же вам изначально нет необходимости управлять группами, то в настройках sshd вместо:

```
Match Group dev-group
```

используйте

```
Match User devbitrix01
```

и так для каждого отдельного пользователя.

Небольшое замечание по работе mount с ключом bind. Тут надо быть аккуратным. Если у вас сложная конфигурация сервера и в какой-то момент вы отмонтируете диск с сайтами, откуда стоят линки на домашние директории пользователей, там эти точки монтирования останутся, как и доступ к файлам. Так что прежде чем что-то делать с разделом, где лежат сайты, отмонтируйте все каталоги, которые биндили пользователям. Посмотреть их можно командой mount без ключей.

```
# mount
```

```
[root@249265 ~]# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=2012544k,nr_inodes=503136,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-agent,name=syst
emd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_prio,net_cls)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/sda1 on / type ext4 (rw,relatime,errors=panic,data=ordered)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=21,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=10044)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
/dev/sda1 on /home/dev-group/site1.ru type ext4 (rw,relatime,errors=panic,data=ordered)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=404524k,mode=700)
tmpfs on /run/user/600 type tmpfs (rw,nosuid,nodev,relatime,size=404524k,mode=700,uid=600,gid=600)
[root@249265 ~]#
```


На этом у меня все по настройке sftp пользователей для bitrix. Надеюсь, эта информация будет для вас полезна. Мне она периодически нужна, поэтому

решил оформить в статью, чтобы самому потом было проще вспоминать последовательность действий.