UNLIMITED PRODUCTION

eXpress

Система коммуникаций

Руководство администратора

Обновление

ОГЛАВЛЕНИЕ

РУЧНОЕ ОБНОВЛЕНИЕ

Внимание! Выполните резервное копирование перед выполнением процедуры обновления!

SINGLE CTS

Для обновления системы версии ниже 1.28:

1. Запустите командную строку.
2. Удалите старую версию инсталлятора:

```
# rm -rf /usr/local/bin/deployka /usr/local/bin/dpl
```

3. Загрузите новый инсталлятор:

```
#docker run -d --rm --name dpl-install \
registry.public.express/dpl:master sleep 10 && \
# docker cp dpl-install:/deployka /usr/local/bin/dpl
```

4. Остановите работу приложения:

```
# DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

5. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить).
6. Выполните команды для замены хозяев файлов некоторых сервисов:

```
# docker volume inspect --format '{{ .Mountpoint }}'
cts_ccs_admin_public \ cts_file_service_uploads
cts_messaging_cache cts_messaging_uploads \
cts_phonebook_uploads | xargs sudo chown -R 888:888
```

Если предыдущая версия nginx меньше, чем 1.20.1 и используются letsencrypt сертификаты:

- Очистите хранилище letsencrypt (один раз):

```
# rm -rf cts/letsencrypt
dpl cadvinstall && dpl nxinstall
```

7. Запустите обновление:

```
# dpl -d
```

После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут).

8. Проверьте логи на наличие ошибок командой:

```
# dpl -dc logs -tail=200 -f
```

Для обновления системы версии 1.28 и выше:

1. Запустите командную строку.
2. Удалите старую версию инсталлятора:

```
# rm -rf /usr/local/bin/deployka /usr/local/bin/dpl
```

3. Загрузите новый инсталлятор:

```
#docker run -d --rm --name dpl-install \
registry.public.express/dpl:master sleep 10 && \
# docker cp dpl-install:/deployka /usr/local/bin/dpl
```

4. Остановите работу приложения:

```
# DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

5. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить).
6. Запустите обновление:

```
# dpl -d
```

После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут).

7. Проверьте логи на наличие ошибок командой:

```
# dpl -dc logs -tail=200 -f
```

FRONT CTS И BACK CTS

Внимание! Проверьте доступность портов 2379/TCP (etcd), 6379/TCP (redis) от Front CTS к Back CTS перед началом работ!

Первым обновляется сервер Front CTS, затем сервер Back CTS.

Для обновления севера Front CTS:

1. Запустите командную строку.
2. Удалите старую версию инсталлятора:

```
# rm -rf /usr/local/bin/deployka /usr/local/bin/dpl
```

3. Загрузите новый инсталлятор:

```
# docker run -d --rm --name dpl-install \
registry.public.express/dpl:master sleep 10 &&
# docker cp dpl-install:/deployka /usr/local/bin/dpl
```

4. Остановите работу приложения командой:

```
# DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

5. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить)

Если предыдущая версия nginx меньше, чем 1.20.1 и используются letsencrypt сертификаты:

- Очистите хранилище letsencrypt (один раз):

```
# rm -rf cts/letsencrypt
```

6. Запустите обновление:

```
# dpl -d
```

После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут)

7. Проверьте логи на наличие ошибок командой:

```
# dpl -dc logs -tail=200 -f
```

Для обновления севера Back CTS:

1. Запустите командную строку.
2. Удалите старую версию инсталлятора:

```
# rm -rf /usr/local/bin/deployka /usr/local/bin/dpl
```

3. Загрузите новый инсталлятор:

```
# docker run -d --rm --name dpl-install \
registry.public.express/dpl:master sleep 10 &&
# docker cp dpl-install:/deployka /usr/local/bin/dpl
```

4. Остановите работу приложения командой:

```
# DEPLOYKA_SKIP_UPDATE=true dpl --dc stop
```

5. Выполните резервное копирование файлов /var/lib/docker/volumes (после нескольких дней эксплуатации скопированные файлы можно удалить)
6. Если версия сервера ниже 1.28, выполните:

```
# docker volume inspect --format '{{ .Mountpoint }}'
cts_ccs_admin_public \ cts_file_service_uploads
cts_messaging_cache cts_messaging_uploads \
cts_phonebook_uploads | xargs sudo chown -R 888:888
# dpl cadvinstall && dpl nxinstall
```

7. Запустите обновление:

```
# dpl -d
```

   После запуска обновления требуется время на проведение внутренних процедур (ориентировочное время 10-15 минут)

8. Проверьте логи на наличие ошибок командой:

```
# dpl -dc logs -tail=200 -f
```

ОТКАЗОУСТОЙЧИВАЯ КОНФИГУРАЦИЯ

В случае невозможности использования скриптов автоматического обновления выполните обновление в ручном режиме.

Для обновления отказоустойчивой конфигурации:

1. Скопируйте новые версии образов docker и скрипт загрузки образов в каталог /tmp/images и загрузите образы с помощью скрипта load.sh:

```
# cp *.tar /tmp/images/
# cp /opt/deploy/script/load.sh /tmp/images/
# cd /tmp/images/
# ./load.sh
```

2. Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02.
3. Выполните команду для остановки антивируса:

```
# systemctl stop kesl klnagent64
```

   Примечание. В случае зависания сервера при остановке антивируса, перезагрузите оба узла кластера через систему виртуализации.

4. Выполните команду:

```
# pcs status
```

5. Убедитесь, что ресурсы кластера запущены согласно списку ниже:
   - dlm-clone [dlm] (back кластер) – запущен на обоих узлах кластера;
   - clvmd-clone [clvmd] (back кластер) – запущен на обоих узлах кластера;
   - clusterfs-clone [clusterfs] (back кластер) – запущен на обоих узлах кластера;
   - cluster_ip – запущен на одном узле кластера;
   - dockerd – запущен на одном узле кластера;
   - node_exporter (back кластер) – запущен на одном узле кластера;
   - cadvisor (back кластер) – запущен на одном узле кластера;
   - vmfence (back кластер) – запущен на одном узле кластера;

   Если ресурсы кластера не находятся в состоянии, перечисленным выше, выполните команду, заменив *resource_name* на имя проблемного ресурса:

```
# pcs resource cleanup resource_name
```

6. На узлах кластера Back с индексом 01 и 02 выполните команду ниже:

```
# ls -la /opt/ex_data/files
```

Примечание. В случае зависание вывода списка директорий необходимо перезагрузить оба узла кластера через систему виртуализации

7. Подключитесь к консоли сервера Back кластера с индексом 01 либо 02 и выполните команду:

```
# pcs status | grep dockerd
```

Примечание. Команда выполняется для определения текущего первичного узла, на котором запущены ресурсы кластера.

8. Подключитесь к консоли текущего первичного узла кластера Back и последовательно выполните команды:

```
# cd /opt/express
# dpl -g
```

9. Подключитесь к консоли сервера Front кластера с индексом 01 либо 02 и выполните команду:

```
# pcs status | grep dockerd
```

Примечание. Команда выполняется для определения текущего первичного узла, на котором запущены ресурсы кластера.

10. Подключитесь к консоли текущего первичного узла кластера Front и последовательно выполните команды:

```
# cd /opt/express
# dpl -g
# cd /opt/express-voice
# dpl -g
```

11. Подключитесь к консоли вторичного узла кластера Back и последовательно выполните команды, заменив full_fqdn_slave_server на полное доменное имя вторичного узла кластера:

```
# pcs resource move cluster_ip full_fqdn_slave_server
# pcs resource move dockerd full_fqdn_slave_server
```

12. Дождитесь переключения ресурсов кластера dockerd и cluster_ip на вторичный узел кластера Back. Для мониторинга состояния ресурсов периодически выполняйте команду:

```
# pcs status
```

13. После переключения ресурсов на вторичный узел кластера Back, последовательно выполните команды:

```
# cd /opt/express
# dpl -g
```

14. Подключитесь к консоли вторичного узла кластера Front и последовательно выполните команды, заменив full_fqdn_slave_server на полное доменное имя вторичного узла кластера:

```
# pcs resource move cluster_ip full_fqdn_slave_server
# pcs resource move dockerd full_fqdn_slave_server
```

15. Дождитесь переключения ресурсов кластера dockerd и cluster_ip на вторичный узел кластера Front. Для мониторинга состояния ресурсов периодически выполняйте команду следующую команду:

```
# pcs status
```

16. После переключения ресурсов на вторичный узел кластера Front, последовательно выполните команды:

```
# cd /opt/express
# dpl -g
# cd /opt/express-voice
# dpl -g
```

17. Подключитесь к консоли текущего первичного узла кластера Back и последовательно выполните команды:

```
# cd /opt/express
# dpl --dc stop
# dpl nxinstall && dpl cadvinstall
# dpl -d
```

18. После завершения обновления сервера откройте вывод логов работы контейнеров:

```
# dpl --dc logs --tail=100 -f
```

19. Дождитесь остановки вывода логов контейнеров кроме контейнера nginx.
20. Подключитесь к консоли сервера Front кластера с индексом 01 либо 02 и выполните команду:

```
# pcs status | grep dockerd
```

Примечание. Команда выполняется для определения текущего первичного узла, на котором запущены ресурсы кластера.

21. Подключитесь к консоли текущего первичного узла кластера Front и последовательно выполните команды:

```
# cd /opt/express
# dpl --dc stop
# dpl -d
# cd /opt/express-voice
# dpl --dc stop
# dpl -d
```

22. После обновления первичных узлов кластеров Front и Back проверьте функционирование системы, выполните проверку логов на ошибки и функции отправки сообщений.
23. Подключитесь к консоли вторичного узла кластера Back и последовательно выполните команды заменив full_fqdn_slave_server на полное доменное имя вторичного узла кластера:

```
# pcs resource move cluster_ip full_fqdn_slave_server
# pcs resource move dockerd full_fqdn_slave_server
```

24. Дождитесь переключения ресурсов кластера dockerd и cluster_ip на вторичный узел кластера Back. Для мониторинга состояния ресурсов периодически выполняйте команду следующую команду:

```
# pcs status
```

25. После переключения ресурсов на вторичный узел кластера Back, последовательно выполните команды:

```
# cd /opt/express
# dpl --dc stop
# dpl nxinstall && dpl cadvinstall
# dpl -d
```

26. После завершения обновления сервера необходимо открыть вывод лога работы контейнеров и дождитесь остановки вывода логов контейнеров кроме контейнера nginx:

```
# dpl --dc logs --tail=100 -f
```

27. Подключитесь к консоли вторичного узла кластера Front и последовательно выполните команды, заменив full_fqdn_slave_server на полное доменное имя вторичного узла кластера:

```
# pcs resource move cluster_ip full_fqdn_slave_server
# pcs resource move dockerd full_fqdn_slave_server
```

28. Дождитесь переключения ресурсов кластера dockerd и cluster_ip на вторичный узел кластера Front. Для мониторинга состояния ресурсов периодически выполняйте команду:

```
# pcs status
```

29. После переключения ресурсов на вторичный узел кластера Front, последовательно выполните команды:

```
# cd /opt/express
# dpl --dc stop
# dpl -d
# cd /opt/express-voice
# dpl --dc stop
# dpl -d
```

30. Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02, выполните команду для запуска антивируса:

```
# systemctl start kesl klnagent64
```

ОБНОВЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ ANSIBLE СЦЕНАРИЕВ

SINGLE CTS, BACK CTS И FRONT CTS

Для обновления сервера:

1. Запустите ansible playbook для обновления всех контейнеров:

```
# ansible-playbook --ask-pass -v 05-update_cts.yaml
```

2. Введите пароль учетной записи root после ввода команды.

Для обновления ПО, установленного в контейнерах docker, на сервере Registry выполните:

Внимание! При выполнении скриптов обновления нельзя пропускать паузы, заложенные в него, т.к. их пропуск может привести к ошибкам обновления.

1. Скопируйте новые версии образов docker и скрипт загрузки образов в каталог /tmp/images и загрузите образы с помощью скрипта load.sh (скрипт доступен по ссылке):

```
# cp *.tar /tmp/images/
# cp /opt/deploy/script/load.sh /tmp/images/
# cd /tmp/images/
# ./load.sh
```

2. Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02, выполните команду для остановки антивируса:

```
# systemctl stop kesl klnagent64
```

Примечание. В случае зависания сервера при остановке антивируса перезагрузите оба узла кластера через систему виртуализации.

3. Выполните команду:

```
# pcs status
```

4. Убедитесь, что ресурсы кластера запущены согласно списку ниже:
   - dlm-clone [dlm] (back кластер) – запущен на обоих узлах кластера;
   - clvmd-clone [clvmd] (back кластер) – запущен на обоих узлах кластера;
   - clusterfs-clone [clusterfs] (back кластер) – запущен на обоих узлах кластера;
   - cluster_ip – запущен на одном узле кластера;
   - dockerd – запущен на одном узле кластера;
   - node_exporter (back кластер) – запущен на одном узле кластера;
   - cadvisor (back кластер) – запущен на одном узле кластера;
   - vmfence (back кластер) – запущен на одном узле кластера;
5. В случае если статус ресурсов кластера не соответствует перечисленным выше, выполните следующую команду, заменив *resource_name* на имя проблемного ресурса:

```
# pcs resource cleanup resource_name
```

6. На узлах кластера Back с индексом 01 и 02 выполните команду ниже:

```
# ls -la /opt/ex_data/files
```

Примечание. В случае зависание вывода списка директорий перезагрузите оба узла кластера через систему виртуализации.

7. Подключитесь к консоли сервера Back и Front кластера с индексом 01 либо 02 и выполните команду для определения текущего первичного узла, на котором запущены ресурсы кластера:

```
# pcs status | grep dockerd
```

8. Подключитесь к консоли текущего первичного узла кластера Back и Front и последовательно выполните команду:

```
# docker ps -a > current_version.txt
```

9. Сохраните полученный файл. Он потребуется для процедуры отката на предыдущую версию.
10. Запустить скрипт автоматического обновления всех контейнеров первичных серверов и ввести пароль учетной записи root после ввода команды:

```
# ansible-playbook --ask-pass -v 05-master_update_cts.yaml
```

11. После обновления первичных серверов проверьте функционирование системы, выполнив проверку логов на наличие ошибок и функции отправки сообщений.
12. Запустите скрипт автоматического обновления всех контейнеров вторичных серверов:

```
# ansible-playbook --ask-pass -v 06-slave_update_cts.yaml
```

13. Введите пароль учетной записи root.
14. Подключитесь к консоли сервера Back и Front кластера с индексом 01 и 02, выполните команду для запуска антивируса:

```
# systemctl start kesl klnagent64
```

Для отката на предыдущую версию ПО, установленного в контейнерах docker:

1. Подключитесь к консоли узлов кластера Back с индексами 01 и 02.
2. Добавьте в файл /opt/express/settings следующие строки, заменив в них версию ПО на значения из файла current_version.txt (файл получен на шаге 3 описания автоматического обновления с помощью скриптов ansible):

```
images:
  messaging: messaging:1.39.6
  settings: settings:1.39.0
  audit: audit:1.39.0
  admin: admin:1.39.1
  file_service: file_service:1.39.0
  voex: voex:1.39.0
  ad_phonebook: ad_phonebook:1.39.1
  email_notifications: email_notifications:1.39.0
  botx: botx:1.39.1
  ad_integration: ad_integration:1.39.0
  kdc: kdc:1.39.0
  routing_schema_service: routing_schema_service:1.39.0
```

3. Подключитесь к консоли узлов кластера Front с индексами 01 и 02.

4. Добавьте в файл /opt/express/settings следующие строки заменив в них версию ПО на значения из файла current_version.txt (получен на шаге 3 описания автоматического обновления с помощью скриптов ansible):

```
images:
  trusts: trusts:1.39.0
```

5. Запустить скрипт автоматического обновления всех контейнеров первичных серверов и ввести пароль учетной записи root после ввода команды:

```
# ansible-playbook --ask-pass -v 05-master_update_cts.yaml
```

6. После обновления первичных серверов проверьте нормальное функционирование системы, выполнив проверку логов и функцию отправки сообщений.
7. Запустить скрипт автоматического обновления всех контейнеров вторичных серверов:

```
# ansible-playbook --ask-pass -v 06-slave_update_cts.yaml
```

8. Введите пароль учетной записи root после ввода команды.

Для обновления ПО, установленное в контейнерах docker Web client кластера, на сервере Registry выполните:

Важно! При выполнении скриптов обновления нельзя пропускать паузы, заложенные в него, т.к. их пропуск может привести к ошибкам обновления.

1. Скопируйте новые версии образов docker и скрипт загрузки образов в каталог /tmp/images сервера Registry.
2. Загрузите образы с помощью скрипта load.sh:

```
# cp *.tar /tmp/images/
# cp /opt/deploy/script/load.sh /tmp/images/
# cd /tmp/images/
# ./load.sh
```

3. С помощью команды ниже необходимо уточнить новую версию образа контейнера web client:

```
# docker images | grep web_client
```

4. Измените параметр web_client_image на актуальную версию, полученную на предыдущем шаге (параметр локализован в файле настроек group_vars/all.yaml в каталоге сценариев ANSIBLE web client (/opt/deploy/playbook-webclient)).
5. Запустите скрипт автоматического обновления всех контейнеров первичного узла кластера Web Client:

```
# ansible-playbook --ask-pass -v 05-master_update_web.yaml
```

6. Введите пароль учетной записи root.
7. После обновления первичного узла кластера Web Client проверьте нормальное функционирование системы, выполнив проверку логов и функции отправки сообщений
8. Запустить скрипт автоматического обновления всех контейнеров вторичного узла кластера Web Client аналогично пп.5-6.

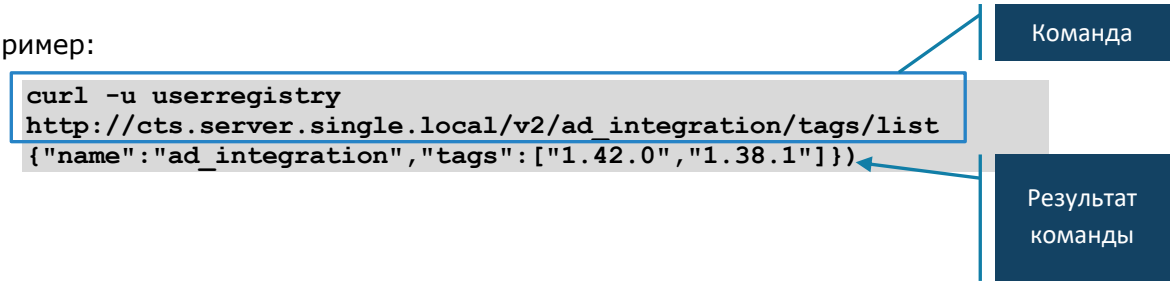
АВАРИЙНЫЕ СИТУАЦИИ ПРИ ОБНОВЛЕНИИ ИЗ ЛОКАЛЬНОГО РЕПОЗИТАРИЯ REGISTERY

Аварийные ситуации, перечисленные ниже, могут произойти в том случае, если имеется локально развернутый сервер Registery.

Ситуация 1. Отсутствия доступа к сети интернет с узла с репозитарием.

1. С узла, имеющего доступ в интернет, скачайте актуальные контейнеры с помощью скрипта по ссылке (вложение download.sh).
2. Запустите второй скрипт по ссылке (вложение upload.sh) и дождитесь окончания загрузки.
3. Сделайте тестовый запрос из консоли при помощи обращения к url и получите версии находящиеся в репозитарии:

(Пример:



Ситуация 2. Если в п.3 предыдущей операции результат команды – "no basic auth credentials".

1. Удалите файл .docker/config.json.
2. Пройдите повторную авторизацию в Docker registry.