



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ»**

РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА

RU.33654484.0004-02 91 02

Листов 23

СОДЕРЖАНИЕ

1 Введение.....	3
1.1 Область применения.....	3
1.2 Краткое описание возможностей.....	3
1.3 Уровень подготовки администратора.....	3
2 Назначение и условия работы кластера высокой доступности СКДПУ.....	5
2.1 Назначение кластера высокой доступности СКДПУ.....	5
2.2 Требования к техническим и программным средствам.....	5
2.3 Требования к аппаратному обеспечению.....	5
2.4 Требования к программному обеспечению.....	6
3 Подготовка к работе.....	7
4 Настройка кластера высокой доступности СКДПУ.....	8
5 Запуск кластера.....	10
6 Прекращение работы/перезапуск кластера высокой доступности.....	11
7 Изменение параметров сети кластера.....	12
8 Замена неисправного узла.....	13
9 Восстановление неисправного тома.....	14
10 Проверка работоспособности режима высокой доступности.....	15
10.1 Переключение с ведущего узла на ведомый (программное).....	15
10.2 Переключение с ведущего узла на ведомый (аппаратное).....	15
10.3 Сбой, обнаруженный на ведущем узле.....	16
10.4 Сбой, обнаруженный на ведомом узле.....	16
10.5 Разрыв связи между двумя узлами.....	17
11 Действия в нештатных ситуациях.....	19
11.1 Восстановление после неустранимой ошибки (технология обеспечения высокой доступности СКДПУ заблокирована).....	19
11.2 Отказы сети и состояние расщепления «Split-Brain».....	19
Перечень сокращений.....	21
Перечень таблиц.....	22
История изменений.....	23

1 ВВЕДЕНИЕ

1.1 Область применения

Настоящий документ предназначен для администраторов, осуществляющих администрирование ИТ-инфраструктуры в части настройки и эксплуатации кластера высокой доступности СКДПУ.

В настоящем документе приводится подробное описание действий, необходимых для настройки кластера высокой доступности СКДПУ и поддержки его функционирования.

1.2 Краткое описание возможностей

Кластер высокой доступности СКДПУ обеспечивает выполнение следующих функции:

- Обеспечение высокой доступности - бесперебойной работы СКДПУ посредством резервного или «активного»/«пассивного» кластера на два устройства, тем самым предоставляется доступ к целевым устройствам и веб-консоли, а также записи сеансов в ситуациях, когда основное устройство по той или иной причине недоступно;
- Автоматический перенос нагрузки на второй (ведомый) узел кластера – за счет того, что два узла СКДПУ в кластере используют один виртуальный IP-адрес, при этом фактические IP-адреса пользователям неизвестны;
- Зеркалирование данных конфигурации, журналов подключений, файлов, содержащих записи сеансов, а также файлов конфигурации СКДПУ на втором (ведомом) узле кластера с помощью устройства DRBD (Distributed Replicated Block Device);
- Уведомление по электронной почте администратора СКДПУ при следующих событиях:
 - Служба переключилась в режим сниженной производительности (переключение на ведомый узел);
 - Ведомый узел недоступен;
 - Обнаружена аномалия (например, недоступна служба);
 - Завершилась синхронизация диска.



Кластер высокой доступности СКДПУ типа «активный»/«пассивный» не поддерживает балансировку нагрузки!

1.3 Уровень подготовки администратора

Администратор должен обладать следующими знаниями:

- Системное администрирование ОС Windows/Linux и активного сетевого оборудования;
- Базовые знания сетевых протоколов;
- Администрирование СКДПУ и умение с его помощью реализовывать корпоративную политику безопасности, в части относящейся к информационному обмену;

- Знание и соблюдение требований конфиденциальности (секретности) при проведении работ.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ РАБОТЫ КЛАСТЕРА ВЫСОКОЙ ДОСТУПНОСТИ СКДПУ

2.1 Назначение кластера высокой доступности СКДПУ

Кластер высокой доступности СКДПУ предназначен для обеспечения бесперебойной работы СКДПУ посредством резервного или «активного»/«пассивного» кластера на два аппаратных устройства, для непрерывного предоставления доступа к целевым устройствам и веб-консоли, а также для записи сеансов.

2.2 Требования к техническим и программным средствам

Минимальные характеристики программного и аппаратного обеспечения для развертывания сервера СКДПУ см. [таблица 1](#).

Таблица 1 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	интерфейс для подключения к LAN
ОС	ОС Astra Linux 1.6 Special Edition
Веб-сервер	HTTP Apache 2.4
База данных	СУБД PostgreSQL версии 9.6
Брокер сообщений	RabbitMQ версии 3.6
Другое ПО	Интерпретаторы языка программирования Python 2.7, Python 3.5
	Библиотеки Python, обеспечивающие удовлетворение зависимостей для *.py части ПО

2.3 Требования к аппаратному обеспечению

АРМ пользователя СКДПУ должно быть оборудовано компьютером, обладающим следующим характеристиками:

Таблица 2 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ

Компонент	Описание
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	Интерфейс для подключения к LAN
Разрешение экрана	От 1280x1024

Режим кластера высокой доступности предназначен для эксплуатации только на аппаратных платформах, в рамках виртуальных машин его эксплуатация не поддерживается. Система предполагает, что 2 узла кластера расположены на отдельно стоящих аппаратных серверах, связанных cross-кабелем Ethernet между интерфейсами eth1 на скорости не менее 100мбит/с.

2.4 Требования к программному обеспечению

Для подключения к СКДПУ не требуется установка специализированного программного обеспечения, обращение осуществляется с APM пользователя по протоколу SSH.

3 ПОДГОТОВКА К РАБОТЕ

Перед настройкой кластера необходимо выполнить следующие действия:

- Настроить IP-подсеть для узлов кластера: ведущий и ведомый узлы должны входить в одну и ту же IP-подсеть в физической сети синхронизации;
- Рабочая подсеть и подсеть синхронизации не должны совпадать или включать друг-друга.

Система резервирует интерфейс `eth1` для использования в качестве интерфейса синхронизации в режиме кластера высокой доступности. Другие интерфейсы для синхронизации использовать не получится.

Для двух узлов кластера задать статичные IP-адреса на рабочем интерфейсе и интерфейсе синхронизации.

Настроить ОС, в частности файлы `etc/hosts` и `etc/network/interfaces` с помощью веб-интерфейса или сценария установки СКДПУ, приведенном в документе RU.33654484.0004-02 91 03 во избежание рассинхронизации с файлами конфигурации в реплицированной файловой системе. Подсистема кластера высокой доступности различает хосты в рамках кластера по `hostname` – правильно настроенные узлы, составляющие кластер высокой доступности должны отзываться на разные имена `host'ов`.



Версии и номера сборок СКДПУ у обоих узлов должны быть идентичны.

В ситуации, когда режим кластера высокой доступности настраивается на системе уже бывшей в работе, настоятельно рекомендуется выполнить процедуру резервного копирования внесенных настроек и накопленных данных.

При проектировании кластерной конфигурации настоятельно рекомендуется использовать режим удаленного сетевого хранилища, для минимизации расходов на объем хранения на аппаратных ресурсах хостов кластера и времени на синхронизацию.

4 НАСТРОЙКА КЛАСТЕРА ВЫСОКОЙ ДОСТУПНОСТИ СКДПУ

Для настройки кластера высокой доступности СКДПУ выполните следующие действия:

- Шаг 1.** Запустите два устройства, входящих в кластер в любом порядке. Устройства предоставляются в предустановленном состоянии, однако функция кластера на них не настроена;
- Шаг 2.** Для того, чтобы войти в систему в качестве привилегированного пользователя, введите команду `sudo -i`;
- Шаг 3.** Убедитесь с помощью команды Linux «date» или путем синхронизации с сервером NTP в том, что на обоих узлах кластера синхронизированы часы;
- Шаг 4.** Протестируйте отправку уведомлений для того, чтобы убедиться в том, что сервер SMTP настроен и готов к работе;
- Шаг 5.** Убедитесь в том, что для данных устройств задан статичный IP-адрес и разные имена компьютеров, в случае, если это не так, необходимо внести корректировки с помощью веб-интерфейса СКДПУ;
- Шаг 6.** Войдите в систему ведущего узла под учетной записью `wabadmin`.



- a.** Все данные на ведомом узле будут удалены без возможности восстановления!
- b.** Простой процедуры вывода узла из кластерной конфигурации намеренно не реализовано. Данная операция достигается переустановкой ОС, ПО и импортом сохраненной резервной копии настроек и данных.
- c.** Применение механизма реплицирования посредством DRBD не рекомендовано на системах, реализуемых на базе виртуальных машин.

- Шаг 7.** Выполните следующую команду:

```
sudo -i WABHASetup
Slave IP:
HA Virtual IP:
HA Virtual netmask:
HA Notification mail address:
```

...

где, необходимо указать следующие значения:

Slave IP

IP-адрес ведомого узла кластера;

HA Virtual IP

виртуальный IP-адрес, по которому будет осуществляться доступ к кластеру высокой доступности;

HA Virtual netmask

маска подсети;

HA Notification mail address

адрес электронной почты, на который будут направляться уведомления.

Шаг 8. После выполнения настройки кластера высокой доступности на адрес электронной почты будет отправлено уведомление следующего вида, содержащее параметры для запуска кластера высокой доступности:

```
Тема: [WAB] - The WAB HA has been configured
```

```
This notification sums up your HA configuration. Initial MASTER  
node: ... Initial SLAVE node: ...HA Virtual ip: ...
```

5 ЗАПУСК КЛАСТЕРА

Для запуска кластера высокой доступности необходимо обратиться к виртуальному IP-адресу, указанному в уведомлении (см. раздел [Настройка кластера высокой доступности СКДПУ](#)).

6 ПРЕКРАЩЕНИЕ РАБОТЫ/ПЕРЕЗАПУСК КЛАСТЕРА ВЫСОКОЙ ДОСТУПНОСТИ



1. Все работы по обслуживанию кластера высокой доступности должны выполняться на ведущем узле!
2. Для предотвращения нежелательного переключения, рекомендуется остановку и запуск кластера начинать с резервного узла.

Для прекращения работы кластера высокой доступности необходимо выполнить следующую команду:

```
sudo /etc/init.d/wabha stop
```

Для перезапуска кластера высокой доступности необходимо выполнить следующую команду:

```
sudo /etc/init.d/wabha restart
```

Для запуска кластера высокой доступности необходимо выполнить следующую команду:

```
sudo /etc/init.d/wabha start
```



Команды `stop`, `restart` и `start` применимы только к локальному узлу.

Для проверки текущего состояния узла используйте следующую команду:

```
# sudo /etc/init.d/wabha status
```

7 ИЗМЕНЕНИЕ ПАРАМЕТРОВ СЕТИ КЛАСТЕРА



Все операции по обслуживанию кластера должны выполняться на ведущем узле!

После настройки СКДПУ в режиме высокой доступности параметры сети, например, IP-адреса, становятся недоступными для редактирования через интерфейс пользователя.

Поскольку диски на обоих узлах синхронизированы через сеть, необходимо подключиться к ведущему узлу через SSH и выполнить следующую команду:

```
# screen - sudo -i WABNASetup -reconfigure_hosts
```

8 ЗАМЕНА НЕИСПРАВНОГО УЗЛА



Все операции по обслуживанию кластера должны выполняться на ведущем узле!

При замене узла сначала необходимо отключить неисправное устройство и запустить ведомый узел кластера СКДПУ. Обязательно необходимо задать для него такой же статичный IP-адрес, как и для неисправного узла, а затем ввести на рабочем узле следующую команду:

```
# WABHSetup -configure_new_slave
```

9 ВОССТАНОВЛЕНИЕ НЕИСПРАВНОГО ТОМА



Все операции по обслуживанию кластера должны выполняться на ведущем узле!

В случае ошибки целостности файловой системы, выявляемой по сообщениям ядра, например, `File system is now read-only due to the potential of on-disk corruption. Please run fsck.ocfs2 once the file system is unmounted`, выполните следующие действия:

Шаг 1. Введите команду

```
sudo -i WABHAInitd -force stop
```

для того, чтобы выключить режим высокой доступности на обоих узлах, начиная с ведомого;

Шаг 2. Убедитесь в том, что с обоих узлов удалена общая файловая система:

```
sudo -i umount /var/wab
```

Шаг 3. Отключите DRBD на ведомом узле:

```
sudo -i drbdadm secondary wab
```

Шаг 4. Включите DRBD на ведущем узле:

```
sudo -i drbdadm primary wab
```

Шаг 5. На ведущем узле выполните следующую команду:

```
sudo -i fsck.ocfs2 -y -f /dev/drbd1  
  
slave_node# WABHAInitd -force stop  
master_node# WABHAInitd -force stop
```

10 ПРОВЕРКА РАБОТОСПОСОБНОСТИ РЕЖИМА ВЫСОКОЙ ДОСТУПНОСТИ

Чтобы проверить, насколько эффективно функция высокой доступности выполняет восстановление после различных ошибок, рекомендуется перед развертыванием данного решения провести следующие тесты.

В качестве примера, ведущий узел будем обозначать как *WabA*, а ведомый — как *WabB*.

10.1 Переключение с ведущего узла на ведомый (программное)

Для проверки переключения с ведущего узла на ведомый необходимо:

Шаг 1. Выключить режим высокой доступности на ведущем узле:

```
WabA# /etc/init.d/wabha stop
```

Возможны две ситуации:

- Ведомый узел обнаружит аномалию, в этом случае уведомление будет иметь следующий вид: [WAB] - WAB HA 'Master' WabA error detected by the WabB! (HA_MASTER_FAULT) Reason: Service unreachable on master node!
- Произойдет переключение на ведомый узел, в этом случае уведомление будет иметь следующий вид: the [WAB] - WAB HA 'Master' WabB is online

Шаг 2. Перезапустить режим высокой доступности на ведущем узле, и он станет новым ведомым узлом:

```
WabA# /etc/init.d/wabha start
```

При этом будет выдано следующее уведомление: the [WAB] - WAB HA 'Slave' WabA is online

10.2 Переключение с ведущего узла на ведомый (аппаратное)

Для проверки переключения с ведущего узла на ведомый необходимо:

Шаг 1. Физически выключить ведущий узел путем отключения кабеля питания.

Возможны две ситуации:

- Ведомый узел обнаружит аномалию, в этом случае уведомление будет иметь следующий вид: [WAB] - WAB HA 'Master' WabA error detected by the WabB! (HA_MASTER_FAULT) Reason: Service unreachable on master node!
- Произойдет переключение на ведомый узел, в этом случае уведомление будет иметь следующий вид: the [WAB] - WAB HA 'Master' WabB is online

- Шаг 2.** Перезапустить режим высокой доступности на ведущем узле, и он станет новым ведомым узлом:

```
WabA# /etc/init.d/wabha start
```

При этом будет выдано следующее уведомление: the [WAB] - WAB HA 'Slave' WabA is online.

10.3 Сбой, обнаруженный на ведущем узле

Для проверки обнаружения сбоя на ведущем узле необходимо:

- Шаг 1.** Создать на ведущем узле условие, которое он воспримет как сбой, например, заблокировать работу определенной веб-службы:

```
WabA# cd /etc/opt/wab/apache2
WabA# mv ssl.crt ssl.crt.tmp
WabA# /etc/init.d/wabgui restart
```

Возможны две ситуации:

- Оба узла обнаружат сбой (недоступность пользовательского интерфейса), при этом будут выданы следующие уведомления:
[WAB] - WAB HA master WabA error detected by WabA Reason: Wabgui service isn't responding and we couldn't restart it!
[WAB] - WAB HA master WabA error detected by WabB Reason: Wabgui service unreachable on master node!
- Произойдет переключение на ведомый узел, а ведущий узел будет назначен ведомым, при этом будут выданы следующие уведомления:
The [WAB] - WAB HA master WabB is online
The [WAB] - WAB HA Slave WabA is online

- Шаг 2.** Устраните сбой, после чего узел *WabA* должен стать ведущим:

```
WabA# mv /etc/opt/wab/apache2/ssl.crt.tmp /etc/opt/wab/apache2/ssl.crt
```

10.4 Сбой, обнаруженный на ведомом узле

Для проверки обнаружения сбоя на ведомом узле необходимо:

- Шаг 1.** Физически выключить ведомый узел путем отключения кабеля питания. В результате ведущий узел должен обнаружить аномалию, при этом будет выдано уведомление:

[WAB] - The WAB HA slave WabB is no longer connected to master WabA! Master data replication isn't working.

- Шаг 2.** В результате, репликация данных прервана, но том по-прежнему продолжает работать в режиме сниженной производительности. Для разрешения данной

ситуации необходимо перезагрузить ведомый узел, при этом будет выдано уведомление:

```
[WAB] - The WAB HA slave WabB is online
```



Если объем данных на ведущем узле со сниженной производительностью пренебрежимо мал, например, нет данных о новых сеансах, синхронизация выполняется мгновенно, если нет, то отправляется уведомление:

```
[WAB] - The WAB HA cluster synchronization completed! Both nodes data are now fully synchronized.
```

10.5 Разрыв связи между двумя узлами

Для проверки разрыва связи между двумя узлами необходимо:

Шаг 1. Отключить один из сетевых узлов или создать условия, препятствующие взаимодействию двух узлов СКДПУ, например, с помощью таблиц IP-адресов:

```
WabA# iptables -A INPUT -s IpWabB -j DROP; iptables -A OUTPUT -d IpWabB -j DROP
```

```
WabB# iptables -A INPUT -s IpWabA -j DROP; iptables -A OUTPUT -d IpWabA -j DROP
```

Возможны три ситуации:

a. Оба узла обнаружат сбой. Основной узел продолжит работу в режиме сниженной производительности, при этом будут выданы уведомления:

```
[WAB] - The WAB HA slave WabB is no longer connected to master WabA! Master data replication isn't working.
```

```
[WAB] - The WAB HA master WabA error detected by sparewab2.ifr.lan Reason: Host does not respond to ping..
```

b. Ведомый узел предположит, что ведущий узел выключен, и переключится в режим ведущего узла, который, в свою очередь, также будет работать в режиме сниженной производительности, при этом будут выданы следующие уведомления:

```
[WAB] - The WAB HA master WabB is online
```

```
[WAB] - The WAB HA slave WabA is no longer connected to master WabB! Master data replication isn't working
```

c. Общий том начнет передавать на узлы разные данные. Наиболее вероятная причина заключается в том, что один из узлов не подключен к сети. В этом

случае следует повторно подключить узлы СКДПУ или, если использовались таблицы IP-адресов:

```
WabA# iptables -F
```

```
WabB# iptables -F
```

При этом будет выдано следующее уведомление:

```
[WAB] - The WAB HA disks diverged (split brain detected)
The WAB HA drbd shared volume is now disconnected. Both
peers had lost connexion to each other and both switched to
master... Now data couldn't be synced cleanly, you'll have
to manually discard one node changes. Once you figure out
which node is really out of date, you'll have to type on
a root shell: failling_node
```

```
#drbdadm secondary wab failling_node # drbdadm--discard-
my-data connect wab recent_node
```

```
#drbdadm connect wab both_node # /etc/init.d/wabha
start
```

Шаг 2. Для разрешения ситуации необходимо следовать инструкциям, содержащимся в сообщении электронной почты:

```
WabB# drbdadm secondary wab
WabB# drbdadm -- --discard-my-data connect wab
WabA# drbdadm connect wab
WabA# /etc/init.d/wabha start
WabB# /etc/init.d/wabha start
```

При этом будет выдано следующее уведомление:

```
[WAB] - The WAB HA master WabA is online Notification:
[WAB] - The WAB HA slave WabB is online
```

11 ДЕЙСТВИЯ В НЕШТАТНЫХ СИТУАЦИЯХ

11.1 Восстановление после неустранимой ошибки (технология обеспечения высокой доступности СКДПУ заблокирована)

Если технология обеспечения высокой доступности обнаруживает неисправность, которую не может устранить автоматически (путем перезапуска соответствующей службы), процедура переключения блокируется.

Система отправляет уведомление об обнаружении неустранимой ошибки, создает файл блокировки и отключается.

Наличие данного файла предотвращает запуск технологии высокой доступности и в течение неопределенного времени препятствует попыткам решить данную проблему.

После устранения неполадки файл блокировки необходимо удалить вручную с помощью команды:

```
affected_node# rm /etc/opt/wab/ha/fatal_error
```

11.2 Отказы сети и состояние расщепления «Split-Brain»

В случае если узлы подключены к сети, но не друг к другу, например, если отсоединен сетевой кабель, соединяющий коммутаторы, пассивный узел становится ведущим – это стандартная процедура, поскольку с точки зрения данного узла ведущий узел больше не активен.

Таким образом, в конфигурации появляются два ведущих узла, и данные в общем томе начинают «расщепляться».

При восстановлении соединения устройство DRBD общего тома обнаружит состояние расщепления («Split-Brain») и кластер прекратит работу. Поскольку узлы кластера некоторое время работали независимо друг от друга, их данные становятся несовместимы, требуется вмешательство администратора.

Для того, чтобы устранить расщепление администратор должен выбрать узел с наиболее актуальными данными. В уведомлении администратору будет представлен список последних изменений файлов на двух экземплярах СКДПУ.

Существует три возможных сценария развития событий:

1. Отказ длился недолго, и в этот период узлы не использовались (не создавались сеансы, не добавлялись учетные записи и т.п.): в этом случае администратор может выбрать любой из узлов в качестве эталонного ведущего узла;
2. Отказ продлился недолго и/или использовался только один узел (на это указывает наличие файлов сеансов и более поздних дат внесения изменений только на одном из узлов): администратор должен выбрать этот узел в качестве нового эталонного ведущего узла;
3. Отказ был сложным, и оба узла использовались параллельно (такая ситуация маловероятна, но может быть связана с серьезным сбоем сети): администратор должен выбрать один из узлов в качестве нового эталонного ведущего узла (узел с наибольшим

количеством изменений) и создать резервную копию данных с другого узла. После этого необходимо вручную импортировать данные в новый ведущий узел. После того, как эталонный ведущий узел будет выбран, необходимо выполнить действия по восстановлению кластера:

```
outdated_node# drbdadm secondary wab
outdated_node# drbdadm -- --discard-my-data connect wab
ref_master# drbdadm connect wab
both_nodes# /etc/init.d/wabha start
```

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

DRBD	Distributed Replicated Block Device — программная система, обеспечивающая синхронизацию (RAID 1) между локальным блочным устройством и удалённым.
IP	Internet Protocol (IP, досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека TCP/IP.
LAN	Local Area Network (локальная компьютерная сеть)
NTP	Network Time Protocol — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.
SSH	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
APM	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ.....	5
Таблица 2 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ.....	5

