Автоматическое развертывание кластерного исполнения AxelNAC

В данной статье приведено описание развертывания кластерного исполнения AxelNAC с помощью утилиты Ansible.

Как работает кластерное исполнение AxelNAC

Кластерное исполнение AxelNAC может состоять из нечетного количества узлов и представляет собой отказоустойчивый кластер. **Отказоустойчивые кластеры** — это группы серверов, которые спроектированы в соответствии с методиками обеспечения высокой доступности и которые гарантируют работу кластера в целом при отказе одного или нескольких его узлов. Без кластеризации, если сервер, на котором запущен AxelNAC, выходит из строя, система будет недоступна до тех пор, пока не будет устранена неполадка на сервере. Отказоустойчивый кластер исправляет эту ситуацию, обнаруживая аппаратные и программные сбои и немедленно перенаправляя трафик на другие узлы, не требуя вмешательства администратора. Кластер AxelNAC может содержать до 9 узлов в разных L2-сегментах, такой кластер называется катастрофоустойчивым.

Данный кластер работает по принципу **active-active**, т.е. один или несколько узлов выступают в качестве балансировщика, который осуществляет прием и распределение запросов между собой и оставшимися узлами кластера. В случае выхода из строя сервера, он исключается из балансировки. В случае выхода из строя узла, выполняющего роль балансировщика, эта роль и кластерный адрес передаются другому узлу кластера.

Кластер AxelNAC будет сохранять полную работоспособность при соблюдении обязательного кворума — более 50% узлов кластера должны быть доступны. При потере кворума, AxelNAC сохраняет частичную работоспособность, переходя в режим только для чтения. В данном режиме изменяется логика основных элементов системы:

- **Аутентификация RADIUS MAC:** продолжит работу и будет возвращать атрибуты RADIUS, связанные с ролью, зарегистрированной в базе данных. Если к этому устройству можно применить фильтры VLAN или RADIUS, они будут применены, но любое изменение роли не будет сохранено;
- **Аутентификация RADIUS 802.1X:** продолжит работу, и если включена функция **Dot1x переопределяет роль с портала**, она будет вычислять роль с использованием доступных источников аутентификации, но не будет сохранять ее в базе данных в конце запроса. Если этот параметр отключен, он будет вести себя так же, как аутентификация по MAC-адресу. Фильтры VLAN и RADIUS по-прежнему будут применяться к подключениям, но любое изменение роли не будет сохранено. Если какие-либо из ваших источников аутентификации являются внешними (LDAP, AD, RADIUS, ...), они должны быть доступны для успешного выполнения запроса:
  - Аутентификация существующих в системе пользователей по протоколам PEAP и EAP-TLS будет выполняться в штатном режиме;
  - Реаутентификация существующих в системе пользователей по таймеру, установленному на коммутаторе, будет выполняться в штатном режиме;
  - Реаутентификация существующих в системе пользователей по периоду реаутентификации, установленному в системе, будет выполняться в штатном режиме;
  - Для новых пользователей, соответствующих правилам, установленным в системе, будет выполняться аутентификация, но новая запись в базе данных системы создаваться не будет.
- **Captive-портал:** будет остановлен. Для пользователей будет отображено сообщение о том, что система в настоящее время находится в режиме обслуживания.
- **Прослушиватели DHCP:** будут отключены, входящие DHCP-пакеты не будут сохраняться в базе данных. Firewall SSO также будет отключен.
- **Веб-интерфейс AxelNAC:** по-прежнему будет доступен в режиме только для чтения для всех разделов и в режиме чтения-записи для раздела конфигурации.

Для реализации данного способа вам потребуется нечетное количество установленных серверов AxelNAC (от трех до девяти). Серверы должны быть расположены в пределах следующих ограничений задержки (требование для **MariaDB Galera** — службы синхронизации БД кластера):

- для небольших развертываний (от трех до пяти узлов) между узлами кластера допускается задержка не более 75 мс;
- для больших развертываний (семь узлов) допускается задержка между узлами кластера не более 50 мс.

Скрипты для сборки кластерной инсталляции необходимо запускать на отдельной виртуальной машине с сетевым доступом ко всем узлам, которая не будет использоваться в кластере. После окончания сборки ее можно будет удалить.

Подготовка к развертыванию кластерного исполнения

Для того чтобы произвести автоматическое развертывание кластерного исполнения AxelNAC, необходимо выполнить следующие подготовительные этапы:

Первичная настройка сетевого интерфейса на узлах

Для начала развертывания кластера необходимо настроить сетевые интерфейсы на каждом из узлов. Для этого выполните следующие шаги:

Шаг 1. Подключитесь к узлу через платформу виртуализации и задайте адрес на сетевом интерфейсе:

nano /etc/network/interfaces

Шаг 2. Измените файл конфигурации на каждом узле по данному примеру:

```
auto <имя_сетевого_интерфейса>
 iface <имя_сетевого_интерфейса> inet static
    address <ip-address>
    netmask <net mask>
    gateway <gateway ip-address>
```

Шаг 3. Для применения конфигурации перезапустите службу сети, используя следующую команду:

```
 systemctl restart networking
```

Предварительная настройка мастер-узла AxelNAC

Для следующего этапа необходимо сконфигурировать мастер-узел. Для этого выполните следующие шаги:

Шаг 1. Подключитесь к узлу по адресу **https://<ip-address>:1443** — откроется веб-конфигуратор AxelNAC.

Шаг 2. Выберите интерфейс, который будет использоваться для управления. На странице его настройки в поле **Тип** выберите значение **Управление** и переместите переключатель **Высокая доступность** в состояние **включено**.

Шаг 3. Пройдите все оставшиеся этапы настройки в веб-конфигураторе.

Предварительная настройка ведомых узлов AxelNAC

После того как мастер-узел предварительно сконфигурирован, можно приступить к преднастройке ведомых узлов кластера. Для этого выполните следующие шаги:

Шаг 1. Подключитесь к ведомому узлу по адресу **https://<ip-address>:1443** — откроется веб-конфигуратор AxelNAC.

Шаг 2. Выберите интерфейс, который будет использоваться для управления. На странице его настройки в поле **Тип** выберите значение **Управление** и переместите переключатель **Высокая доступность** в состояние **включено**.

Необходимо пройти только первый шаг веб-конфигуратора, после чего вы можете закрыть страницу.

Процесс сборки кластерной инсталляции

- Рекомендуется выполнять сборку с помощью консольной утилиты **tmux**, которая позволит вам сохранить работу при отключении SSH;
- Вся информация о процессах сборки записывается в журнал /usr/local/pf/addons/tech-support-utils/ansible-cluster-tools/ansible.log. При выходе из консоли, вы можете продолжить отслеживание процесса, выведя содержимое этого журнала любым удобным способом.

Шаг 1. Перейдите в каталог **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools/**. Запустите скрипт генерации шифрованных паролей для Ansible с помощью указанной ниже команды и введите пароли, которые вы будете использовать для работы с кластером:

- Пароль от пользователя **anac**, который используется для доступа к управлению системой через **SSH**. Данный пароль будет использоваться для переменной **ansible_ssh_pass** в конфигурационном файле **Ansible**;
- Пароль для доступа к службе репликации баз данных. Данный пароль будет использоваться для переменной **db_pfcluster_pass** в конфигурационном файле **Ansible**. После сборки кластера он будет указан в переменной **galera_replication_password** из блока **[active_active]** в конфигурационном файле **/usr/local/pf/conf/pf.conf**;
- Пароль для доступа к службе синхронизации конфигураций узлов кластера. Данный пароль будет использоваться для переменной **web_srv_pass** в конфигурационном файле **Ansible**. После сборка кластера он будет указан в переменной **pass** из блока **[webservices]** в конфигурационном файле **/usr/local/pf/conf/pf.conf**.

```
bash init-env.sh
```

Для упрощения процесса обновления кластера в будущем, рекомендуется сохранить эти пароли.

Шаг 2. Откройте конфигурационный файл **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools/inventory/group_vars/all.yml** и для переменной **type** укажите тип инсталляции (может принимать значения **normal** и **l3** (для **multizone**)).

Шаг 3. Заполните инвентарный файл для запуска развертывания. Для этого в директории **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools/inventory** отредактируйте:

- для кластерной инсталляции с одним VIP-адресом файл **normal**;
- для кластерной инсталляции с несколькими VIP-адресами файл **multizone**.

Значение **hostname_узла_n** должно строго совпадать с именем хоста этого узла кластера, указанном при первичной настройке, иначе значения будут перезаписаны при сборке.

Пример заполненного инвентарного файла **normal**:

```
[cluster:children]
dc1

[dc1]
hostname_узла_1 ansible_host=IP-адрес_узла_1 vip=VIP-адрес_кластера master=true
hostname_узла_2 ansible_host=IP-адрес_узла_2
hostname_узла_3 ansible_host=IP-адрес_узла_3
```

Пример заполненного инвентарного файла **multizone**:

```
[cluster:children]
dc1
dc2

[dc1]
hostname_узла_1 ansible_host=IP-адрес_узла_1 vip=VIP-адрес_dc1 master=true
hostname_узла_2 ansible_host=IP-адрес_узла_2
hostname_узла_3 ansible_host=IP-адрес_узла_3

[dc2]
hostname_узла_4 ansible_host=IP-адрес_узла_4 vip=VIP-адрес_dc2
hostname_узла_5 ansible_host=IP-адрес_узла_5
```

Шаг 4. Выполните проверку доступности узлов будущего кластера. Для этого перейдите в директорию **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools/** и выполните команду:

```
ansible -i inventory/normal all -m ping
```

Шаг 5. Выполните ротацию инвентарных файлов и выгрузку журнала **ansible.log** с помощью следующей команды:

```
bash chk.sh [inventory:normal|multizone] clean
```

При выполнении этой команды журнал **ansible.log** очистится и все записи будут перенесены в файл вида **ansible-current-date-time.log** (например: **ansible-2026-06-01_12:12:28.log**)

Шаг 6. Запустите сборку кластера из этой же директории, выполнив следующую команду:

```
ANSIBLE_CONFIG=./ansible.cfg ansible-playbook -i inventory/<normal|multizone> playbooks/create-cl.yml -vv -Kb
```

При выполнении команды система запросит пароль от пользователя **root**. Данный пароль в открытом виде не поставляется. Он вводится сетевыми инженерами Axel PRO или партнерами, выполняющими развертывание кластерной инсталляции.

Работа с плейбуком

Описание стадий

Плейбук для автоматической сборки кластерного исполнения разделен на стадии, по которым можно запускать/повторять отдельно серию задач при необходимости. Для этого используются теги:

Тег	Описание
init	• Вносит необходимые правки в **sysctl**; • Вносит изменения в **hostname** согласно инвентарному файлу и обновляет записи **/etc/hosts**; • Создает пользователя реплики; • Перезапускает узлы.
galera1	• Формирует конфигурационные файлы кластера; • Перезапускает службы на мастер-узле.
galera2	• Переводит мастер-узел в режим создания кластера; • Отключает службу **iptables**.
galera3	• Синхронизирует конфигурационные файлы ведомых узлов с мастер-узлом.
galera4	• Скачивает конфигурационные файлы для проверки их идентичности.
galera5	• Перезагружает службы на узлах.
galera6	• Возвращает мастер-узел в обычный режим; • Включает службу **galera-autofix**.
galera7	• Перезагружает службы на узлах; • Перезагружает все узлы.

Дополнительные варианты запуска плейбука

Плейбук может быть запущен в различных режимах. Ниже приведено описание каждого из дополнительных режимов с примерами:

Запуск конкретного шага:

ANSIBLE_CONFIG=./ansible.cfg ansible-playbook -i inventory/<**normal|multizone**> playbooks/create-cl.yml -t <ТЕГ_СТАДИИ>

Такой командой вы можете запустить определенную стадию плейбука (например, если во время исполнения плейбука произошла остановка операций, или пришлось прервать его работу вручную).

Запуск конкретного шага на конкретном узле:

ANSIBLE_CONFIG=./ansible.cfg ansible-playbook -i inventory/<**normal|multizone**> playbooks/create-cl.yml -t <ТЕГ_СТАДИИ> -l <IP-АДРЕС_УЗЛА>

Такой командой вы можете запустить определенную стадию плейбука на определенном узле.

Запуск нескольких шагов:

ANSIBLE_CONFIG=./ansible.cfg ansible-playbook -i inventory/<**normal|multizone**> playbooks/create-cl.yml -t <ТЕГ_СТАДИИ>,<ТЕГ_СТАДИИ>,<ТЕГ_СТАДИИ>

Такой командой вы можете запустить определенные стадии плейбука.

Проверка работоспособности кластера

Для того чтобы проверить работоспособность кластера необходимо открыть веб-интерфейс AxelNAC. После ввода учетных данных откроется раздел **Статус → Система**, в котором можно будет увидеть подключенные узлы.

IP-адреса всех узлов кластера также должны быть отображены в файле **/usr/local/pf/conf/cluster.conf** и соответствовать содержимому, указанному в файле **create-cl.yml**.

Пример файла для кластера с двумя VIP-адресами из 5 узлов:

```
# MULTI ZONE CLUSTER CFG
[general]
multi_zone=enabled

[dc1 CLUSTER]
management_ip=10.21.209.41

[dc1 CLUSTER interface <имя_сетевого_интерфейса>]
ip=10.21.209.41

[dc1 deb-to-astra-dc1-1]
management_ip=10.21.209.36

[dc1 deb-to-astra-dc1-1 interface <имя_сетевого_интерфейса>]
ip=10.21.209.36
```

[dc1 deb-to-astra-dc1-2]
management_ip=10.21.209.37

[dc1 deb-to-astra-dc1-2 interface <имя_сетевого_интерфейса>]
ip=10.21.209.37

[dc1 deb-to-astra-dc1-3]
management_ip=10.21.209.38

[dc1 deb-to-astra-dc1-3 interface <имя_сетевого_интерфейса>]
ip=10.21.209.38

[dc2 CLUSTER]
management_ip=10.21.209.42

[dc2 CLUSTER interface <имя_сетевого_интерфейса>]
ip=10.21.209.42

[dc2 deb-to-astra-dc2-1]
management_ip=10.21.209.39

[dc2 deb-to-astra-dc2-1 interface <имя_сетевого_интерфейса>]
ip=10.21.209.39

[dc2 deb-to-astra-dc2-2]
management_ip=10.21.209.40

[dc2 deb-to-astra-dc2-2 interface <имя_сетевого_интерфейса>]
ip=10.21.209.40

Также статусы можно проверить с помощью консоли управления. Для этого подключитесь по**SSH** к любому узлу и выполните следующую команду:

/usr/local/pf/bin/pfcmd service pf status

Еще один способ проверки — проверка статусов через MySQL. Чтобы просмотреть все активные узлы в кластере перейдите в оболочку SQL и выполните следующую команду:

show status like '%wsrep%';

Активные узлы кластера будут перечислены в строке **wsrep_incoming_addresses**.

ID статьи: 1876
Последнее обновление: 1 июн., 2026
Обновлено от: Егоров В.
Ревизия: 46
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.2.0 -> AxelNAC. Руководство по настройке кластера -> Автоматическое развертывание кластерного исполнения AxelNAC
https://docs.axel.pro/entry/1876/