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:

- **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;
- **RADIUS 802.1X:** продолжит работу, и если включена функция **Перерасчет роли Dot1x 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;
- **Captive-портал:** будет остановлен. Для пользователей будет отображено сообщение о том, что система в настоящее время наблюдаются неполадки.
- **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):

- 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.

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 eth0
 iface eth0 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**.

Установка и конфигурация утилиты Ansible

Для того, чтобы автоматизировать настройку кластера, необходимо установить утилиту **Ansible** на виртуальную машину с сетевым доступом ко всем узлам, которая не будет использоваться в кластере и сконфигурировать ее:

Шаг 1. В интерфейсе командной строки выполните следующую команду:

apt install ansible

Шаг 2. Обозначьте переменную конфигурации для совместимости с предустановленным в AxelNAC плейбуком, введя следующую команду:

export ANSIBLE_CONFIG=ansible.cfg

Инструменты для развертывания кластерного исполнения

Все инструменты для развертывания кластерного исполнения расположены в директории **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools**:

- **create-cl.yml** — плейбук (набор скриптов) для сборки кластера из готовых узлов AxelNAC;
- **create-local-upgrade.sh** — скрипт для создания **docker-anac-update.tar**;
- **upgrade-cl.yml** — плейбук для обновление кластера из локального архива с обновлениями;
- **ansible.cfg** — файл локальной конфигурации Ansible;
- **multizone** — пример инвентарного файла для сборки кластера с двумя мастер-узлами;
- **normal** — пример инвентарного файла для сборки кластера с одним мастер-узлом;
- **files** — дополнительные файлы для плейбуков (например архив обновления **docker-anac-update.tar**);
- **templates** — шаблоны конфигурационных файлов для кластера и hosts для узлов;
- **roles** — роль обновления;
- **encrypt.sh** — пример скрипта для получения файла **val.cry**;
- **pass.sh** — пример скрипта генерации пароля для шифрования;
- **val.cry** — пример шифрованных данных для плейбука.

Подготовка среды

При исполнении плейбука ansible использует хранилище (vault) **val.cry** для определения паролей доступа к разделам AxelNAC. Поставляемое с AxelNAC хранилище содержит стандартные для системы пароли. Если вы меняли пароли для доступа, необходимо сгенерировать хранилище с актуальными паролями. Для этого вы можете использовать скрипт **encrypt.sh**, в котором содержатся следующие поля:

- **ansible_ssh_pass** — пароль для доступа к AxelNAC по протоколу **SSH**;
- **db_pfcluster_pass** — пароль от базы данных AxelNAC. Пароль должен соответствовать следующим требованиям:
  - Не содержит ни один специальный символ из списка: **'**, **%,** **|**, **(**, **)**, /, \, а также **пробел;**
  - Длина пароля не более 16 символов.
- **web_srv_pass** — пароль от службы синхронизации конфигураций узлов кластера.

Для генерации актуального хранилища паролей выполните следующие действия:

Шаг 1. Сделайте файл **pass.sh** исполняемым, выполнив следующую команду:

chmod +x ./pass.sh

Шаг 2. Зайдите в файл **encrypt.sh** и отредактируйте находящиеся в нем значения паролей.

Шаг 3. Сгенерируйте хранилище с актуальными паролями. Для этого запустите скрипт **encrypt.sh**, используя следующую команду:

bash encrypt.sh

После выполнения команды у вас появится сгенерированный файл **val.cry**.

Запуск скрипта требует прав пользователя **sudo**, поэтому их необходимо выполнять из-под оболочки **bash**.

Шаг 5. Откройте сгенерированный файл **val.cry** и замените значения зашифрованных паролей в файле **create-cl.yml** на значения из файла **var.cry** с сохранением табуляции:

```
---
- name: (check) GET_INFO
  hosts: all
  #  serial: 7
  #  any_errors_fatal: true
  gather_facts: true
#  become: yes
#  become_user: root
  vars:
    HOST_COUNT: "{{ ansible_play_hosts | length }}"
    ansible_ssh_pass: !vault |
      $ANSIBLE_VAULT;1.1;AES256
      62643565363835666436323339326630396263383937323533656338383430613933356337653430
      65646563333765663232643636366266643631393339633 00a373935316162666663363031323663
      31663966326666623263643465383663346662613838633464646630663937353239356336353536
      38613763363437373 20a62643866373334633383830393036646339353939636666383361653831 65
      31386531366238303138393539373563313534333662386638343563386337663738
    db_pfcluster_pass: !vault |
      $ANSIBLE_VAULT;1.1;AES256
      62643565363835666436323339326630396263383937323533656338383430613933356337653430
      65646563333765663232643636366266643631393339633 00a373935316162666663363031323663
      31663966326666623263643465383663346662613838633464646630663937353239356336353536
      38613763363437373 20a62643866373334633383830393036646339353939636666383361653831 65
      31386531366238303138393539373563313534333662386638343563386337663738
    web_srv_pass: !vault |
      $ANSIBLE_VAULT;1.1;AES256
      31336437363537396461613830316333633933666131336434326238666165633834366461373137
      64353361383064666331343931303631626462393937353 70a37613435373864343039343163 9239
      63633766616437653936616534343862323363643632343866373264616364366464363663646261
      37323634626636393 50a383966383963616333306234663136353239356662366166643530663436
      33356662316233323833333261313931323032323138366438376262633465356161
```

Запуск автоматического развертывания кластерного исполнения AxelNAC

Сборка кластера с одним мастер-узлом

Для того, чтобы запустить сборку кластерного исполнения с одним мастер-узлом, выполните следующие шаги:

Шаг 1. Перенесите директорию **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools** на виртуальную машину, которая не будет использоваться в кластере.

Шаг 2. В файле **normal**, в разделе **cluster** укажите IP-адреса и имена хоста узлов в секциях **master** и **nodes**.

Шаг 3. В секции **vars** укажите от имени какого пользователя производятся действия: **ansible_user=root**.

Шаг 4. Укажите пароль для доступа к пользователю: **ansible_ssh_pass=superpassword**.

- Для доступа от имени пользователя **root** требуется настройка службы **sshd** на всех узлах, т.к. в целях безопасности доступ к пользователю **root** запрещен;
- Для запуска плейбуков от имени обычного пользователя дополнительно нужно указать ключ **-bK**, при этом дополнительно в командной строке будет запрошен пароль от пользователя **root**).

Шаг 5. Укажите виртуальный IP-адрес кластера в строке **cluster_mng_ip**.

Шаг 6. В файле **create-cl.yml** сконфигурируйте параметры проверки на соответствие.

Пример инвентарного файла

```
[cluster:children]
dc1

[dc1]
dc1-anac3-n1 ansible_host=10.31.205.87 vip=10.31.205.111 master=true
dc1-anac3-n2 ansible_host=10.31.205.119
dc1-anac3-n3 ansible_host=10.31.205.120

[cluster:vars]
####### !!!!!!!!!!!! type = 'normal' or 'l3' !!!!!!!!!!! #######
type=normal

ansible_ssh_common_args='-o StrictHostKeyChecking=no -o PasswordAuthentication=yes'
ansible_user=root/user
ansible_ssh_pass=root_pass
#ansible_ssh_pass=123123
ansible_python_interpreter="/usr/bin/python3"
# mem >= 8 Gb
mem=7944
# cpu >= 4
cpu=4
# sda.size >= 200 Gb
hdd=100
```

Сборка кластера с двумя и более мастер-узлами

Для того, чтобы запустить сборку кластерного исполнения с двумя и более мастер-узлами, выполните следующие шаги:

Шаг 1. Перенесите директорию **/usr/local/pf/addons/tech-support-utils/ansible-cluster-tools** на виртуальную машину, которая не будет использоваться в кластере.

Шаг 2. В файле **multizone**, в разделе **cluster** укажите IP-адреса узлов в секциях **master** и **nodes**.

Шаг 3. В секции **vars** укажите от имени какого пользователя производятся действия: **ansible_user=root**.

Шаг 4. Укажите пароль для доступа к пользователю: **ansible_ssh_pass=superpassword**.

- Для доступа от имени пользователя **root** требуется настройка службы **sshd** на всех узлах, т.к. в целях безопасности доступ к пользователю **root** запрещен;
- Для запуска плейбуков от имени обычного пользователя дополнительно нужно указать ключ **-bK**, при этом дополнительно в командной строке будет запрошен пароль от пользователя **root**).

Шаг 5. Укажите виртуальные IP-адреса кластера в строке **cluster_mng_ip**.

Шаг 6. В файле **create-cl.yml** сконфигурируйте параметры проверки на соответствие.

Пример инвентарного файла

```
[cluster:children]
```

```
dc1
dc2

[dc1]
dc1-anac5-n1 ansible_host=10.31.205.87 vip=10.31.205.111 master=true
dc1-anac5-n2 ansible_host=10.31.205.119
dc1-anac5-n3 ansible_host=10.31.205.120

[dc2]
dc2-anac5-n1 ansible_host=10.31.205.121 vip=10.31.205.112
dc2-anac5-n2 ansible_host=10.31.205.122

[cluster:vars]
####### !!!!!!!!!!!! type = 'normal' or 'l3' !!!!!!!!!!! #######
type=l3

ansible_ssh_common_args='-o StrictHostKeyChecking=no -o PasswordAuthentication=yes'
ansible_user=root/user
ansible_ssh_pass=root_pass
#ansible_ssh_pass=123123
ansible_python_interpreter="/usr/bin/python3"
# mem >= 8 Gb
mem=7944
# cpu >= 4
cpu=4
# sda.size >= 200 Gb
hdd=100
```

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
check	• ansible_memtotal_mb.real | int >= 7944 (проверяется MEM >8Gb); • ansible_devices.sda.size[:-5] | int >= 100 (проверяется HDD > 100Gb); • db_service_status.status.ActiveState == 'active' (проверяется работает ли MariaDB).
init	• Вносит необходимые правки в **sysctl**; • Устанавливает недостающее ПО; • Вносит изменения в **hostname** согласно инвентарному файлу и обновляет записи **/etc/hosts**; • Создает пользователя реплики; • Перезапускает узлы.
galera1	• Формирует конфигурационные файлы кластера; • Перезапускает сервисы 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 ведомые узлы.

Запуск плейбука

Плейбук может быть запущен в различных режимах. Ниже приведено описание каждого режима с примерами.

Если вы запускаете скрипт обновления с узла, который будет сейчас обновляться, необходимо после первой перезагрузки запустить команду со следующими тегами:

ansible-playbook -i normal --vault-id ./pass.sh create-cl.yml -t galera1,galera2,galera3,galera4,galera5,galera6,galera7

Стандартный запуск

ansible-playbook -i normal --vault-id ./pass.sh create-cl.yml

Такой командой вы можете запустить все шаги. Ее можно использовать, если вы запускаете плейбук с узла, не обновляемого в данный момент.

Запуск конкретного шага:

ansible-playbook -i normal --vault-id ./pass.sh 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-playbook -i normal --vault-id ./pass.sh 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-playbook -i normal --vault-id ./pass.sh create-cl.yml -t <ТЕГ_СТАДИИ>,<ТЕГ_СТАДИИ>,<ТЕГ_СТАДИИ>

Такой командой вы можете запустить определенные стадии плейбука (например, при запуске плейбука с узла, который обновляется в данный момент).

Дополнительные команды Ansible

Проверка доступа узлов

ansible -i normal all --vault-id ./pass.sh -m ping

Запуск команд на удаленных узлах

ansible -i normal all --vault-id ./pass.sh -m shell -a "/usr/local/pf/bin/pfcmd service pf restart"

Отображение информации о хосте в виде дерева

ansible -i normal all -m ansible.builtin.gather_facts --tree

Отображение информации о хосте в общем виде

ansible -b -i normal all -m gather_facts

Отображение полной информации о хосте

ansible -i normal all --vault-id ./pass.sh -m setup

Просмотр журнала ansible

ansible-playbook -i normal --vault-id ./pass.sh create-cl.yml -t init -l dc1-anac5-n1 -vvv

Возможные ошибки и пути их решения

Остановка службы mariadb

Некорректная остановка службы **maridb** не приводит к остановке выполнения плейбука и может быть проигнорирована.

Не определяется sda (HDD) и memory (RAM)

Пример вывода:

fatal: [ds-net-axelnac-01]: FAILED! => {"msg": "The task includes an option with an undefined variable. The error was: 'dict object' has no attribute 'sda'. 'dict object' has no attribute 'sda'\\n\\nThe error appears to be i

Решение:

Дальнейшие действия выполняются по усмотрению пользователя и могут повлечь за собой риски.

Выполните команду для запуска нескольких шагов, пропустив тег **check**.

ansible-playbook -i normal --vault-id ./pass.sh create-cl.yml -t init,galera1,galera2,galera3,galera4,galera5,galera6,galera7

ID статьи: 275
Последнее обновление: 4 июл., 2025
Обновлено от: Егоров В.
Ревизия: 10
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 1.2.0 -> AxelNAC. Руководство по настройке кластера -> Автоматическое развертывание кластерного исполнения AxelNAC
https://docs.axel.pro/entry/275/