Управление резервным копированием AxelNAC

В данной статье описан процесс резервного копирования и восстановления инсталляции AxelNAC.

Требования и ограничения резервного копирования

- Процесс восстановления инсталляции может быть выполнен только на одиночном сервере. Автоматическое восстановление кластера на данный момент не поддерживается;

Если вам необходимо восстановить инсталляцию, включенную в кластер, выполните восстановление одиночного узла, затем введите его обратно в кластер.

- Восстановление узла из резервной копии необходимо производить на чистой инсталляции AxelNAC той же версии;
- При восстановлении из резервной копии, узел не будет автоматически введен в домены Active Directory. Повторный ввод в домен необходимо выполнить вручную;
- Из резервной копии могут быть восстановлены следующие файлы:
  - Конфигурационные файлы, расположенные в директории **/usr/local/pf/conf/*.conf**;
  - Шаблоны страниц Captive-портала, расположенные в директории **/usr/local/pf/html/captive-portal/profile-templates/**;
  - Сертификаты, расположенные в директориях **/usr/local/pf/conf/ssl/*** и **/usr/local/pf/raddb/certs/***;
  - Дополнительные конфигурационные файлы службы iptables (**/usr/local/pf/conf/iptables-input*.conf.inc** и **/usr/local/pf/conf/ip6tables-input-management.conf.inc**).
- Ниже приведен список конфигурационных файлов, которые не будут восстановлены из резервной копии. Восстановление этих файлов необходимо выполнить вручную:
  - **/usr/local/pf/conf/radiusd/***;
  - **/usr/local/pf/conf/log.conf**;
  - **/usr/local/pf/conf/log.conf.d/***;
  - **/usr/local/pf/conf/iptables.conf**;
  - **/usr/local/pf/conf/cluster.conf**.

Создание резервной копии

Для кластерной инсталляции, процесс резервного копирования необходимо начинать на узле, IP-адрес которого является первым в списке, получаемом при выполнении запроса **show status like 'wsrep_incoming_addresses'** в базе данных MariaDB.

Для того чтобы создать резервную копию, выполните следующие действия:

Шаг 1. Запустите процесс резервного копирования инсталляции, выполнив следующую команду:

/usr/local/pf/addons/backup-and-maintenance.sh

По умолчанию AxelNAC автоматически создаёт резервную копию в 00:30 каждый день. Если вы хотите использовать автоматически созданную копию, пропустите этот шаг.

Шаг 2. Запустите скрипт экспорта резервной копии:

/usr/local/pf/addons/full-import/export.sh /tmp/export.tgz

Данный скрипт создаст архив с резервной копией в директории **/tmp/export.tgz**.

Восстановление одиночной инсталляции из резервной копии

Для того чтобы восстановить одиночную инсталляцию из резервной копии, выполните следующие действия:

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

Шаг 2. Пройдите все шаги веб-конфигуратора.

Шаг 3. Скопируйте архив с резервной копией **export.tgz** на узел, который вы восстанавливаете.

Шаг 4. Запустите скрипт восстановления из резервной копии:

/usr/local/pf/addons/full-import/import.sh -f /директория_в_которой_хранится_резервная_копия/export.tgz

Во время восстановления базы данных потребуется ввести пароль от пользователя **root**.

Шаг 5. Укажите какой IP-адрес необходимо сохранить:

- **y:** сохранить существующий IP-адрес;
- **n:** заменить существующий IP-адрес значением из резервной копии.

Конфигурация сетевых карт не будет восстановлена из резервной копии.

Восстановление кластерной инсталляции из резервной копии

Для того чтобы восстановить кластерную инсталляцию из резервной копии, выполните следующие действия:

Шаг 1. Подключитесь к узлу с чистой инсталляцией 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**. Также необходимо задать hostname.

Шаг 3. Скопируйте архив с резервной копией **export.tgz** на узел, который вы восстанавливаете.

Шаг 4. Запустите скрипт восстановления из резервной копии:

/usr/local/pf/addons/full-import/import.sh -f /директория_в_которой_хранится_резервная_копия/export.tgz

Во время восстановления базы данных потребуется ввести пароль от пользователя **root**.

Шаг 5. Укажите какой IP-адрес необходимо сохранить:

- **y:** сохранить существующий IP-адрес;
- **n:** заменить существующий IP-адрес значением из резервной копии.

Конфигурация сетевых карт не будет восстановлена из резервной копии.

Шаг 6. В файл **/etc/sysctl.conf** добавьте следующие строки:

net.ipv4.ip_nonlocal_bind = 1
net.ipv6.conf.all.disable_ipv6 = 1

Шаг 7. Для применения настроек ,через платформу виртуализации выполните следующие команды:

sysctl -p
reboot

Шаг 8. Остановите службу баз данных, используя следующую команду:

systemctl stop packetfence-mariadb

Шаг 9. Включите службу кластеризации на каждом из ведомых узлов, используя следующую команду:

systemctl set-default packetfence-cluster

Шаг 10. Интегрируйте узел в кластер.

ID статьи: 1032
Последнее обновление: 26 дек., 2024
Обновлено от: Михалева А.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Резервное копирование и восстановление инсталляции -> Управление резервным копированием AxelNAC
https://docs.axel.pro/entry/1032/