Настройка отказоустойчивого кластера в контексте безопасности в НАЙС ОС

Введение

Отказоустойчивый кластер представляет собой группу серверов, работающих вместе для обеспечения высокой доступности сервисов. В случае отказа одного из серверов его задачи автоматически перенимаются другими серверами в кластере. В данной документации рассмотрены установка, настройка и использование отказоустойчивого кластера в НАЙС ОС, а также примеры использования команд и рекомендации по обеспечению безопасности.

Установка необходимых компонентов

Для настройки отказоустойчивого кластера в НАЙС ОС потребуется установить следующие пакеты: `pacemaker`, `corosync` и `crmsh`. Используйте пакетный менеджер `tdnf` или `dnf` для установки:

```
$ sudo tdnf install pacemaker corosync crmsh
```

Настройка Corosync

Corosync - это система обмена сообщениями, которая обеспечивает связь между узлами кластера. Конфигурационный файл Corosync находится по пути `/etc/corosync/corosync.conf`. Пример базовой конфигурации:

```
totem {
    version: 2
    secauth: on
    cluster_name: my_cluster
    transport: udpu
    interface {
        ringnumber: 0
        bindnetaddr: 192.168.1.0
        mcastport: 5405
        ttl: 1
    }
}

logging {
    to_logfile: yes
    logfile: /var/log/corosync/corosync.log
    to_syslog: yes
}

quorum {
    provider: corosync_votequorum
    two_node: 1
```

```
}
```

После настройки конфигурационного файла перезапустите Corosync:

```
$ sudo systemctl restart corosync
```

Настройка Pacemaker

Pacemaker - это менеджер ресурсов кластера, который контролирует и управляет сервисами в кластере. Для инициализации кластера используйте команду:

```
$ sudo crm cluster init
```

Добавьте узлы кластера:

```
$ sudo crm cluster join -c node1
$ sudo crm cluster join -c node2
```

Проверьте статус кластера:

```
$ sudo crm status
```

Настройка ресурсов кластера

После настройки кластера необходимо настроить ресурсы, которые будут управляться Pacemaker. Например, для настройки IP-адреса в качестве ресурса кластера выполните следующие команды:

```
$ sudo crm configure primitive ClusterIP ocf:heartbeat:IPaddr2 params
ip=192.168.1.100 cidr_netmask=24 op monitor interval=30s
```

Настройка ресурса для Apache:

```
$ sudo crm configure primitive WebServer ocf:heartbeat:apache params
configfile=/etc/httpd/conf/httpd.conf statusurl="http://127.0.0.1/server-status"
op monitor interval=30s
```

Обеспечение безопасности кластера

Для обеспечения безопасности отказоустойчивого кластера в НАЙС ОС следует учитывать следующие рекомендации:

Шифрование и аутентификация

Используйте шифрование и аутентификацию для обеспечения безопасности связи между узлами кластера. Включите `secauth` в конфигурации Corosync:

```
totem {
    secauth: on
    ...
}
```

Ограничение доступа

Ограничьте доступ к конфигурационным файлам и управляющим утилитам кластера, установив соответствующие права доступа:

```
$ sudo chmod 600 /etc/corosync/corosync.conf
$ sudo chmod 600 /etc/pacemaker/authkey
```

Мониторинг и логирование

Настройте логирование и мониторинг активности кластера для своевременного выявления и реагирования на инциденты безопасности. Проверьте настройки логирования в файлах `/etc/corosync/corosync.conf` и `/etc/pacemaker/pacemaker.conf`.

Регулярное обновление

Обеспечьте регулярное обновление ПО кластера для защиты от известных уязвимостей. Используйте пакетный менеджер для обновления:

```
$ sudo tdnf update
```

Рекомендации по безопасности

- Регулярно проверяйте и обновляйте конфигурацию кластера для соответствия текущим требованиям безопасности.
- Используйте шифрование и аутентификацию для защиты данных, передаваемых между узлами кластера.
- Ограничьте доступ к конфигурационным файлам и управляющим утилитам кластера.
- Настройте мониторинг и логирование для своевременного выявления инцидентов безопасности.
- Регулярно обновляйте программное обеспечение кластера для защиты от известных уязвимостей.

Заключение

Настройка отказоустойчивого кластера в НАЙС ОС с использованием Pacemaker и Corosync обеспечивает высокую доступность сервисов и защиту от отказов. Следуя приведенным

рекомендациям и примерам, вы сможете эффективно настроить и использовать отказоустойчивый кластер для повышения уровня безопасности и надежности вашей системы.