НОРСИ-ТРАНС

Закрытое Акционерное Общество

Информационная безопасность и вопросы хранения и защиты персональных данных при предоставлении услуг “Виртуальный хостинг”, VPS и “Аренда серверов”

Докладчик: Нестеров Иван Михайлович

i.nesterov@norsi-trans.ru

+79055326382

Основные виды хостинга:

- ❑ Виртуальный хостинг (shared)
- ❑ VPS (виртуальный выделенный сервер, VDS)
- ❑ Выделенный сервер (Dedicated Server)

Виртуальный хостинг (shared)

- ❑ Преимущества:
- ✓ Дешевизна.
- ✓ Хостинг-провайдер поддерживает и обновляет системное ПО сервера.
- ❑ Недостатки:
- ✓ нельзя произвести тонкие настройки системного ПО.
- ✓ сайт может «тормозить» из-за нагрузки на другие сайты на сервере

VPS (виртуальный выделенный сервер, VDS)

- ❑ Преимущества:
- ✓ Выделяемые ресурсы гарантированы каждому сайту, нет «торможения» из-за других сайтов.
- ✓ Посещаемость до нескольких тысяч посетителей в сутки.
- ✓ VPS можно «настроить» для более быстрой работы сайта.
- ❑ Недостаток: Необходимость администрирования (настойки), как следствие требования к достаточно высокому уровеню знаний пользователя VPS/VDS

Выделенный сервер (Dedicated Server)

- Преимущества: Огромные выделенные мощности.
- Недостаток: Необходимо администрировать. Неограниченное количество посетителей в месяц.

Виртуализация для реализации VPS/VDS: аппаратная виртуализация

- ✓ Упрощение разработки программных платформ виртуализации за счет предоставления аппаратных интерфейсов управления и поддержки виртуальных гостевых систем.
- ✓ Возможность увеличения быстродействия платформ виртуализации.
- ✓ Улучшается защищённость, появляется возможность переключения между несколькими запущенными независимыми платформами виртуализации на аппаратном уровне.
- ✓ Гостевая система становится не привязана к архитектуре хостовой платформы и к реализации платформы виртуализации.
- ✓ Технология аппаратной виртуализации делает возможным запуск 64-битных гостевых систем на 32-битных хостовых системах (с 32-битными средами виртуализации на хостах).

Виртуализация для реализации VPS/VDS: на уровне операционной системы

- ✓ Виртуализация на уровне операционной системы позволяет запускать изолированные и безопасные виртуальные машины на одном физическом узле, но не позволяет запускать операционные системы с ядрами, отличными от типа ядра базовой операционной системы.
- ✓ При виртуализации на уровне операционной системы не существует отдельного слоя гипервизора. Вместо этого сама хостовая операционная система отвечает за разделение аппаратных ресурсов между несколькими виртуальными машинами и поддержку их независимости друг от друга.

Виртуализация для реализации VPS/VDS: аппаратная виртуализация на основе Xen

- Xen — это гипервизор, который поддерживает архитектуры x86, x86_64, Itanium и ARM и может запускать Linux, Windows, Solaris и некоторые BSD в качестве гостевых на поддерживаемых CPU архитектурах.
- Xen поддерживается рядом компаний, прежде всего Citrix, но также используется Oracle для Oracle VM и другими.
- Xen может выполнять полную виртуализацию в системах, поддерживающих расширения виртуализации и тех у кого нет поддержки расширения виртуализации.

Виртуализация для реализации VPS/VDS: аппаратная виртуализация на основе OpenVZ.

- OpenVZ - виртуализация уровня операционной системы. Технология базируется на ядре ОС Linux и позволяет на одном физическом сервере создавать и запускать изолированные друг от друга копии выбранной операционной системы (Debian, CentOS, Ubuntu).

Виртуализация для реализации VPS/VDS: аппаратная виртуализация на основе KVM.

- Виртуализация KVM (Kernel-based Virtual Machine) — технология аппаратной виртуализации, позволяющая создать на хост-машине полный виртуальный аналог физического сервера. KVM позволяет создать полностью изолированный от «соседей» виртуальный сервер с собственным ядром ОС, который пользователь может настраивать и модифицировать под собственные нужды без ограничений. Каждому такому серверу выделяется своя область в оперативной памяти и пространство на жестком диске, что повышает общую надежность работы такого сервера.

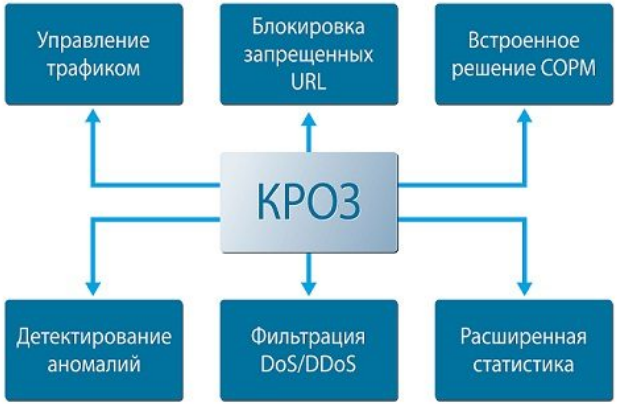
Сравнение типов виртуализации OpenVZ и KVM:

OpenVZ	KVM
ОС из ряда предложенных: Debian, CentOS, Ubuntu	Linux, Windows, FreeBSD, установка собственного дистрибутива
Изменение ресурсов без перезагрузки (жёсткий диск, память, процессор)	Память и процессор изменятся после перезагрузки, жёсткий диск — только после обращения в поддержку (на готовых тарифах память изменить нельзя)
Смена тарифного плана без перезагрузки	Смена тарифного плана по запросу в поддержку. Сервер будет недоступен 1-2 часа.
Мягкие лимиты: максимальная производительность сервера может отклоняться в большую или меньшую сторону	Жёсткие лимиты: каждый сервер получает заявленные ресурсы
Ограничение на запуск высоконагруженных проектов. Запрещено запускать Java-приложения, массовые рассылки и проксировать трафик. TUN/TAP выключен.	Возможность запуска любых проектов (кроме систем распределённых вычислений)

Какое же хранилище мы используем?

Ceph — это программно-определяемая распределенная файловая система с открытым исходным кодом, лишенная узких мест и единых точек отказа, которая представляет из себя легко масштабируемый до петабайтных размеров кластер узлов, выполняющих различные функции, обеспечивая хранение и репликацию данных, а также распределение нагрузки, что гарантирует высокую доступность и надежность.

Для корректной работы хранилища и клиентов также необходимо резервирование питания и высокоскоростные каналы доступа в интернет с защитой от DDoS атак, мы используем две собственных защиты SOPSA и КРОЗ.



СОПСА —Система Обнаружения и Предотвращения Сетевых Атак

Основные функции системы:

— Мониторинг объектов контроля, сервисов, оборудования
— Выявление аномалий, DOS/DDOS атак, утечки данных, уязвимых объектов сети
— Аудит взаимодействия и передачи трафика
— Маршруты прохождения и планирование расширения сети
— Статистический и эмпирический анализ взаимодействия BGP, NetFlow, SNMP
— BGP Flow Spec фильтрация DOS/DDOS атак
— Система фильтрации для очистки вредоносного трафика, который нельзя фильтровать статистическими правилами и фаерволом

Дополнительная функция — фильтрация запрещенных (Url) ресурсов в РФ

Используемая схема подключения, позволяет использовать систему СОПСА для ограничении доступа к ресурсам сети Интернет, содержащим информацию, распространение которой в РФ запрещено, в соответствии:

— фз от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»
— фз от 28 июля 2012 г. №139-ФЗ «О внесении изменений в ФЗ “О защите детей от информации, причиняющей вред их и здоровью и развитию» и отдельными законодательными актами РФ»
— приказ Роскомнадзора от 17.07.2014 №103
— фз от 28 декабря 2013 г. N 398-ФЗ;
— фз от 2 июля 2013 г. № 187-ФЗ;
— фз от 5 апреля 2013 г. № 50-ФЗ.

КРОЗ - Аппаратно-программный комплекс автоматического обнаружения и блокирования DDOS-атак.

Функциональность:

- Фоновый статистический контроль метрик сети с целью обнаружения профиля злоумышленника;
- Автоматическое блокирование трафика злоумышленника во всей контролируемой сети;
- Настраиваемые уровни и режимы контроля для выделенных подсетей, личный кабинет для клиентов оператора;
- Блокирование атак, исходящих от клиентов;
- Специальные функции защиты от сильно распределенных атак;
- Возможность ручного анализа и задания правил;
- Возможность распределения сети зондов;
- Возможность активной защиты WEB-сервисов на уровне прикладных сессий;
- Детектирование широкого спектра DDoS-атак;
- Отчеты в режиме реальном времени;
- Автоматическая запись дампов трафика атак, ретроспективный анализ.

Информационная безопасность виртуального сервера.

«Информационная безопасность виртуального сервера» — это процесс обеспечения доступности, целостности и конфиденциальности информации.

- Под «доступностью» понимается соответственно обеспечение доступа к информации.
- «Целостность» — это обеспечение достоверности и полноты информации.
- «Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.
- Под «Угрозой» понимается потенциальная возможность тем или иным способом нарушить информационную безопасность. Попытка реализации угрозы называется «атакой», а тот, кто реализует данную попытку, называется «злоумышленником». Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем.

Информационная безопасность виртуального сервера. Угрозы ИБ, которые наносят наибольший ущерб

1. Угроза непосредственно информационной безопасности:
- ❑ Доступность
- ❑ Целостность
- ❑ Конфиденциальность

2. Компоненты на которые угрозы нацелены:
- ❑ Данные
- ❑ Программы
- ❑ Аппаратура
- ❑ Поддерживающая инфраструктура

3. По способу осуществления:
- ❑ Случайные или преднамеренные
- ❑ Природного или техногенного характера

4. По расположению источника угрозы бывают:
- ❑ Внутренние
- ❑ Внешние

Информационная безопасность виртуального сервера. Угрозы непосредственно информационной безопасности

К основным угрозам доступности можно отнести

1.Внутренний отказ информационной системы;

2.Отказ поддерживающей инфраструктуры.

Основными источниками внутренних отказов являются:

•Нарушение (случайное или умышленное) от установленных правил эксплуатации

•Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)

•Ошибки при (пере)конфигурировании системы

•Вредоносное программное обеспечение

•Отказы программного и аппаратного обеспечения

•Разрушение данных

•Разрушение или повреждение аппаратуры

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

•Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

•Разрушение или повреждение помещений;

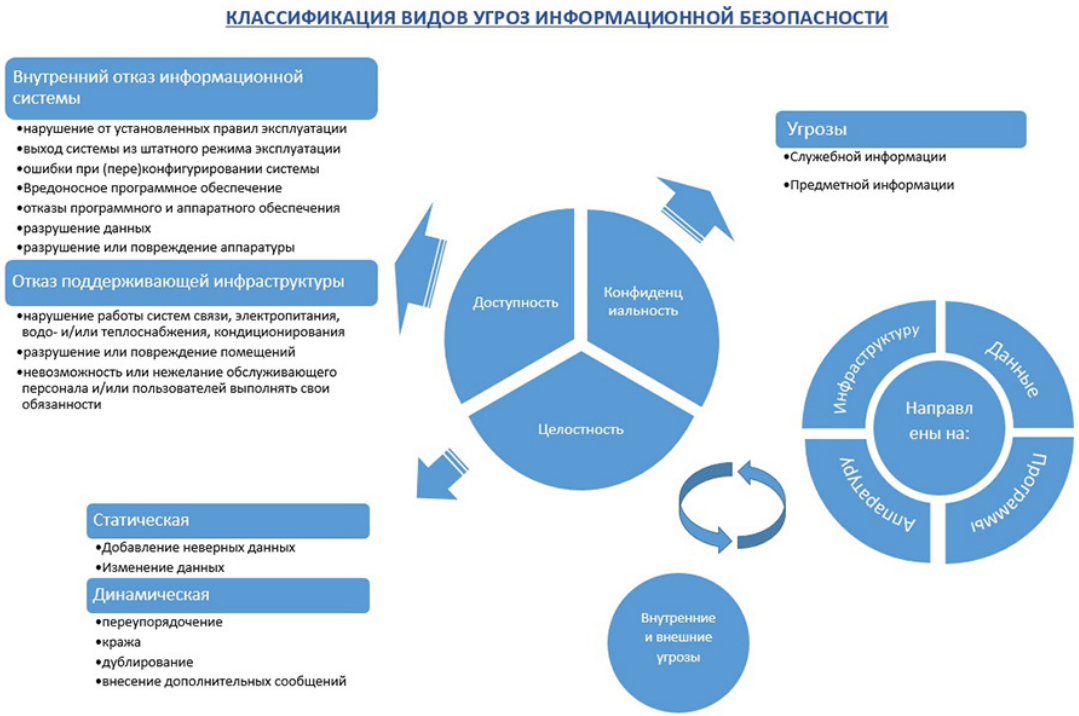
•Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Информационная безопасность виртуального сервера. Основные угрозы целостности

С целью нарушения статической целостности злоумышленник может:

- Ввести неверные данные
- Изменить данные
- Угрозами динамической целостности являются, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений.

Информационная безопасность виртуального сервера. Основные угрозы конфиденциальности



Информационная безопасность виртуального сервера. Оценка ущерба.

Каждый кто приступает к организации информационной безопасности, должен ответить на три основных вопроса:

1.Что защищать?
2.От кого защищать, какие виды угроз являются превалирующими: внешние или внутренние?
3.Как защищать, какими методами и средствами?

Резервирование хостинга: полного отказа невозможно.

- ❑ Защита от DDoS защищает сеть
- ❑ Резервирование питания
- ❑ Отказоустойчивый ceph обеспечивает целостность и изолированность информации, а также возможность бесшовной live миграции KVM.

Таким образом, мы не имеем единой точки отказа.

Схематично итоговая схема проект выглядит следующим образом:

Резервное питание

|

Сервера — высокоскоростная сеть - хранилище

|

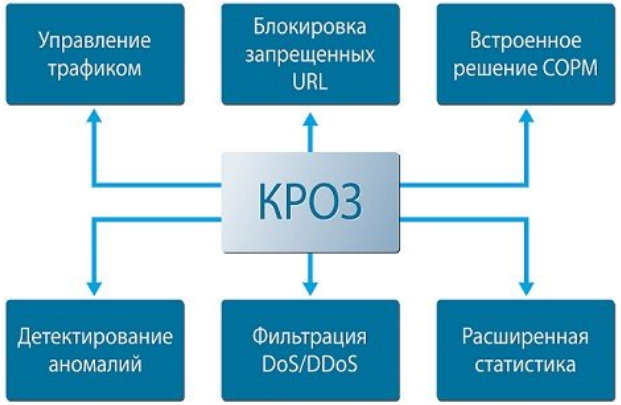
Резервируемый Интернет

|

Защита от DDoS атак

Требования ФСТЭК для СОВ

Для дифференциации требований к функциям безопасности систем обнаружения вторжений установлено шесть классов защиты систем обнаружения вторжений.



- Системы обнаружения вторжений, соответствующие 6 классу защиты, применяются в информационных системах персональных данных 3 и 4 классов.
- Системы обнаружения вторжений, соответствующие 5 классу защиты, применяются в информационных системах персональных данных 2 класса.

Спасибо за внимание.

Приглашаем к сотрудничеству

ЗАО «Норси-Транс»

E-mail: info@norsi-trans.ru i.nesterov@norsi-trans.ru

Тел.: +7 495 748 7483; +7 9055326382.