Проблемы с программно-определяемыми сетями (SDN)

- Недоступность ВМ с FIP при живой миграции между гипервизорами
- Не работает изменение параметров внешних сетей
- Ошибка перемещения хоста с отключенным IPv6 в кластер SDN
- Неработоспособность SDN при перемещении хоста из кластера без ovirt-provider-ovn в кластер SDN
- ВМ в кластере SDN теряет сеть после восстановления из снимка с памятью

Руководство администратора

- Администрирование и обслуживание zVirt
- Администрирование ресурсов zVirt
- Управление средой zVirt
- Мониторинг zVirt
- Конвертация виртуальных машин
- Руководство по миграции
- VDSM и хуки
- Прокси-серверы

Проблемы при аутентификации и авторизации

- Ошибка "Cannot authenticate using при настройке ovirt-engine-extension-aaa-ldap-setup"
- Ошибка "Cannot resolve principal" при попытке подключения к внешнему серверу аутентификации AD
- Ошибка "server error data 52e" при авторизации
- При входе в Портал администрирования ошибка "Unable to log in A number of active sessions is exceeded"

Автоматизация

- Введение в автоматизацию работы zVirt с помощью Ansible
- Автозапуск виртуальных машин при перезагрузке менеджера управления (BM HostedEngine)
- Работа с шаблонами zVirt с помощью Ansible
- Удаление устаревших LUN на хостах средствами Ansible
- Динамический Ansible inventory в zVirt
- Выключение стенда
- Импорт OVA-файлов в zVirt с помощью "Ansible"
- Управление инфраструктурой кластера с помощью Ansible
- Управление инфраструктурой виртуальных машин с помощью Ansible
- Управления разрешениями на виртуальные машины zVirt с помощью Ansible

При резервном копировании

- Ошибка ВМ приостановлена из-за отсутствия места в хранилище при восстановлении CPK Acronis
- Ошибка "Must be owner of extension uuid-ossp" при восстановлении из резервной копии
- Ошибка "Manual backup for VM NAME has failed"
- ВМ выключается при выполнении резервного копирования с помощью Acronis

Лучшие практики

1. Физическая инфраструктура

Аннотация

В этой главе представлены рекомендации по выбору и настройке оборудования для использования с платформой виртуализации zVirt.

1.1. Серверы

1.1.1. Проверка оборудования

Перед развертыванием системы мы рекомендуем следующее:

- Убедитесь, что всё оборудование включено в список совместимого оборудования.

  Матрицу совместимости можно посмотреть на официальном сайте Orion soft.

- Убедитесь, что ваше оборудование соответствует минимальным требованиям.

  Требования к оборудованию описаны в разделе Требования в Руководстве по предварительному планированию инфраструктуры.

- Протестируйте системную память на наличие аппаратных ошибок.

1.1.2. Рекомендации относительно ЦП

В этом разделе содержится описание некоторых особенностей относительно ЦП серверов и их влияние на использование в среде zVirt.

1.1.2.1. Уязвимости бокового канала процессора

Во многих современных процессорах был обнаружен класс уязвимостей безопасности, известных как "уязвимости бокового канала". Например, к ним относятся: Spectre, Meltdown, Foreshadow, L1TF. Некоторые меры по устранению этих уязвимостей могут оказать значительное влияние на производительность.

Способы устранения уязвимостей:

- аппаратно;
- с помощью микрокода;

Аппаратные меры по устранению

Некоторые недавние выпуски ЦП включают аппаратные средства защиты, которые могут устранить уязвимости с минимальным влиянием на производительность или вообще без него. Таким образом, в дополнение к любому приросту производительности этих процессоров, выбор их для новой системы может обеспечить еще больший прирост производительности по сравнению со старыми процессорами, которые требуют решения на уровне микрокода или ПО для устранения уязвимостей.

Устранение на уровне микрокода

Некоторые "уязвимости бокового канала" могут быть устранены на уровне микрокода. Микрокод — это слой кода, который выполняется на ЦП ниже видимого извне набора инструкций ЦП. Микрокод, поставляемый с процессором, может быть обновлен либо с помощью обновлений BIOS, либо с помощью операционной системы (ОС).

1.1.2.2. Аппаратная виртуализация

Большинство процессоров Intel® и AMD оснащены аппаратными функциями для поддержки виртуализации и повышения производительности. Функции: аппаратная виртуализация ЦП, виртуализация MMU и виртуализация ввода-вывода MMU — описаны ниже.

Аппаратная виртуализация ЦП (Intel VT и AMD-V™)

Аппаратная поддержка виртуализации ЦП, называемая **Intel VT** (в процессорах Intel) или **AMD-V** (в процессорах AMD), обеспечивает производительность, сравнимую с производительностью невиртуализованной машины.

Аппаратная виртуализация MMU (Intel EPT и AMD RVI)

Аппаратная виртуализация MMU, называемая Rapid Virtualization Indexing (RVI) в процессорах AMD и Extended Page Table (EPT) в процессорах Intel, устраняет накладные расходы, которые связаны с виртуализацией блоков управления памятью (MMU), и обеспечивает аппаратную поддержку для виртуализации MMU.

Аппаратная виртуализация MMU позволяет создать дополнительный уровень таблиц страниц, которые сопоставляют физическую память гостевой системы с адресами физической памяти. При этом устраняется необходимость в обслуживании теневых таблиц страниц. Это снижает потребление памяти и ускоряет рабочие нагрузки, в которых гостевые ОС часто изменяют таблицы страниц.

Несмотря на то, что аппаратная виртуализация MMU повышает производительность большинства рабочих нагрузок, она увеличивает время, необходимое для обслуживания промаха TLB. Тем самым снижается производительность рабочих нагрузок, нагружающих TLB. Тем не менее, эту возросшую стоимость промаха TLB можно смягчить, настроив гостевую ОС и приложения на использование больших страниц памяти.

Аппаратная виртуализация ввода-вывода MMU (VT-D и AMD-Vi)

Аппаратная виртуализация ввода-вывода MMU (IOMMU), называемая Intel VT-d в процессорах Intel и AMD-VI в процессорах AMD, представляет собой функцию управления памятью ввода-вывода, которая переназначает передачу ввода-вывода DMA и прерывания устройства. Эта функция может позволить ВМ иметь прямой доступ к аппаратным устройствам ввода-вывода, таким как сетевые карты, контроллеры хранения данных (HBA) и графические процессоры.

1.1.2.3. Общие рекомендации в отношении ЦП

В таблице ниже описаны параметры ЦП, которые следует учитывать при подготовке сервера к использованию в среде zVirt.

Параметр	Описание/рекомендации
Марка процессора	• zVirt поддерживает процессоры как AMD, так и Intel, поэтому выбор зависит от ваших требований. • Выбирайте конкретный бренд и придерживайтесь его. Особенно если большинство текущих серверов уже используют определенный бренд. • При наличии в парке серверов с процессорами различных марок необходимо учитывать невозможность их размещения в одном кластере при планировании.
Расширения виртуализации	• Для использования в качестве хоста zVirt, сервер должен иметь процессоры, поддерживающие расширение AMD-V или Intel-VT. • Использование процессоров с поддержкой аппаратной виртуализации MMU (Intel EPT или AMD RVI) в большинстве случаев позволяет повысить производительность. Некоторые тесты показывают прирост производительности до 40-50%. • Использование процессоров с поддержкой аппаратной виртуализации IOMMU (VT-D и AMD-Vi) позволяет напрямую пробрасывать устройства сервера (например, GPU или сетевые интерфейсные карты) в ВМ.
Многоядерные процессоры	• zVirt поддерживает работу только с архитектурой x86_64 (AMD64 и Intel64). • Наличие большего количества ядер дает планировщику ЦП гипервизора большую гибкость при сопоставлении физических ядер и виртуальных ЦП и, как правило, увеличивает производительность при одновременной работе на хосте большого количества ВМ. • Если в среде не планируется запускать большое количество ВМ, то целесообразнее использовать процессоры с меньшим количеством ядер, но большей тактовой частотой. В этом случае конкуренция за процессорное время со стороны ВМ не значительная. Не требуются сложные топологии сопоставления физического и виртуального процессоров, что обеспечивает упрощение планирования ресурсов ЦП и увеличение производительности ВМ.
Поддерживаемая память	Используйте ЦП с поддержкой новейшего поколения памяти, что позволит выбрать модули памяти с более высокой частотой и объемом.

1.1.3. Рекомендации относительно памяти

В этом разделе приведены рекомендации по использованию памяти с zVirt.

Параметр	Описание/рекомендации
Бренд	Старайтесь не смешивать бренды в одном сервере.
Поколение	• Используйте память новейшего поколения, так как она обеспечивает более высокую производительность и стабильность. • При выборе памяти проверьте, что она совместима с имеющимися компонентами. ℹ В некоторых случаях на старых платформах для поддержки выбранной памяти может потребоваться обновление прошивки.
Объем памяти	• Используйте максимально возможный объем памяти, так как это самый нагружаемый ресурс при использовании виртуализации. Его нехватка может привести к значительному снижению производительности, а также остановке важных процессов. • Для достижения максимального объема памяти изучите руководство по эксплуатации вашей серверной платформы и выберете оптимальную конфигурацию размещения модулей в слотах. ❗ Обратите внимание, что максимальный объем памяти, который может быть использован на хосте zVirt составляет 12 ТБ.
Эффективная частота	Старайтесь использовать модули с максимально допустимой частотой, но убедитесь, что эта частота поддерживается ЦП. Если частота выбранного модуля превышает допустимую частоту процессора и системной платы, он будет либо работать на частоте, поддерживаемой процессором, либо не будет работать совсем.
Многоканальное подключение	• Используйте многоканальный режим подключения RAM, так как он является наиболее стабильным. • Старайтесь задействовать все каналы. • При использовании многоканального подключения обязательно сверьтесь с руководством по эксплуатации вашей платформы, чтобы не получить неподдерживаемую конфигурацию.
Многоранговая память	• Многоранговые модули позволяют достичь большего объема памяти, но при этом возможно некоторое снижение производительности. • 4-х и 8-ранговые модули могут накладывать различные ограничения. • Старайтесь избегать установки памяти с разными рангами.

Параметр	Описание/рекомендации
Типы памяти (RDIMM и LRDIMM)	• По возможности старайтесь использовать модули LRDIMM, так как они имеют массу положительных свойств по сравнению с RDIMM. • Не смешивайте на одной платформе RDIMM и LRDIMM. ! При выборе LRDIMM убедитесь, что ваша платформа поддерживает этот тип памяти.

1.1.4. Рекомендации по проверке и настройке BIOS

Аппаратные настройки BIOS по умолчанию на серверах не всегда могут быть лучшим выбором для оптимальной производительности. В этом разделе перечислены некоторые настройки BIOS, которые следует проверить, особенно при первой настройке нового сервера.

1.1.4.1. Общие настройки

- Убедитесь, что вы используете последнюю версию BIOS, доступную для вашей системы.

  i После обновления BIOS необходимо повторно проверить настройки BIOS на случай, если станут доступны новые параметры BIOS или изменились настройки старых параметров.

- Убедитесь, что BIOS настроен на активацию всех заполненных процессорных сокетов и на активацию всех ядер в каждом сокете.
- Активируйте **Turbo Boost** в BIOS, если ваши процессоры его поддерживают.
- Убедитесь, что технология **Hyper-Threading** активирована в BIOS для процессоров, которые ее поддерживают.
- В некоторых системах, поддерживающих архитектуру NUMA, предусмотрена возможность деактивации NUMA путем активации чередования узлов. В большинстве случаев наилучшую производительность можно получить, отключив чередование узлов (другими словами, оставив NUMA активированным).
- Убедитесь, что все функции аппаратной виртуализации (VT-x, AMD-V, EPT, RVI и т.д.) активированы в BIOS.

  i После внесения изменений в эти функции аппаратной виртуализации некоторым системам может потребоваться полное отключение питания, прежде чем изменения вступят в силу.

- Деактивируйте в BIOS все устройства, которые вы не будете использовать. Это могут быть, например, ненужные последовательные, USB или сетевые порты.

1.1.4.2. Настройки BIOS для конкретного процессора

Помимо общих настроек BIOS, некоторые семейства процессоров имеют свои специальные настройки, которые могут повлиять на производительность. К ним относятся:

- Выбор режима "Snoop".
- Настройки NUMA процессора AMD EPYC.

1.2. Системы хранения данных

zVirt поддерживает различные типы хранилищ (подробнее см. в разделе Хранилище руководства по администрированию ресурсов zVirt). В этом разделе приведены рекомендации по СХД.

1.2.1. Общие рекомендации

Многие рабочие нагрузки очень чувствительны к задержке операций ввода-вывода. Поэтому важно, чтобы устройства хранения данных были правильно настроены.

Для обеспечения должной производительности СХД учитывайте следующие рекомендации:

- Обеспечьте достаточную пропускную способность инфраструктуры хранения данных.
- При проектировании производительности сети хранения данных учитывайте физические ограничения сети, а не логические распределения. Использование VLAN или VPN не является подходящим решением проблемы превышения лимита подписки на каналы в общих конфигурациях. VLAN и другие способы виртуального разделения сети обеспечивают способ логической конфигурации сети, но не изменяют физические возможности каналов и магистралей между коммутаторами.

  Виртуальные локальные сети и VPN позволяют использовать функции качества обслуживания сети (QoS). Эти функции не устраняют превышение лимита подписки, но позволяют распределять полосу пропускания предпочтительно или пропорционально определенному трафику.
- Убедитесь, что адаптеры памяти установлены в слоты с достаточной пропускной способностью для поддержания ожидаемой пропускной способности. Будьте внимательны, чтобы различать похожие по звучанию, но потенциально несовместимые архитектуры шин, включая PCI, PCI-X, PCI Express (PCIe), PCIe 3.0 (он же PCIe Gen 3) и PCIe 4.0 (он же PCIe Gen 4). И обязательно обратите внимание на количество "полос" для тех архитектур, которые могут поддерживать более одной полосы.

  Например, для обеспечения полной пропускной способности однопортовые платы HBA Fibre Channel 32 Гбит/с должны быть установлены как минимум в слоты PCIe Gen2 x8 или PCIe Gen 3 x4 (каждый из которых способен обеспечить максимальную пропускную способность 32 Гбит/с в каждом направлении), а двухпортовые HBA-платы Fibre Channel 32 Гбит/с должны быть установлены как минимум в слоты PCIe Gen 3 x8 (которые

способны обеспечить максимальную пропускную способность 64 Гбит/с в каждом направлении).

- Убедитесь, что скорость Fibre Channel стабильна, чтобы избежать проблем с производительностью.
- При необходимости настройте максимальную длину очереди для плат HBA Fibre Channel.
- Для iSCSI и NFS убедитесь, что топология вашей сети не содержит узких мест Ethernet, когда множество каналов маршрутизируются через малое количество каналов, что может привести к превышению лимита подписки и потере сетевых пакетов.

1.2.2. Рекомендации по подготовке СХД

В следующей таблице рассмотрены рекомендации, которые будут полезны при планировании и подготовке СХД для использования в среде виртуализации zVirt.

Параметр	**Описание/рекомендации**
Физическое хранилище и накопители	• При выборе типов накопителей учитывайте возможные нагрузки. Если в среде виртуализации предполагается наличие ВМ с высокой интенсивностью операций ввода/вывода в хранилище или планируется одновременная работа достаточно большого количества ВМ — стоит либо отказаться от HDD в пользу SSD, либо разделить нагрузку между несколькими хранилищами. • Накопители можно организовать в RAID-массив для повышения отказоустойчивости и/или производительности.
Использование нескольких хранилищ для изоляции ввода-вывода	Когда несколько ВМ работают с одним и тем же хранилищем данных, тои все они используют одни и те же ресурсы ввода-вывода. Это может привести к конфликтам и проблемам с производительностью. Поэтому на этапе планирования и проектирования инфраструктуры следует рассмотреть возможность изоляции потоков ввода/вывода. Для изоляции можно использовать несколько хранилищ для различных групп ВМ, чтобы они не конкурировали за ресурсы. Это повысит производительность и предотвратит проблемы, связанные с конфликтами.
Переподписка на ресурсы хранилища	На этапе подготовки СХД важно корректно рассчитать необходимые ресурсы хранилища, чтобы не возникло ситуации при которой возникает переподписка.
Использование блочных хранилищ	• Со средой zVirt рекомендуется использовать блочные хранилища (iSCSI или Fibre Channel). Хранилища NFS менее производительны, чем блочные системы хранения, и не обеспечивают такой же уровень безопасности и защиты от потери данных. • Если используется NFS, то необходимо убедиться, что сеть правильно настроена и имеет достаточную пропускную способность (рекомендуется не менее 10 Гбит/с).

Параметр	Описание/рекомендации
Мониторинг использования хранилища	Необходимо убедиться, что в среде настроена система мониторинга за использованием хранилища и объемом свободного пространства.
Создание плана резервного копирования	Для резервного копирования ВМ можно использовать: • встроенную в zVirt функцию создания доменов хранения резервных копий; • ПО для резервного копирования от сторонних производителей. Независимо от выбранного метода необходимо регулярно тестировать план резервного копирования для проверки корректной работы.
Защита данных с помощью избыточности	Для защиты данных от потери используйте избыточность. Для этого можно использовать RAID и/или репликацию на резервную СХД.
Избыточный доступ к хранилищу	• Обеспечьте наличие резервных путей между хостами и СХД. • Для iSCSI или FC настройте многоканальность.

1.3. Проектирование сетевой инфраструктуры

В этом разделе приведены рекомендации по сетевому оборудованию для использования с zVirt.

1.3.1. Общие рекомендации относительно сетей

Перед оптимизацией сети ознакомьтесь с физическими аспектами сети:

- Рассмотрите возможность использования сетевых адаптеров (NIC) серверного класса для достижения наилучшей производительности.
- Убедитесь, что сетевая инфраструктура между исходной и целевой сетевыми картами не создает узких мест. Например, если обе сетевые карты имеют скорость 10 Гбит/с, проверьте, что все кабели и коммутаторы могут обеспечить такую пропускную способность и что коммутаторы не настроены на более низкое значение.
- Убедитесь, что сетевые карты установлены в слоты с достаточной пропускной способностью для поддержания их максимальной пропускной способности. Например:
  - однопортовые сетевые адаптеры Ethernet 10 Гбит/с должны использовать PCIe x8 (или выше) или PCI-X 266;
  - двухпортовые сетевые адаптеры Ethernet 10 Гбит/с должны использовать PCIe x16 (или выше);
  - однопортовые сетевые адаптеры Ethernet 40 Гбит/с должны использовать слоты PCIe Gen 3 x8 (или выше);

    - двухпортовые адаптеры 40 Гбит/с (или выше) должны использовать слоты PCIe Gen 3 x16 (или выше).
- Желательно, чтобы на пути к фактическому устройству Ethernet не было «микросхемы-моста» (например, PCI-X-PCIe или PCIe-PCI-X) (включая любую встроенную микросхему моста на самом устройстве), так как эти микросхемы могут снизить производительность.

Для достижения наилучшей производительности сети рекомендуется использовать сетевые адаптеры, поддерживающие следующие функции:

- Checksum Offload (CSO) или TCP Checksum Offloading (TCO) — обеспечивает проверку заголовка пакета с помощью сетевой карты, а не ЦП.
- Разгрузка сегментации TCP (TCP segmentation offload, TSO) — увеличивает исходящую пропускную способность сетевого интерфейса и снижение нагрузки на центральный процессор.
- Разгрузка большого приёма (large receive offload, LRO) — увеличивает входящую пропускную способность сетевого интерфейса и снижение нагрузки на центральный процессор.
- Возможность работы с несколькими элементами Scatter Gather на кадр Tx.
- Jumbo frames.

1.3.2. Резервирование

Основные способы резервирования сети:

- Установка дублирующего оборудования и обеспечение отказоустойчивых сервисов для критически важных устройств.
- Использование резервных путей.

Рисунок 1. Использование резервных путей для трафика, возникающего между сервером и СХД

Чтобы избежать возникновения петель при резервировании путей на уровне 2, используйте протоколы STP и RSTP.

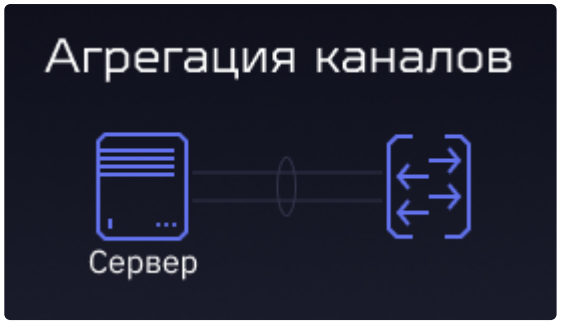

Рисунок 2. Резервирование путей между сервером и коммутатором с помощью Bond

- Использование устройств уровня 3 в магистральной системе. Уровень 3 не требует активации STP, а также обеспечивает лучший выбор пути и более высокую сходимость во время переключения на резервный ресурс.
- Использование протоколов динамической маршрутизации (OSPF, EIGRP, ISIS).

1.3.3. Уменьшение размера домена отказов

Домен отказов представляет собой область сети, затронутую сбоями в работе критически важного устройства или сетевого сервиса.

Использование резервных каналов и надежных устройств корпоративного класса сводит к минимуму вероятность нарушения работы сети.

Пример 1. Влияние отказа устройств

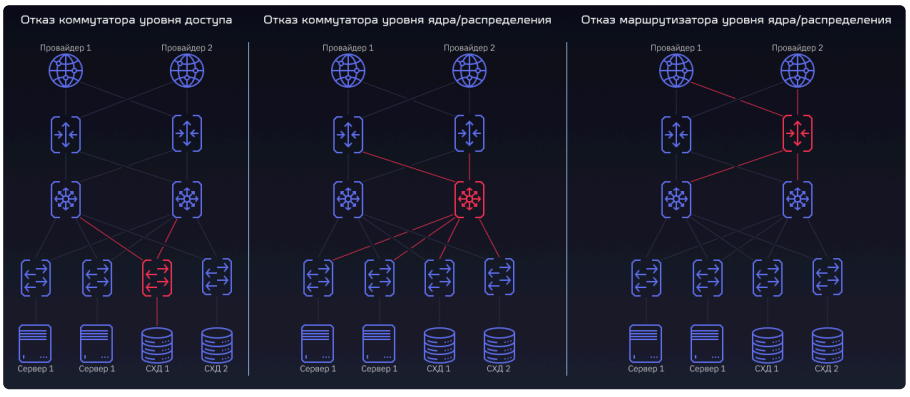

Рисунок 3. Качественно спроектированная сеть

Как видно из первого рисунка, при правильном проектировании сети сбой одного устройства вызывает минимальные неблагоприятные последствия для инфраструктуры в целом:

- При сбое коммутатора уровня доступа: инфраструктура теряет связь с конкретным устройством, подключенным к этому коммутатору. С точки зрения zVirt отключение отдельного домена хранения или сервера виртуализации не вызывает масштабный сбой среды (при корректном проектировании логической инфраструктуры), хотя

последствия могут быть чувствительны. Уменьшения времени недоступности можно достичь за счет наличия резервного коммутатора уровня доступа, на который можно быстро переключиться.

- При сбое одного коммутатора уровня ядра/распределения: система продолжает функционировать в нормальном режиме. Связь с хранилищами сохраняется, доступ к среде и виртуализированным сервисам также сохраняется (как изнутри, так и из внешних сетей).
- При сбое граничного маршрутизатора: система продолжает функционировать в нормальном режиме. Связь с хранилищами сохраняется, доступ к среде и виртуализированным сервисам также сохраняется (как изнутри, так и из внешних сетей).

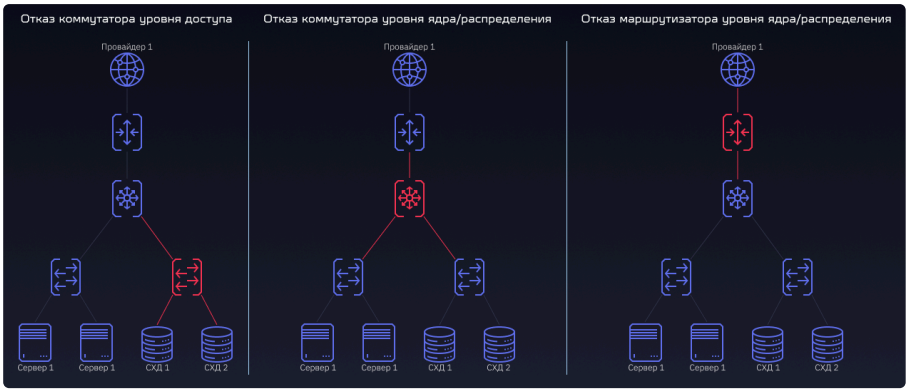

Рисунок 4. Сеть построенная без учёта рекомендаций

Из данного рисунка видно, что при подобном проекте сетевой инфраструктуры, последствия сбоя устройств могут быть значительными:

- При сбое коммутатора уровня доступа: пропадает связь со всеми устройствами, подключенными к нему. В случае, например, если все серверы виртуализации подключены к одному коммутатору. Это приведёт к масштабному сбою среды и недоступности всех виртуализированных сервисов.
- При сбое коммутатора уровня ядра/распределения: пропадает связь между всеми компонентами, что также вызывает масштабный сбой среды и недоступность всех виртуализированных сервисов.
- При сбое граничного маршрутизатора: система продолжает функционировать в нормальном режиме, но виртуализированные сервисы теряют доступ во внешнюю среду, а также невозможно получить доступ к этим сервисам извне.

1.3.3.1. Увеличение пропускной способности

В иерархической модели сети в некоторых каналах между коммутаторами доступа и коммутаторами распределения может потребоваться обработка большего объема трафика, чем в других каналах. Поскольку трафик из нескольких каналов объединяется в одном исходящем канале, такой канал может стать "узким местом". Агрегация каналов позволяет

администратору увеличить пропускную способность между устройствами за счет создания единого логического канала, состоящего из нескольких физических каналов.

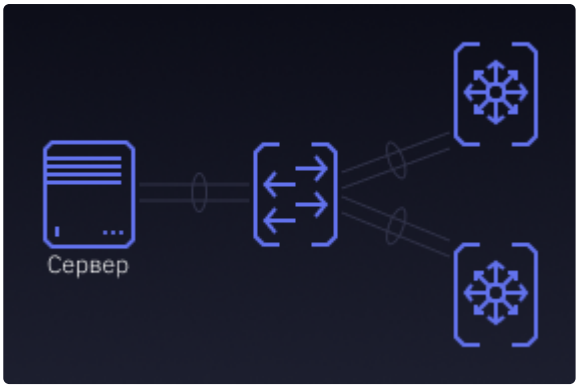

Рисунок 5. Использование агрегации на разных уровнях модели

2. Логическая инфраструктура

Аннотация

В этой главе представлены рекомендации по работе с логическими объектами среды zVirt.

2.1. Общие рекомендации

Ниже приведены общие рекомендации по инфраструктуре среды виртуализации:

- Используйте NTP (в zVirt поддерживается chrony) на всех хостах и виртуальных машинах в среде для синхронизации времени. Аутентификация и сертификаты особенно чувствительны к разнице во времени.
- Для разрешения имён в продуктивной среде используйте DNS. Внесите в зоны прямого и обратного просмотра записи обо всех хостах виртуализации и менеджере управления.
- Документируйте всё, чтобы все, кто работает с окружением, знали о его текущем состоянии и необходимых процессах.

2.2. Рекомендации по развертыванию Менеджера управления

В этом разделе описаны рекомендации по развертыванию Менеджера управления zVirt.

Менеджер управления — это центральная сущность в системе управления виртуализацией zVirt. От его работоспособности напрямую зависит доступность среды.

Ниже описаны параметры Менеджера управления, на которые стоит обратить внимание.

Таблица 1. Рекомендации относительно менеджера управления

Категория	Описание/рекомендации

Режимы развертывания	Развертывание в режиме Hosted Engine:
	• Это рекомендуемый режим развертывания zVirt, так как:
	  ◦ Обеспечение высокой доступности Менеджера управления не требует использования стороннего ПО.
	  ◦ Не требуются дополнительные серверы/среды виртуализации.
	• При развертывании в этом режиме обеспечьте наличие дополнительных хостов с ролью Hosted Engine в кластере с ВМ HostedEngine для высокой доступности Менеджера управления. Рекомендуемое количество таких хостов от 2 до 4.
	
	Развертывание в режиме Standalone:
	• Обеспечьте высокую доступность Менеджера управления средствами ПО сторонних производителей.
	
	Для продуктивной среды не разворачивайте Менеджер управления в режиме Standalone all-in-one, так как при выходе из строя хоста с Менеджером вы рискуете потерять все данные в этой среде.

Вычислительные мощности	Для обеспечения должной производительности Менеджера управления рекомендуем предусмотреть для него следующие мощности (в зависимости от планируемого размера среды): • До 50 Хостов и 200 ВМ - 4 CPU, 16 ГБ RAM. • До 100 Хостов и 500 ВМ- 8 CPU, 32 ГБ RAM. • До 200 Хостов и 1000 ВМ- 16 CPU, 64 ГБ RAM. • До 400 Хостов и 2000 ВМ- 16 CPU, 128 ГБ RAM. • При развертывании в режиме Hosted Engine необходимо, чтобы все хосты с ролью Hosted Engine всегда имели достаточное количество ресурсов для запуска ВМ HostedEngine. • При развертывании в режиме Hosted Engine рекомендуем, чтобы все хосты с ролью Hosted Engine имели одинаковое семейство процессоров.

Категория	Описание/рекомендации

Хранилище	• При развертывании в режиме HostedEngine:
	  ◦ Используйте выделенное хранилище, в котором будет располагаться только диск ВМ HostedEngine. Не используйте это хранилище для хранения образов или дисков других ВМ.
	  ◦ Не используйте локальное хранилище сервера, поскольку это приведёт к потере высокой доступности ВМ HostedEngine.
	• Необходимый размер хранилища как для режима HostedEngine, так и для Standalone вычисляется исходя из следующих значений:
	  ◦ Базовое пространство для рекомендованной структуры разделов:
	  ▪ При развертывании в режиме HostedEngine минимальный размер хранилища под виртуальный диск ВМ Hosted Engine составляет 51 ГБ.
	  ▪ При развертывании в режиме Standalone минимальный размер хранилища хоста, на котором будет разворачиваться Менеджер управления, составляет 94 ГБ.
	  ! Anaconda резервирует 20% от размера тонкого пула в группе томов для будущего расширения метаданных. Обязательно предусмотрите запас пространства под этот резерв. В ином случае авторазметка при установке zVirt Node будет экономить пространство за счет корневого раздела (/).
	  ◦ Пространство, необходимое для хранения данных DWH, зависит от размера среды. Приблизительные размеры следующие:
	  ▪ До 50 Хостов и 200 ВМ — до 1 ГБ.
	  ▪ До 100 Хостов и 500 ВМ — до 50 ГБ.
	  ▪ До 200 Хостов и 1000 ВМ — до 50 ГБ.
	  ▪ До 400 Хостов и 2000 ВМ — до 100 ГБ.

Размещение компонентов	Среда zVirt может быть настроена на размещение Менеджера управления, базы engine и базы DWH на разных хостах, но мы не рекомендуем их разделять. Раздельное размещение создаёт дополнительные точки отказа, требует резервирования каждого компонента по отдельности, а также Менеджер становится чувствителен к снижению производительности сети, соединяющей эти компоненты.
Резервное копирование	• Сразу после завершения развертывания создайте полную резервную копию и сохраните ее в отдельном месте. • Регулярно выполняйте резервное копирование Менеджера управления.

2.3. Рекомендации относительно хостов

Таблица 2. Рекомендации относительно хостов

Категория	Описание/рекомендации
Стандартизация оборудования	Для обеспечения стабильной производительности: • Размещайте в одном кластере серверы одинаковой марки и модели. • Размещайте в одном кластере серверы с процессорами одного семейства, одинаковыми сетевыми картами, идентичными HBA, RAID-контроллерами и т.д. • Если все же необходимо разместить в кластере серверы с разными поколениями процессоров, начните добавление с хоста с процессорами самого старого поколения.

Развертывание хостов	• Все хосты должны иметь полные доменные имена, разрешаемые в зонах прямого и обратного просмотра DNS.
	• Включите сеть и настройте хотя бы один интерфейс для получения доступа к хосту через SSH.
	• Настоятельно рекомендуем использовать автоматическое разбиение на разделы. Если принято решение разметить накопитель хоста вручную, следует иметь в виду следующее:
	  ◦ Для разделов необходимо использовать "LVM Thin Provisioning" с "LVM Thin pools"
	  ◦ Требуется наличие отдельных разделов **/var**, **/var/crash**, **/var/log**, **/var/log/audit**.
	• Настройте на хостах устройства ограждения для функционирования высокой доступности ВМ.

Безопасность хостов	• Не подключайте к хостам сторонние репозитории. • Устанавливайте на хосты только те пакеты и службы, которые удовлетворяют требованиям виртуализации, производительности, безопасности и мониторинга. • Не отключайте firewalld и SELinux на хостах. • Не делитесь root-доступом к хосту виртуализации. Доступ к хосту zVirt Node нужен только администраторам. Большинство административных операций, связанных со средой zVirt, выполняются с помощью Менеджера управления. Поэтому для ограничения доступа и облегчения аудита создайте индивидуальных пользователей для администраторов с минимально необходимым для решения их задач набором прав.
Дополнительные настройки хостов	Для хостов с объемом ОЗУ 128Гб и более включите поддержку hugepages.

2.4. Рекомендации по проектированию центров данных и кластеров

Таблица 3. Рекомендации по проектированию

Категория	Описание/рекомендации
Центры данных	• Используйте центры данных, чтобы разделить доступ к данным или ресурсам между потребителями. Например, если в организации есть категории пользователей "Разработчики" и "Тестировщики", создайте для этих категорий разные центры данных. • Используйте центры данных, чтобы разделить приложения, для которых используются различные планы резервного копирования.
Кластеры	• Используйте кластеры для разделения компонентов многоуровневых приложений, например, для разделения фронтэнда, бекэнда и БД приложения. • Используйте кластеры для создания естественных барьеров живой миграции или для использования правил affinity/antiaffinity. • Используйте кластеры для группировки схожего оборудования. • При создании кластера настройте политики планирования. Рекомендуемая политика — **Равномерное распределение**. Она позволит распределить ВМ в кластере на основе потребляемых ресурсов и равномерно нагрузить хосты. Конкретные параметры политик необходимо определять в индивидуальном порядке, ориентируясь на профили нагрузки.

2.5. Рекомендации относительно сетей

Таблица 4. Общие рекомендации

Категория	Описание/рекомендации

Использование агрегации (бондинга)	• Сетевые интерфейсы на продуктивных хостах должны быть связаны, предпочтительно с помощью **LACP** (**802.3ad**). Это будет способствовать общей доступности сервисов, а также увеличению пропускной способности сети.
	• Несмотря на то, что zVirt поддерживает все режимы бондинга, для сетей ВМ доступны только следующие режимы:
	  ◦ **Active Backup**.
	  ◦ **XOR**.
	  ◦ **Broadcast**.
	  ◦ **802.3ad**.
	• Если коммутатор не поддерживает **LACP** (**802.3ad**), рекомендуем использовать режим **Active Backup**.

Сети Ethernet	• 1GbE следует использовать только для трафика управления. • Сети ВМ, сети миграции, сети хранения должны использовать 10GbE и выше.

Категория	Описание/рекомендации
Использование VLAN	Мы рекомендуем активно использовать VLAN по следующим причинам: • Это позволит оптимизировать использование сети посредством QoS. • Тегирование VLAN позволяет назначать несколько логических сетей одному физическому интерфейсу хоста.
Размер MTU и jumbo-кадры	Для сетей хранения данных и сетей ВМ использование больших размеров MTU/jumbo-кадры обеспечит повышение эффективности сети. Jumbo-кадры требуют поддержки коммутаторов во всей сетевой инфраструктуре среды zVirt.
Пропускная способность и VLAN	При использовании VLAN необходимо определить приоритет и относительный размер требований к пропускной способности для продуктивных хостов, содержащих наиболее критичные рабочие нагрузки. В общем случае требования к пропускной способности следующие: • Сети отображения (SPICE) и управления — низкая пропускная способность. Поскольку трафик SPICE имеет высокую степень сжатия, а трафик управления не создаёт значительную нагрузку на сеть, можно объединить сеть отображения и сеть управления в одной VLAN. • Сеть миграции — высокая пропускная способность. • Сеть хранения (для хранилищ на базе Ethernet) — высокая пропускная способность. • Сеть взаимодействия пользователей с сервисами внутри ВМ — зависит от сервиса.
Сеть ограждения	Используйте отдельные аппаратные коммутаторы для трафика ограждения. Если трафик управления и ограждения проходят через один коммутатор, этот коммутатор становится единой точкой отказа.

Таблица 5. Дополнительные рекомендации в отношении логических сетей

Категория	Описание/рекомендации

Категория	Описание/рекомендации
Уровень центра данных	• Если к хосту добавляются дополнительные физические интерфейсы для взаимодействия с хранилищем, снимите флажок Сеть ВМ в настройках логической сети. Это позволит избежать попадания трафика ВМ в эту сеть. • Для организации безопасной эксплуатации системы виртуализации zVirt, для сети ovirtmgmt используйте отдельные физические интерфейсы, которые подключены к физически изолированной сети. При отсутствии возможности выделения отдельных физических интерфейсов, используйте выделенную VLAN. Для организация доступа из других сетей к сети ovirt-mgmt, необходимо применять межсетевой экран (при необходимости сертифицированный). • Создайте различные VLAN для подключения к хранилищам различного типа, то есть отдельную VLAN для трафика NFS и отдельную VLAN для трафика iSCSI.
Уровень кластера	• Создайте раздельные VLAN для различных приложений. • Создайте отдельную VLAN для внешнего трафика.
Использование меток	Для автоматического связывания создаваемых логических сетей с нужными хостами используйте метки.

2.6. Рекомендации относительно доменов хранения

Таблица 6. Рекомендации относительно доменов хранения

Категория	Описание/рекомендации

Категория	Описание/рекомендации

Типы хранилищ	• NFS
	  ◦ Для продуктивных рабочих нагрузок используйте серверы NFS корпоративного уровня.
	  ◦ Для увеличения скорости взаимодействия с хранилищем типа NFS:
	  ▪ Реализуйте сеть хранения на базе 10GbE или более скоростного канала.
	  ▪ Выделите сеть для NFS в отдельную VLAN.
	  ▪ Настройте сервисы, использующие NFS, на работу с определёнными портами.
	• iSCSI
	  ◦ Для продуктивных рабочих нагрузок используйте серверы iSCSI корпоративного уровня.
	  ◦ Реализуйте сеть хранения на базе 10GbE или более скоростного канала.
	  ◦ Выделите сеть для iSCSI в отдельные VLAN.
	  ◦ Настройте мультиканальное соединение.
	  ◦ Настройте аутентификацию CHAP.
	• FC
	  ◦ Является быстрым и безопасным решением, но требует высоких административных и финансовых расходов. Если в наличии есть квалифицированные кадры, или даже существует инфраструктура FC рекомендуется её использовать.
	  Несмотря на то, что zVirt поддерживает локальное хранилище, не используйте его в продуктивной среде.

Категория	Описание/рекомендации
Размеры доменов и технические ограничения	• В одном центре данных можно разместить до 50 доменов хранения. Но стоит учитывать, что каждый домен хранения постоянно сканируется на факт работоспособности. Большое количество доменов хранения в центре данных может вызвать снижение производительности и даже нестабильность SPM. Поэтому рекомендуем начинать с малого количества доменов. Если доменов формируется слишком много, возможно следует рассмотреть разделение их на центры данных. • Практических рекомендации по правильной конфигурации LUN (один большой LUN в одном домене или 100 малого размера в нескольких доменах) не существует, поскольку этот вопрос должен решаться индивидуально. Но можно дать следующие советы: ◦ Профилируйте нагрузки. Определите общую нагрузку ввода/вывода для группы ВМ. ◦ На основании результатов определите, какие ВМ смогут существовать вместе на одном LUN, а какие нет и какой объем LUN для этого потребуется. ◦ Учтите нагрузки на хранилище во время операций резервного копирования. • Существует ограничение в 1500 логических томов на домен хранения. При этом логический том формируется не только при создании виртуального диска, но и каждого снимка. Если существует вероятность превышения данного лимита, рекомендуем разделить хранилище на несколько доменов. • При использовании доменов хранения необходимо предусмотреть запас свободного пространства: ◦ При горячем перемещении диска ВМ в другой домен хранения в исходном домене необходимо свободное пространство равное размеру перемещаемого диска. ◦ При удалении снимка, необходимо свободное пространство равное размеру дельты, содержащейся в удаляемом снимке.
Домен хранения с ролью **Мастер**	• После развертывании Менеджера управления в режиме HostedEngine и добавления дополнительных доменов хранения, перенесите роль **Мастер** с домена hosted_storage на другой домен в центре данных. Это позволит избежать серьёзных проблем с ВМ при потере доступа к домену hosted_storage. Подробнее см. Поведение компонентов среды zVirt при отказе доменов хранения.

2.7. Рекомендации относительно виртуальных машин

Таблица 7. Рекомендации относительно виртуальных машин

Категория	Описание/рекомендации

Категория	Описание/рекомендации

Выделение ресурсов	**ОЗУ**
	• Начните с выделения минимального количества памяти, необходимого для работы приложения, и, при необходимости, увеличьте значение.
	ЦП
	• Переподписка (overcommit):
	  ◦ Коэфициент переподписки не должен быть больше 10:1.
	  ◦ Для высоконагруженных хостов не рекомендуется превышать 4:1.
	• Не следует отдавать ВМ слишком большое количество ядер. Это может привести к значительному снижению производительности, так как гипервизору придется каждый раз при запросе ресурсов ЦП от ВМ искать указанное количество свободных ядер.
	Особенности применения vCPU
	При создании иногда ВМ может не видеть все выделенные ей виртуальные процессоры (vCPU). Например, у ВМ под управлением Windows есть следующие ограничения по процессоров:
	• Windows 10 Home – 1 CPU
	• Windows 10 Professional – 2 CPU
	• Windows 10 Workstation – до 4 CPU
	• Windows Server 2016 – до 64 CPU
	Это ограничение не распространяется на ядра. То есть для повышения производительности вместо 8 виртуальных CPU вы можете предоставить vCPU в виде 2 сокетов по 4 ядра в каждом.
	Архитектура vCPU и NUMA
	• При назначении ядер на сокете учитывайте наличие NUMA архитектуры. Не рекомендуется назначать ВМ количество ядер на сокет (и общее количество vCPU) больше, чем доступно ядер на физическом сокете/ процессоре (узле NUMA).
	• Если количество требуемых vCPU превышает количество ядер на 1 физическом сокете (узле NUMA), нужно создать несколько виртуальных сокетов (процессоров) с необходимым количество ядер.
	• Не рекомендуется использовать нечетное количество процессоров (лучше добавить 1 vCPU).

Категория	Описание/рекомендации
Производительность ВМ	• При наличии требований к повышенной производительности ОЗУ виртуальных машин, настройте ВМ на использование больших страниц (**huge pages**). • Не используйте объединение одинаковых страниц памяти (KSM) и избыточное выделение памяти для процессов, требующих стабильно высокой производительности и низкой задержки. • Используйте KSM, когда увеличение плотности виртуальных машин (экономичность) важнее производительности.

Виртуальные диски	• Выбор типа диска зависит от приложения, которое будет использовать диск:
	  ◦ Если в ВМ работает приложение, имеющее низкую интенсивность взаимодействия с диском, то выберите диск с динамическим расширением (тонкий).
	  ◦ Если в ВМ работает приложение, интенсивно использующее дисковое пространство или оно критично к производительности диска, то используйте предварительно размеченный диск.
	• При использовании Direct LUN учитывайте следующее:
	  ◦ Direct LUN не поддерживает живую миграцию.
	  ◦ При экспорте ВМ с дисками типа Direct LUN, такие диски не будут экспортированы.
	  ◦ Диски Direct LUN не включаются в снимки ВМ
	• При подключении в ВМ нескольких дисков и наличии высоких требований к дисковой подсистеме ВМ используйте многопоточность I/O (**Выделение ресурсов > Количество потоков I/O**) и мультиочерёдность.

Шаблоны ВМ	При проектировании среды необходимо учитывать, как будут развертываться ВМ и приложения: • Настоятельно рекомендуется проектировать ВМ с помощью шаблонов. • Рекомендуется использовать комбинацию средств для автоматизации и оркестрации развертывания и настройки как виртуальных машин, так и их приложений. • Документируйте процесс развертывания.

Сертификаты

- Замена SSL-сертификата для веб-портала (zVirt 3.3 и выше)
- Замена SSL-сертификата для веб-портала (zVirt 3.2 и ниже)
- Обновление SSL сертификата на хостах и менеджере управления
- Обновление просроченного SSL сертификата на хосте
- Обновление сертификата libvirt
- Выпуск самоподписанного SSL сертификата в ЦС Windows Server для менеджера управления zVirt
- Проверка срока истечения SSL сертификатов