NUMA TECHNOLOGY®

Numa vServer

Руководство пользователя

Оглавление

© 2025 Нума Технологии, ООО

© 2025 Нума Технологии, ООО

© 2025 Нума Технологии, ООО

1. О документе

Название документа	Numa vServer. Руководство пользователя
Обозначение документа	643.АМБН.00021-01 34 01
Версия документа	1.2.1
Идентификация изделия	Серверная доверенная виртуальная среда функционирования программных средств Numa vServer 643.АМБН.00021-01
Сертификат соответствия ФСТЭК России	№ 4580 от 23.09.2022
Идентификация разработчика	ООО "НумаТех"
Официальная электронная документация по продукту	kb.numavserver.ru

© 2025 Нума Технологии, ООО

2. Администрирование пулов ресурсов

2.1. Определение пула ресурсов

Пул ресурсов – это совокупность из одного или нескольких серверов Numa vServer, соединённых друг с другом в общую единицу, на которой возможно развертывание, запуск и исполнение ВМ. Один пул может объединить до 64 серверов.

В пуле ресурсов есть один физический сервер, называемый мастером, который предоставляет интерфейс для администрирования всем пулом. По мере надобности мастер передает команды отдельным участникам.

При использовании общего хранилища пул ресурсов позволяет запускать виртуальные машины на любом сервере Numa vServer, имеющим достаточный объем оперативной памяти для функционирования ВМ, и в дальнейшем динамически перемещаться между серверами с минимальными простоями. При сбое отдельного сервера администратор может перезапустить отказавшую ВМ на другом сервере того же пула ресурсов. Если для пула включен механизм обеспечения высокой доступности (High Availability, HA), то в случае отказа сервера ВМ будут автоматически перемещены на работающий сервер.

> **Примечание**
>
> Если происходит отказ мастера пула, то автоматическое переизбрание мастера происходит только если в пуле настроен механизм обеспечения высокой доступности.

2.2. Требования к созданию пула ресурсов

При конфигураии пула учитывайте нижеприведенные требования.

2.2.1. Требования к аппаратному обеспечению

- Вендор ЦП (Intel, AMD) должен быть одинаковым на всех серверах.
- На серверах пула должна быть установлена одна версия программного обеспечения Numa vServer.

В зависимости от схожести ЦП, пул может быть одним из следующих типов:

- Гомогенный пул — это совокупность серверов с идентичными ЦП. ЦП на сервере, присоединяющемся к гомогенному пулу ресурсов, должны быть тех же вендоров, моделей и характеристик, что и ЦП на серверах, уже находящихся в пуле.
- Гетерогенный пул — это совокупность серверов с разными ЦП. На практике часто бывает трудно получить несколько серверов с одинаковыми процессорами, поэтому допускаются незначительные изменения. Если необходимо, чтобы в вашей среде серверы с разными ЦП находились в одном и том же пуле ресурсов, вы можете принудительно объединить пул (см. раздел Создание гетерогенного пула ресурсов).

2.2.2. Требования к конфигурации сервера, присоединяющегося к пулу

- Сервер не является членом существующего пула ресурсов.
- На сервере не настроено общее хранилище.
- На сервере не размещены ни работающие, ни приостановленные виртуальные машины.
- На виртуальных машинах сервера не ведутся активные операции, такие как завершение работы виртуальной машины.
- Системное время на сервере синхронизировано с системным временем мастера пула (например, с помощью NTP).

© 2025 Нума Технологии, ООО

- Интерфейс управления сервером не агрегирован. Вы можете настроить интерфейс управления, когда сервер успешно присоединится к пулу.
- Управляющий IP-адрес является статическим, либо настроен на самом сервере, либо с помощью соответствующей конфигурации на DHCP-сервере.

Серверы Numa vServer в пулах ресурсов могут содержать различное количество физических сетевых интерфейсов и иметь локальные хранилища данных различного размера.

2.2.3. Требования к хранилищам данных

Преимущества пулов (например, возможность динамически выбирать, на каком хосте Numa vServer запускать ВМ) доступны, только при наличии хотя бы одного подключенного общего хранилища. При возможности необходимо отложить создание пула до тех пор, пока подобное хранилище не станет доступно. Когда это произойдёт, рекомендуется переместить существующие ВМ и диски, которых хранились локально, в общее хранилище пула.

> Примечание
>
> Серверы, предоставляющие общее хранилище NFS, iSCSI, SAMBA для пула, должны иметь статический IP-адрес или быть адресуемыми в DNS.

2.3. Создание пула ресурсов

Когда новый сервер присоединяется к пулу ресурсов, присоединяющийся сервер синхронизирует свою локальную базу данных со всей базой данных пула и наследует некоторые параметры из пула:

- конфигурации ВМ, локального и удаленного хранилища добавляются в общую базу данных пула. Если возможно или необходимо сделать ресурсы общими, они будут собраны в объединённом хосте в пуле;
- присоединяемый сервер наследует существующие общие хранилища для пула, также создаются соответствующие записи физического блочного устройства (PBD) так, чтобы новый сервер мог автоматически получить доступ к существующему общему хранилищу;
- сетевая информация наследуется присоединяемым сервером частично: наследуются структурные особенности сетевого адаптера, виртуальных сетей VLAN, агрегаций сетевых интерфейсов. Данные установленных политик не наследуются. К подобным свойствам, которые не могут получить значения наследованием и должны быть переконфигурированы вручную, относятся:
  - IP-адреса интерфейсов управления, которые сохраняются из исходной конфигурации;
  - местонахождение интерфейса управления, которое не меняется по сравнению с исходной конфигурацией. Например, если другие серверы пула имеют свои интерфейсы управления в агрегации интерфейсов, то добавляемый сервер должен быть в обязательном порядке включён в агрегацию после вхождения в пул;
  - сетевые адаптеры, выделенные для соединения с хранилищем, которые должны быть пересвязаны с новым хостом через интерфейс командной строки, и физические блочные устройства, которые для правильного распределения трафика должны быть переподключены (это вызвано отсутствием операции присвоения IP-адресов при объединении пула; без правильной настройки интерфейсы, выделенные для соединения с хранилищем, бесполезны). Более подробно о настройке сетевых интерфейсов с помощью команд см. в разделе Настройка сетевого интерфейса, выделенного для соединения с хранилищем.

> Примечание
>
> Вы можете присоединить новый сервер к пулу ресурсов только в том случае, если интерфейс управления сервером находится в той же VLAN, что и пул ресурсов.

© 2025 Нума Технологии, ООО

2.3.1. Добавление сервера в пул ресурсов

Для добавления сервера host2 в пул ресурсов с мастером host1 выполните следующие действия:

1. Откройте консоль на сервере host2.
2. Выполните следующую команду:

```
xe pool-join master-address=<host1-IP-address> master-username=<administrator-username> master-password=<password>
```

где:

- `master-address` – IP-адрес или доменное имя сервера host1;
- `master-username` – логин администратора, присвоенный при установке Numa vServer на сервер host1;
- `master-password` – пароль администратора, присвоенный при установке Numa vServer на сервер host1.

2.3.2. Создание гетерогенного пула ресурсов

Numa vServer позволяет объединять в пул отличающимся по своим характеристикам серверам. Такой пул принято называть гетерогенным. Создание гетерогенного пула возможно при использовании технологий в процессорах Intel (FlexMigration) и AMD (Extended migration), которые обеспечивают процессор свойствами «маскирования» (masking) или «выравнивания» (leveling). Эти свойства позволяют конфигурировать процессор так, чтобы он отображал другие марку, модель и функциональность, чем он есть на самом деле. Эта функция позволяет вам создавать пулы ресурсов с разнородными ЦП, но при этом безопасно поддерживать живую миграцию.

Условия создания гетерогенного пула:

- Процессоры сервера, вступающего в пул, должны быть от того же поставщика (AMD, Intel), что и процессоры на серверах, которые уже находятся в пуле. Однако идентичность семейства, модели и версии не обязательна.
- Процессоры сервера, вступающего в пул, должны поддерживать технологию FlexMigration фирмы Intel или технологию Extended Migration фирмы AMD.
- Характеристики процессоров сервера, являющихся членами пула, должны составлять подмножество набора характеристик процессоров сервера, вступающего в пул.
- сервер, вступающий в пул, и серверы, находящиеся в пуле, должны работать с одинаковыми версиями программного обеспечения Numa vServer.

Для объединения серверов host1 и host2 в гетерогенный пул ресурсов выполните следующие действия:

1. Откройте консоль на сервере host2.
2. Выполните следующую команду:

```
xe pool-join master-address=<host1-IP-address> master-username=<administrator-username> master-password=<password> force=true
```

где:

- `master-address` – IP-адрес или доменное имя сервера host1;
- `master-username` – логин администратора, присвоенный при установке Numa vServer на сервер host1;
- `master-password` – пароль администратора, присвоенный при установке Numa vServer на сервер host1.

Любые изменения в наборе конфигураций пула не влияют на виртуальные машины, которые в данный момент работают в пуле. Работающая ВМ продолжает использовать набор конфигураций, который был применен при запуске. Этот набор конфигураций фиксируется при загрузке и сохраняется при переносе, приостановке и возобновлении операций. Если уровень пула падает, когда к нему присоединяется сервер с более низкими характеристиками, работающую виртуальную машину можно перенести на любой сервер в пуле, кроме недавно добавленного. При перемещении или миграции виртуальной машины на другой сервер в пределах или между пулами Numa vServer сравнивает набор функций виртуальной машины с набором функций сервера назначения. Если установлено, что наборы функций совместимы, виртуальная машина может

© 2025 Нума Технологии, ООО

мигрировать. Это позволяет виртуальной машине свободно перемещаться внутри и между пулами независимо от того, какие функции использует виртуальная машина.

При создании гетерогенного пула маскирование процессора и выравнивание процессора по функциональным возможностям осуществляется автоматическом режиме и не требует ввода дополнительных команд и конфигураций.

2.4. Присвоение имени пулу ресурсов

По умолчанию серверы Numa vServer принадлежат безымянному пулу или пулу, имеющего имя мастер сервера. Для присвоения нового имени пулу ресурсов выполните команду:

```
xe pool-param-set name-label=<new-pool=name> uuid=<pool-uuid>
```

Для поиска нужного идентификатора `pool_uuid` воспользуйтесь функцией автодополнения (клавиша `Tab ↹`) или командой `xe pool-list`.

2.5. Добавление системы хранения с общим доступом

> **Подсказка**
>
> Полный список поддерживаемых типов хранилищ приведен в разделе Создание и настройка хранилищ данных.

В данном разделе описывается пример создания хранилища данных с общим доступом на существующем сервере NFS.

Для добавления общего NFS-хранилища к пулу ресурсов через CLI Numa vServer выполните следующие действия:

1. Откройте консоль на любом сервере в пуле.
2. Создайте хранилище данных на `<server:/path>`:

```
xe sr-create content-type=user type=nfs name-label=<sr-name> shared=true device-
config:server=<server-IP-address> device-config:serverpath=<path>
```

   где параметр `device-config:server` – адрес сервера, на котором запущен сервер NFS, параметр `device-config:serverpath` – путь к каталогу на сервере NFS. После установки параметра `shared=true` общее хранилище будет автоматически присоединено к каждому серверу в пуле и в дальнейшем любые подключаемые к пулу серверы будут присоединены к этому хранилищу. UUID созданного хранилища данных будет выведен на экран.
3. Узнайте UUID пула:

```
xe pool-list
```

4. Задайте хранилище по умолчанию в качестве места хранения для участников пула:

```
xe pool-param-set uuid=<pool-uuid> default-SR=<sr-uuid>
```

   После выполнения данной команды все будущие ВМ будут создавать свои диски в общем хранилище (см. раздел Создание и настройка хранилищ данных для получения информации по созданию других типов общих хранилищ).

© 2025 Нума Технологии, ООО

2.6. Управление серверами в пуле ресурсов

2.6.1. Выключение и перезапуск сервера

Рекомендуем использовать команды xe для выключения или перезапуска серверов Numa vServer. Не используйте аппаратные методы сброса для выключения и/или перезапуска серверов во время их нормальной работы. Это может привести к неожиданному поведению серверов и пула.

Чтобы завершить работу или перезапустить сервер, используйте следующие команды:

1. Запретите запуск или миграцию любых новых виртуальных машин на выбранный сервер:

```
xe host-disable host=<host-name>
```

2. При необходимости перенесите все работающие виртуальные машины с сервера:

```
xe host-evacuate uuid=<host-uuid>
```

3. Выключите или перезапустите хост с помощью одной из следующих команд:

   • Чтобы корректно завершить работу хоста:

   ```
   xe host-shutdown host=<host-name>
   ```

   • Для корректной перезагрузки хоста:

   ```
   xe host-reboot host=<host-name>
   ```

2.6.2. Вывод сервера из пула ресурсов

> Внимание!
>
> 1. Перед выводом сервера из пула убедитесь, что все ВМ, запущенные на этом сервере, выключены или перенесены на другие серверы, иначе сервер нельзя будет вывести из пула.
> 2. Нельзя извлекать сервер, если он содержит важные данные на его локальном диске, так как все данные будут удалены после извлечения. Если нужно сохранить эти данные, следует скопировать ВМ в общее хранилище пула командой:
>
> ```
> xe vm-copy sr-uuid=<sr-uuid> vm=<vm-name> new-name-label=<new-vm-name>
> ```

Для вывода сервера из пула ресурсов выполните следующие действия:

1. Откройте консоль на любом сервере в пуле.
2. Узнайте UUID сервера:

```
xe host-list
```

3. Извлеките выбранный сервер из пула:

© 2025 Нума Технологии, ООО

```
xe pool-eject host-uuid=<host-uuid>
```

После вывода сервера из пула, сервер будет перезагружен, переинициализирован и возвращен в исходное состояние (состояние после инсталляции).

После извлечения сервера из пула сохранённые на нём ВМ будут отображены в базе данных пула и видны другими участникам пула. Они не могут быть запущены, пока местоположения ассоциированных с ними виртуальных дисков в общей хранилище не станут видны серверам пула или пока диски не будут удалены. По этой причине рекомендуется перемещать любое локальное хранилище в общее хранилище при вводе нового сервера в пул, это позволит вывести из пула любой отдельный сервер без потери данных.

2.6.3. Подготовка серверов пула к обслуживанию

Перед проведением на сервере, входящего в пул, операций по обслуживанию необходимо заблокировать данный сервер (это предотвратит несанкционированный старт ВМ на нем), затем переместить его ВМ на другой сервер пула.

> **Примечание**
>
> Перевод в режим обслуживания мастера пула приведет к потере данных циклической базы данных за последние 24 часа для недействующих ВМ. Причиной является синхронизация резервных копий, которая происходит каждые 24 часа.

Для подготовки участника пула к обслуживанию и возобновления его функционирования после проведения обслуживания выполните следующую последовательность действий:

1. Заблокируйте сервер:

```
xe host-disable uuid=<host_uuid>
```

2. Переместите ВМ к другим серверам в пуле.

```
xe host-evacuate uuid=<host_uuid>
```

3. Выполните требуемые операции по обслуживанию сервера.
4. После выполнения операций по обслуживанию разблокируйте сервер:

```
xe host-enable uuid=<host_uuid>
```

После разблокировки обслуженного сервера на нем можно запустить ВМ.

© 2025 Нума Технологии, ООО

3. Администрирование сети

В данном разделе описано администрирование сетей Numa vServer, включая сети VLAN, и методы агрегирования сетевых адаптеров (NIC bonds), а также методы управления конфигурацией сети и устранения неполадок.

Следует заметить, что используемым по умолчанию в Numa vServer сетевым стеком является виртуальный коммутатор, однако при желании администратор может использовать стек сети на основе Linux Bridge (см. раздел Сети на основе стека виртуального коммутатора).

Для получения непосредственных практических инструкций можно использовать следующие разделы:

- о создании сетей для одиночных хостов Numa vServer (см. раздел Создание сетей на автономном сервере);
- об организации сети между хостами Numa vServer, объединёнными в пул (resource pool) (см. раздел Создание сетей в пуле ресурсов);
- о создании VLAN для хостов Numa vServer (см.раздел Создание виртуальных локальных сетей (VLAN));
- о настройке агрегаций сетевых интерфейсов (адаптеров) одиночных хостов Numa vServer (см. раздел Агрегирование сетевых адаптеров автономного сервера);
- о настройке агрегаций сетевых интерфейсов (адаптеров) для серверов Numa vServer, объединённых в общий пул (см. раздел Агрегирование сетевых адаптеров в пуле).

> **Примечание**
>
> Термин «интерфейс управления» («управляющий интерфейс», management interface) используется далее для обозначения сетевого интерфейса, который служит для передачи управляющего трафика.

3.1. Поддержка сетевых интерфейсов

Numa vServer поддерживает до 16 физических сетевых интерфейсов (или до 8 агрегированных сетевых интерфейсов) на одном сервере и до 7 виртуальных сетевых интерфейсов на одну ВМ.

> **Предупреждение**
>
> Numa vServer предоставляет автоматическую настройку и управление сетевыми адаптерами посредством интерфейса командной строки. Не рекомендуется редактировать конфигурационные файлы сети напрямую.

3.2. Сети на основе стека виртуального коммутатора

Виртуальный коммутатор значительно упрощает администрирование виртуальных сетей – все настройки и данные статистики ВМ остаются связанными с ВМ, даже если она мигрирует с одного сервера общего пула на другой.

При использовании контроллера программно-определяемых сетей (SDN-controller), поддерживающего протокол OpenFlow, виртуальные коммутаторы обеспечивают дополнительную функциональность, например, списки управления доступом (Access Control List, ACL).

> **Внимание!**
>
> Контроллер программно-определяемых сетей не входит в стандартный состав дистрибутива Numa vServer.

© 2025 Нума Технологии, ООО

Для определения сетевого стека, настроенного в настоящее время, выполните команду:

```
xe host-list params=software-version
```

В полученных результатах следует искать параметр `network_backend`:

- если в качестве сетевого стека настроен vSwitch, то в результатах выполнения команды будет выведена следующая строка:

```
network_backend: openvswitch
```

- если в качестве сетевого стека настроен Linux-мост (Linux bridge), в результатах выполнения команды будет выведена следующая строка:

```
network_backend: bridge
```

Для возврата к стеку Linux-моста выполните команду:

```
xe-switch-network-backend bridge
```

После её выполнения следует перезагрузить сервер.

> **Предупреждение**
>
> Стек Linux-моста не поддерживает протокол OpenFlow, межсерверные частные сети (Cross Server Private Networks) и не может управляться посредством контроллера программно-определяемых сетей.

3.3. Описание сетевых возможностей Numa vServer

В этом разделе описываются общие концепции, используемые при построении сетей в среде Numa vServer.

Во время установки Numa vServer автоматически создаётся по одной сети для каждого физического интерфейса сетевой карты. Когда администратор добавляет сервер в общий пул ресурсов, сети по умолчанию объединяются так, чтобы все физические сетевые адаптеры с одним именем устройства оказались прикреплены к одной и той же сети.

Как правило, администратор добавляет новую сеть только при необходимости создания внутренней сети, нового VLAN или агрегации сетевых адаптеров (NIC bond).

В Numa vServer может быть настроено четыре различных типа сетей:

- внешние сети (external networks), ассоциированные с физическим интерфейсом и обеспечивающие мост между виртуальными машинами и физическим сетевым интерфейсом, подключенного к физическим сетям передачи данных;
- агрегированные сети (bonded networks) создают связь между двумя и более физическими сетевыми интерфейсами для получения единого высокопроизводительного и высокодоступного канала между виртуальной машиной и физической сети передачи данных;
- частные сети одиночного сервера (single-server private networks) не имеют никакой связи с физическим сетевым интерфейсом и могут использоваться для обеспечения соединения между виртуальными машинами на данном сервере, без возможности связи со внешними сетями;
- межсерверные частные сети (cross-server private networks) позволяет виртуальным машинам, развёрнутым на разных серверах, общаться друг с другом при помощи программно-определяемых частных сетей (для создания такой сети обязательно наличие контроллера программно-определяемых сетей).

© 2025 Нума Технологии, ООО

> Примечание
>
> Поведение некоторых сетевых функций различается в зависимости от того, используется один сервер Numa vServer или же пул серверов. Данный раздел содержит информацию о функциях, выполняющихся в обоих случаях, сопровождая описание каждой из них дополнительной информацией.

3.4. Сетевые объекты

В разделе описывается три типа сетевых объектов, существующих на стороне сервера и являющихся отражением трёх независимых сетевых сущностей:

- PIF (Physical Interface File) является отображением физического сетевого адаптера на сервере Numa vServer. Объекты PIF имеют имя, описание, UUID, параметры сетевой карты, которую они представляют, а также сеть и сервер, к которым они подключены;
- VIF (Virtual Interface File) является отображением виртуального сетевого адаптера на виртуальной машине. Объекты VIF имеют имя, описание, UUID, а также сеть и виртуальную машину, к которой они подключены;
- Network (сеть) представляет собой виртуальный Ethernet-коммутатор на сервере. Объекты типа Network имеют имя, описание, UUID и набор подключенных к ним VIF и PIF.

Интерфейс командной строки позволяет настраивать параметры работы в сети, управлять тем, какой из сетевых интерфейсов используется для передачи управляющего трафика, а также настраивать дополнительные возможности сети: виртуальные локальные сети (VLAN) и агрегации сетевых адаптеров (NIC bonds).

3.4.1. Сетевой объект Network (сеть)

Каждый сервер Numa vServer имеет одну или более сетей, являющихся виртуальными Ethernet-коммутаторами. Сети, не связанные с PIF, считаются внутренними и могут быть использованы для обеспечения связи только между виртуальными машинами, без возможности связи со внешними сетями. Сети, ассоциированные с PIF, считаются внешними и являются связующим звеном между VIF и PIF, обеспечивают подключение ВМ к сетям передачи данных доступным через физический интерфейс сетевого адаптера.

3.5. Виртуальные локальные сети (VLAN)

Виртуальные локальные сети (VLAN), согласно стандарту IEEE 802.1Q, позволяют создавать на одной физической сети несколько логических сетей. Сети Numa vServer могут работать с виртуальными локальными сетями различными способами.

> Примечание
>
> Все поддерживаемые конфигурации виртуальной локальной сети в равной степени применимы как к пулам, так и к автономным серверам, как в случаях использования агрегации сетевых интерфейсов, так и без таковой.

3.5.1. Использование VLAN с управляющими интерфейсами

Интерфейс управления может быть настроен на VLAN на порту коммутатора, настроенного как магистральный порт (trunk port) или порт режима доступа (access port).

© 2025 Нума Технологии, ООО

3.5.2. Использование VLAN с виртуальными машинами

Порты коммутатора, настроенные согласно стандарту IEEE 802.1Q в качестве магистральных для виртуальных сетей, могут быть использованы в сочетании с функциями Numa vServer VLAN для подключения гостевых виртуальных сетевых интерфейсов (VIF) к конкретным VLAN. В этом случае сервер выполняет функции VLAN Tagging / Untagging для гостевой системы, которой недоступны никакие сведения о конфигурации VLAN.

Виртуальные локальные сети сервера представляются дополнительными PIF-объектами в соответствии с заданными тегами виртуальных сетей. Сети Numa vServer могут быть подключены как к PIF-объекту, представляющему физический сетевой адаптер или к PIF-объекту, связанному с виртуальной сетью, помеченный её тегом. Подробные инструкции, касающиеся создания виртуальных локальных сетей для серверов Numa vServer (автономных или входящих в пул), приведены в разделе Создание виртуальных локальных сетей (VLAN).

3.5.3. Использование VLAN с сетевыми адаптерами, выделенными для соединения с хранилищем

Сетевые адаптеры, выделенные для соединения с хранилищем (также известные как IP-enabling NIC или просто «интерфейсы управления»), могут быть сконфигурированы таким образом, чтобы использовать порты с нативной поддержкой Native VLAN (порты в режиме доступа) или магистральные порты и виртуальные сети Numa vServer. Подробнее о конфигурации сетевых адаптеров, выделенных для соединения с хранилищем, см. в разделе Настройка сетевого интерфейса выделенного для соединения с хранилищем.

3.5.4. Объединение интерфейсов управления и гостевых VLAN на сетевом адаптере автономного хоста

Порт виртуального коммутатора может быть сконфигурирован для одновременной работы с Native VLAN и Tagged VLAN, позволяя одному сетевому адаптеру сервера использоваться, например, для интерфейса управления и для соединения VIF-объектов гостевой системы с определенными идентификаторами виртуальных сетей.

3.6. Jumbo-кадры

Jumbo-кадры (или сверхдлинные Ethernet-кадры) могут использоваться для оптимизации производительности сетевого трафика. Jumbo-кадры называются Ethernet-кадры, содержащие больше, чем 1500 байтов полезной нагрузки. Обычно они используются для достижения лучшей пропускной способности, уменьшая загрузку на память системной шины и процессора.

> **Примечание**
>
> Numa vServer поддерживает Jumbo-кадры только при использовании vSwitch в качестве сетевого стека сервера.

Администратор должен учитывать следующие особенности использования Jumbo-кадров:

- поддержка Jumbo-кадров настраивается на уровне пула;
- vSwitch должен быть сконфигурирован в качестве сетевого стека по умолчанию на всех сетевых устройствах в пуле;
- каждое устройство в подсети должно быть соответствующим образом настроено на использование Jumbo-кадров;
- рекомендуется, чтобы администратор включал поддержку Jumbo-кадров только для выделенной сети хранения;
- поддержка Jumbo-кадров в сети управления отсутствует;
- Jumbo-кадры не поддерживаются для использования на BM.

Для использования Jumbo-кадров следует установить значение параметра Maximum Transmission Unit (MTU) в диапазоне между 1500 и 9216. Это может быть сделано при помощи интерфейса командной строки `xe`.

© 2025 Нума Технологии, ООО

3.7. Агрегация сетевых интерфейсов

Агрегирование сетевых адаптеров (англ. NIC bond или NIC teaming) повышает доступность и/или пропускную способность, позволяя администраторам сконфигурировать два или более сетевых адаптера вместе таким образом, чтобы они логически функционировали как единый адаптер. Все связанные таким образом сетевые адаптеры будут совместно использовать один MAC-адрес.

В случае сбоя на одном из сетевых адаптеров агрегированного порта, сетевой трафик будет автоматически перенаправлен через другой сетевой адаптер. Numa vServer поддерживает до 8 сетевых интерфейсов в одной группе агрегации.

Numa vServer поддерживает следующие режимы агрегации:

- активно-активный (active-active);
- активно-пассивный (active-passive);
- агрегацию с использованием протокола LACP (Link Aggregation Control Protocol).

Число поддерживаемых адаптеров и поддерживаемый режим связывания изменяются согласно выбранному сетевому стеку.

LACP-агрегация доступна только при использовании сетевого стека vSwitch, тогда как активно-активная и активно-пассивная агрегация – как для vSwitch, так и для сетевого стека Linux Bridge.

Когда в качестве сетевого стека выступает vSwitch, есть возможность связать вместе от 2 до 4 сетевых адаптеров, в случае использования Linux Bridge – только 2 сетевых адаптера.

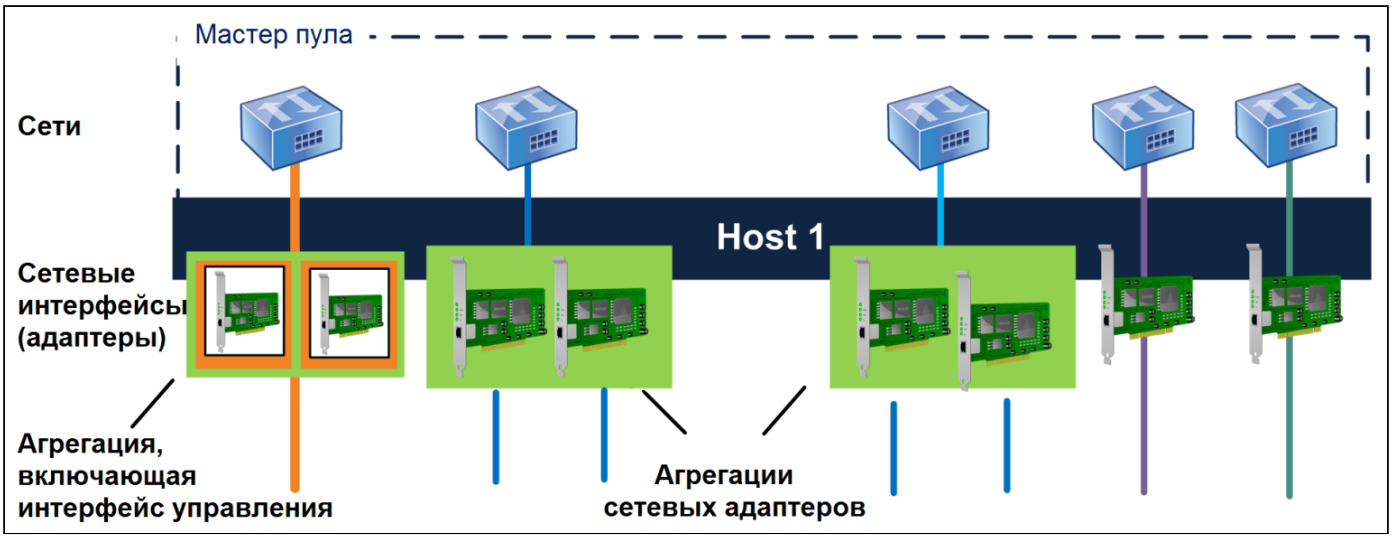


Схема сетевого взаимодействия сервера, когда некоторые пары сетевых адаптеров агрегированы

На рисунке выше интерфейс управления находится в группе агрегации двух сетевых адаптеров. Numa vServer будет использовать эту связь для управляющего трафика. Помимо агрегации сетевых адаптеров, предназначенной для управляющего трафика, сервер также использует другие две пары групп агрегаций и два независимых друг от друга сетевых адаптера для трафика ВМ.

Все режимы агрегации поддерживают автоматическое восстановление после сбоя (failover), однако не все режимы позволяют всем соединениям быть активными для всех типов трафика. Numa vServer поддерживает агрегирование следующих типов сетевых адаптеров:

- сетевые адаптеры (интерфейсы) общего назначения (не управляющие). Можно объединять сетевые адаптеры, которые Numa vServer использует исключительно для трафика ВМ. Агрегация этих сетевых адаптеров не только обеспечивает отказоустойчивость, но и также равномерно распределяет трафик многочисленных ВМ между сетевыми адаптерами;
- интерфейсы управления. Можно связать сетевой адаптер, обслуживающий трафик управления с другим сетевым адаптером так, чтобы последний обеспечил его резервирование, рекомендуемый тип такой агрегации - активно-активно;
- вторичные интерфейсы. Можно объединить сетевой адаптер, сконфигурированный в качестве вторичного интерфейса (например, для обмена данными с хранилищем). Однако для большинства серверов, выступающих в роли инициаторов обмена с системами хранения посредством протокола iSCSI, рекомендуется настройка многоканального (multipath) соединения вместо агрегации сетевых адаптеров.

© 2025 Нума Технологии, ООО

Агрегацию можно создать, если VIF уже использует один из адаптеров, которые предполагается агрегировать: трафик ВМ будет автоматически перемещён на новый связанный сетевой интерфейс.

В Numa vServer агрегация сетевых адаптеров представляется дополнительным PIF-объектом. Агрегации сетевых адаптеров в Numa vServer полностью включаются в категорию базовых физических устройств (PIF).

> Примечание
>
> Создание агрегации, содержащей только один сетевой адаптер, не поддерживается.
>
> Создание агрегации не поддерживается на сетевых картах, которые передают трафик FCoE.

3.7.1. Основные положения об IP-адресации агрегированных интерфейсов

Агрегированный сетевой интерфейс либо имеют один IP-адрес, либо не имеют IP-адресов, как показано ниже:

- Сети управления и сети обмена данными с хранилищем:
  - если агрегировать управляющий или вторичный интерфейс, единственный IP-адрес будет присвоен всей агрегации в целом. То есть отдельный интерфейс, входящий в агрегацию не имеет своего собственного IP-адреса. Агрегированное соединение рассматривается сервером как единое логическое соединение;
  - если агрегированные интерфейсы используются для трафика, не связанного с виртуальной машиной, например, для подключения к общему сетевому хранилищу, то ему можно настроить IP-адрес. Однако если назначен IP-адрес одному из сетевых интерфейсов (то есть создали интерфейс управления или дополнительный интерфейс), этот IP-адрес автоматически назначается всей агрегации;
  - если администратор агрегирует интерфейс управления или вторичный интерфейс с сетевым адаптером, не имеющим IP-адреса, агрегация принимает имеющийся IP-адрес соответствующего интерфейса автоматически;
- Сети виртуальных машин. Если агрегированные сетевые интерфейсы используются для трафика виртуальных машин, то необязательно настраивать IP-адрес для агрегированного интерфейса. Это происходит потому, что агрегация работает на уровне 2 модели OSI, и на этом уровне не используется IP-адресация.

3.7.2. Типы агрегаций

Numa vServer предоставляет три различных типа агрегаций:

- активно-активный режим (Active-Active mode), с балансировкой трафика виртуальной машины между сетевыми интерфейсами агрегации (см. раздел Активно-активный тип агрегации (Active-Active mode));
- активно-пассивный режим (Active-Passive mode), в котором только один сетевой интерфейс активно осуществляет передачу трафика (см. раздел Активно-пассивный тип агрегации (Active-Passive mode));
- LACP-агрегация (LACP Link Aggregation), при которой активные и резервные сетевые интерфейсы согласованы между коммутатором и сервером (см. раздел Агрегация на основе протокола LACP (Link Aggregation Control Protocol)).

> Примечание
>
> При агрегировании параметры задержки Up Delay и Down Delay выставляются, соответственно, в 31000 и 200 мс. Большие значения Up Delay являются оправданными из-за того, что некоторые коммутаторы тратят довольно существенное время на фактическое включение порта. Для получения информации об изменении задержки см. раздел Изменение времени задержки Up Delay трафика агрегации.

© 2025 Нума Технологии, ООО

3.7.3. Состояние агрегации

Numa vServer обеспечивает регистрацию состояний для агрегированных подключений в журнале событий каждого сервера. Если один или более из агрегированных интерфейсов перестали работать или были восстановлены, в журнал заносится соответствующая запись. Аналогично можно запросить статус интерфейсов в составе агрегации, используя параметр `links-up`:

```
xe bond-param-get uuid=<bond_uuid> param-name=links-up
```

Numa vServer проверяет состояние интерфейсов в агрегациях приблизительно каждые 5 секунд. Следовательно, если в пятисекундном окне произойдёт отказ ещё каких-то интерфейсов, эти отказы не будут зарегистрированы до следующей проверки состояния.

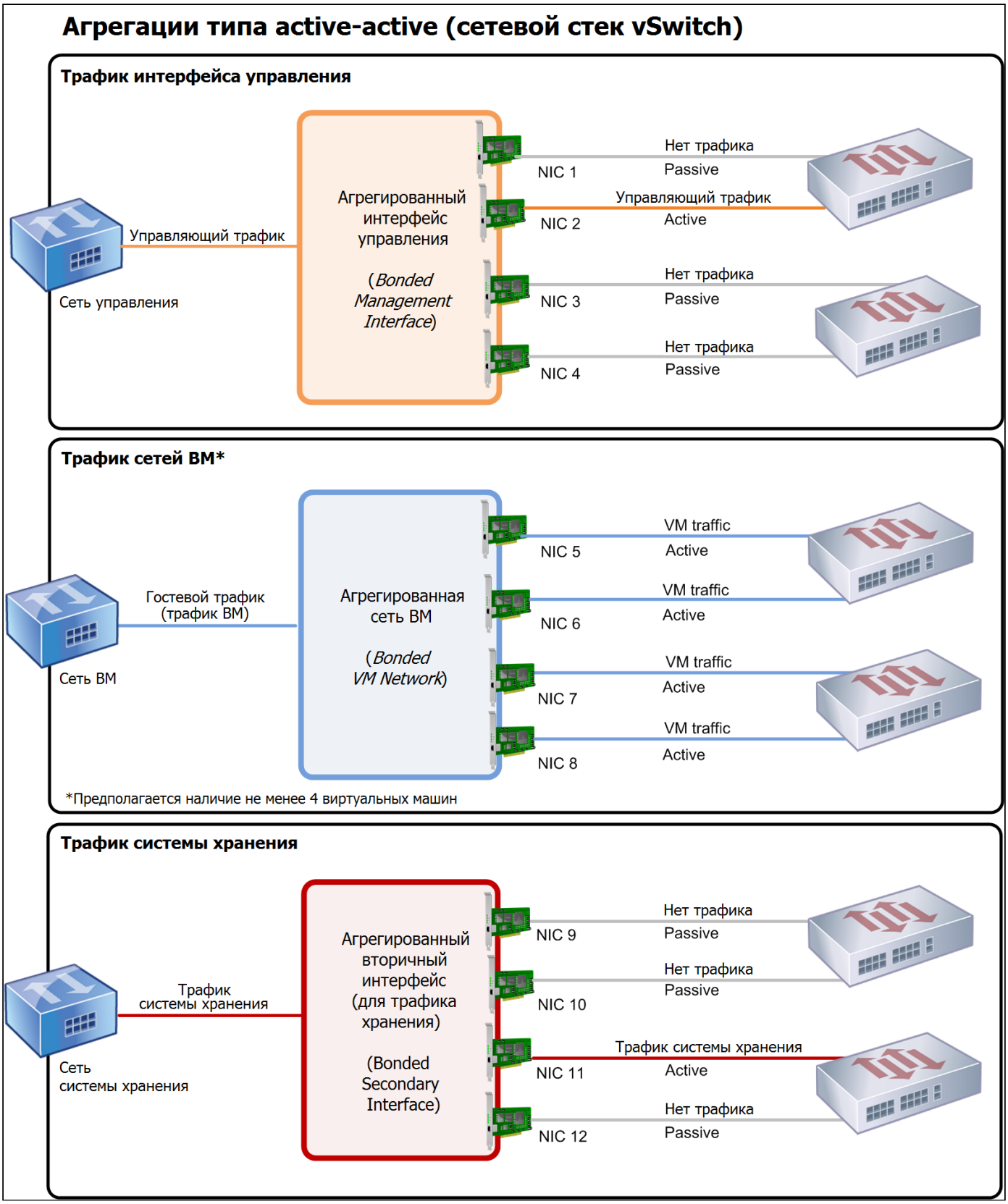
Журналы событий доступны в виде файла `/var/log/journal/38855a3423a049e2be9042a56f9aa8a3/system.journal` на каждом хосте.

3.7.4. Активно-активный тип агрегации (Active-Active mode)

Активно-активный (Active-Active mode) – конфигурация по принципу «активный – активный» для передачи гостевого трафика: оба сетевых адаптера могут передавать трафик ВМ одновременно. Когда агрегация используется для трафика управления, только один сетевой адаптер в связи может направить трафик: другой сетевой адаптер остается неиспользованным и обеспечивает поддержку обработки отказа (failover). Активно-активный режим является режимом по умолчанию, когда в качестве сетевого стека используется Linux Bridge или vSwitch.

Когда активно-активная агрегация используется с Linux Bridge, возможна агрегация только из двух сетевых адаптеров. При использовании vSwitch в качестве сетевого стека становится возможно агрегировать два, три, или четыре адаптера в активно-активном режиме. Однако в активно-активном режиме агрегирование трёх или четырёх сетевых адаптеров обычно эффективно только для трафика виртуальных машин.

© 2025 Нума Технологии, ООО



Активно-активный тип агрегации

Numa vServer может отправлять трафик через два или большее количество сетевых адаптеров, только когда имеется более одного MAC-адреса, ассоциированного с агрегацией адаптеров. Numa vServer может использовать виртуальные MAC-адреса в VIF-объекте, чтобы распараллелить трафик через несколько соединений. В соответствии с типом трафика:

© 2025 Нума Технологии, ООО

- трафик ВМ. При агрегировании сетевых адаптеров, переносящих только трафик ВМ, все соединения будут являться активными, и распределение трафика ВМ по адаптерам внутри агрегации будет балансировать между интерфейсами. Трафик отдельного VIF никогда не разделяется между сетевыми картами;
- трафик управления или обмена с системой хранения. Только одно из соединений (то есть сетевых адаптеров) в агрегации является активным, другие же остаются неиспользованными, если только активная роль не передаётся им в результате сбоя основного интерфейса. Таким образом, конфигурация, при которой интерфейс управления или вторичный интерфейс агрегируются с другими, обеспечивает отказоустойчивость.
- смешанный трафик. Если агрегация сетевых адаптеров передаёт смесь из IP-трафика обмена с хранилищем и гостевого трафика ВМ, только гостевой трафик и управляющий трафик домена пользуются возможностью балансировки трафика.

3.7.4.1. Балансировка трафика в режиме агрегации активно-активно

Numa vServer балансирует распределение трафика между сетевыми адаптерами на основе MAC-адреса, с которого отправляется пакет. Для трафика управления существует только один MAC-адрес источника, поэтому в активном-активном режиме используется только одна сетевая карта, и трафик не распределяется. Трафик распределяется на основе двух следующих факторов:

- ВМ и связанный с ней VIF-объект, отправляющие или получающие сетевые пакеты;
- количество пересылаемых данных (в килобайтах).

Numa vServer оценивает объем данных, отправленных и полученных каждой сетевой картой, в килобайтах. Когда объем данных, отправленных на одну сетевую карту, превышает объем данных на другой сетевой карте, Numa vServer пытается перебалансировать трафик VIF-объектов между сетевыми адаптерами. Нагрузка одного VIF не делится между двумя сетевыми адаптерами.

Активно-активный режим агрегации сетевых адаптеров может обеспечить выравнивание нагрузки от трафика нескольких ВМ, этот режим не может предоставить одной ВМ пропускную способность двух сетевых адаптеров. Любой VIF-объект использует строго один из агрегированных интерфейсов за один раз. Поскольку Numa vServer периодически балансирует трафик, VIF-объекты не оказываются закрепленными за определенными сетевыми адаптерами агрегации постоянно.

Активно-активный режим иногда упоминается как Source Load Balancing-агрегация (SLB-агрегация), поскольку Numa vServer использует SLB для совместного использования потока пакетов через агрегированные сетевые адаптеры. SLB является ответвлением Adaptive Load Balancing (ALB) с открытым исходным кодом и использует возможность ALB динамически балансировать нагрузку на сетевые адаптеры.

При повторной балансировке количество байтов, пересланных через каждое ведомое устройство (сетевой интерфейс), отслеживается в течение установленного промежутка времени. Когда пакет, который необходимо отправить, содержит MAC-адрес нового источника, этот адрес присваивается сетевому адаптеру с самым низким уровнем загруженности. Распределение трафика производится через равномерные промежутки времени.

Каждый MAC-адрес имеет соответствующую нагрузку, и Numa vServer может перемещать нагрузку между сетевыми адаптерами в зависимости от количества данных, которые ВМ отправляет и получает. Для активно-активного режима весь трафик одной ВМ может быть перераспределён только целиком на другой адаптер.

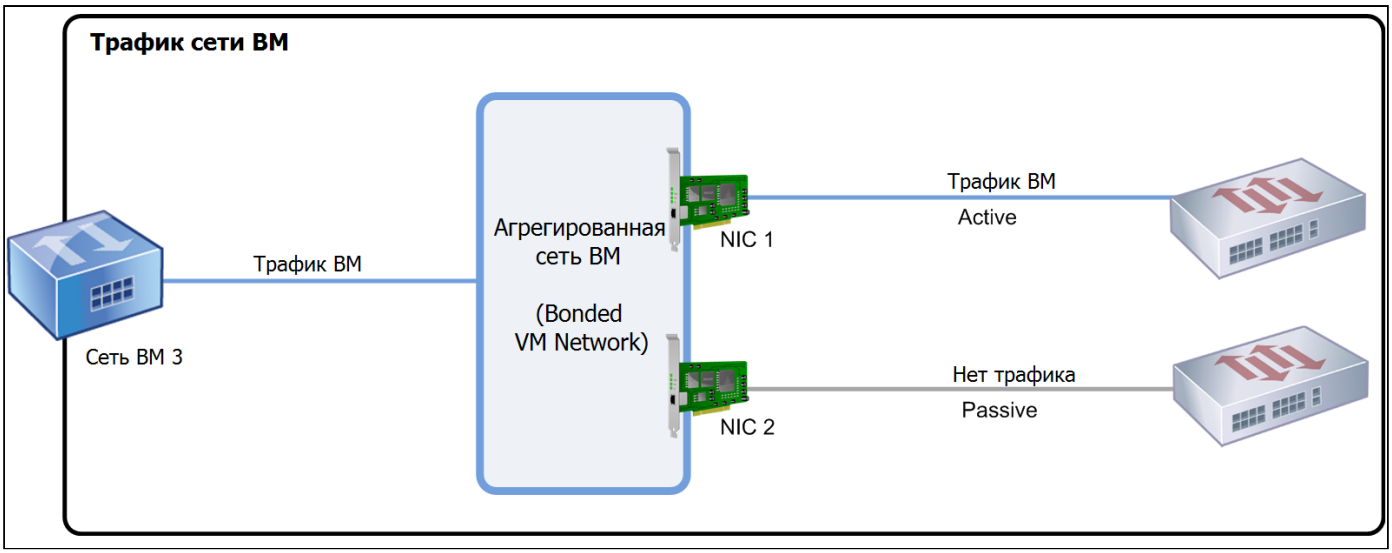
> **Примечание**
>
> Активно-активный режим агрегации не требует от коммутатора поддержки EtherChannel или 802.3ad (LACP).

3.7.5. Активно-пассивный тип агрегации (Active-Passive mode)

Активно-пассивная агрегация направляет трафик только по одному из сетевых адаптеров. Таким образом, трафик передаётся другому сетевому адаптеру в агрегации, только если происходит сбой соединения текущего активного сетевого адаптера (failover).

Активно-пассивный тип агрегации доступен при использовании сетевого стека Linux Bridge или vSwitch. При использовании Linux Bridge можно агрегировать только два сетевых адаптера, в случае vSwitch – два, три или четыре. Однако, независимо от типа трафика, когда сетевые адаптеры агрегируются в активно-пассивном режиме, только один интерфейс является активным, балансировка нагрузки отсутствует.

© 2025 Нума Технологии, ООО



Два сетевых адаптера, агрегированные в активно-пассивном режиме

Так как активно-активный тип агрегации является типом по умолчанию в среде Numa vServer, для конфигурирования агрегации в активно-пассивном режиме необходимо определять этот параметр при настройке интерфейса.

Активно-пассивный режим может быть хорошим решением для обеспечения отказоустойчивости, так как предлагает несколько преимуществ:

1. При использовании активно-пассивных агрегаций трафик передается только по одному интерфейсу, что позволяет для обеспечения избыточности использовать два коммутатора, в которых отсутствует возможность стекирования.
2. Активно-пассивный режим не требует от коммутатора поддержки EtherChannel или стандарта 802.3ad (LACP).
3. Активно-пассивный режим актуален в ситуациях, когда система не нуждается в балансировке нагрузки или когда предполагается отправка трафика через единственный сетевой адаптер.

> ⚠ Внимание!
>
> После создания VIF-объектов или создания пула администратору следует быть чрезвычайно осторожным при внесении изменений в настройки существующих агрегаций или создания новых.

3.7.6. Агрегация на основе протокола LACP (Link Aggregation Control Protocol)

Протокол управления агрегацией каналов (Link Aggregation Control Protocol, LACP) является типом агрегирования, при котором группа портов связывается вместе и обрабатывается как единый логический канал. Агрегированные каналы LACP используются как для повышения пропускной способности, так и повышения отказоустойчивости.

В отличие от других типов агрегация на основе протокола LACP требует поддержки протокола и настройки на отправителе и получателе, т.е. на сервере и коммутаторе. Для использования LACP на сервере, в качестве сетевого стека должен использоваться vSwitch.

В таблице ниже приведено сравнение активно-активного типа агрегации SLB (балансировка на основе источника) и LACP-агрегации.

Режим	Преимущества	Ограничения
Активно-активная агрегация SLB	Не требует от коммутаторов поддержки стекирования Поддерживает агрегацию до 4 сетевых адаптеров	Оптимальное выравнивание нагрузки требует наличия, по меньшей мере, одного сетевого адаптера на один VIF-объект Управляющий трафик, равно как и трафик обмена с хранилищем, не может быть распараллелен между несколькими сетевыми адаптерами

© 2025 Нума Технологии, ООО

Режим	Преимущества	Ограничения
		Выравнивание нагрузки происходит только при наличии нескольких MAC-адресов
LACP-агрегация	Все соединения могут быть активными, независимо от типа трафика	Коммутаторы должны поддерживать стандарт IEEE 802.3ad
	Балансирование трафика не подразумевает зависимости от исходных MAC-адресов – таким образом, все типы трафика могут быть сбалансированы	Требует наличие управляемого коммутатора
		Поддерживается только в сетевом стеке vSwitchv
		Требует один коммутатора или коммутаторов в стеке

3.7.6.1. Балансировка трафика в режиме агрегации LACP

Numa vServer поддерживает при использовании LACP-агрегации два типа хеширования (термин хеширование здесь относится к способу, согласно которому сетевые адаптеры и коммутатор распределяют трафик):

- балансировка нагрузки, основанная на IP-адресе и используемых портах источника и получателя;
- балансировка нагрузки, основанная на MAC-адресе источника.

В зависимости от типа хеширования и типа трафика, LACP-агрегация потенциально позволяет распределять трафик более равномерно, чем активно-активная агрегация.

> **Примечание**
>
> Необходимо задать настройки для входящего и исходящего трафика – и на сервере, и на коммутаторе: конфигурация не обязательно должна совпадать с обеих сторон.

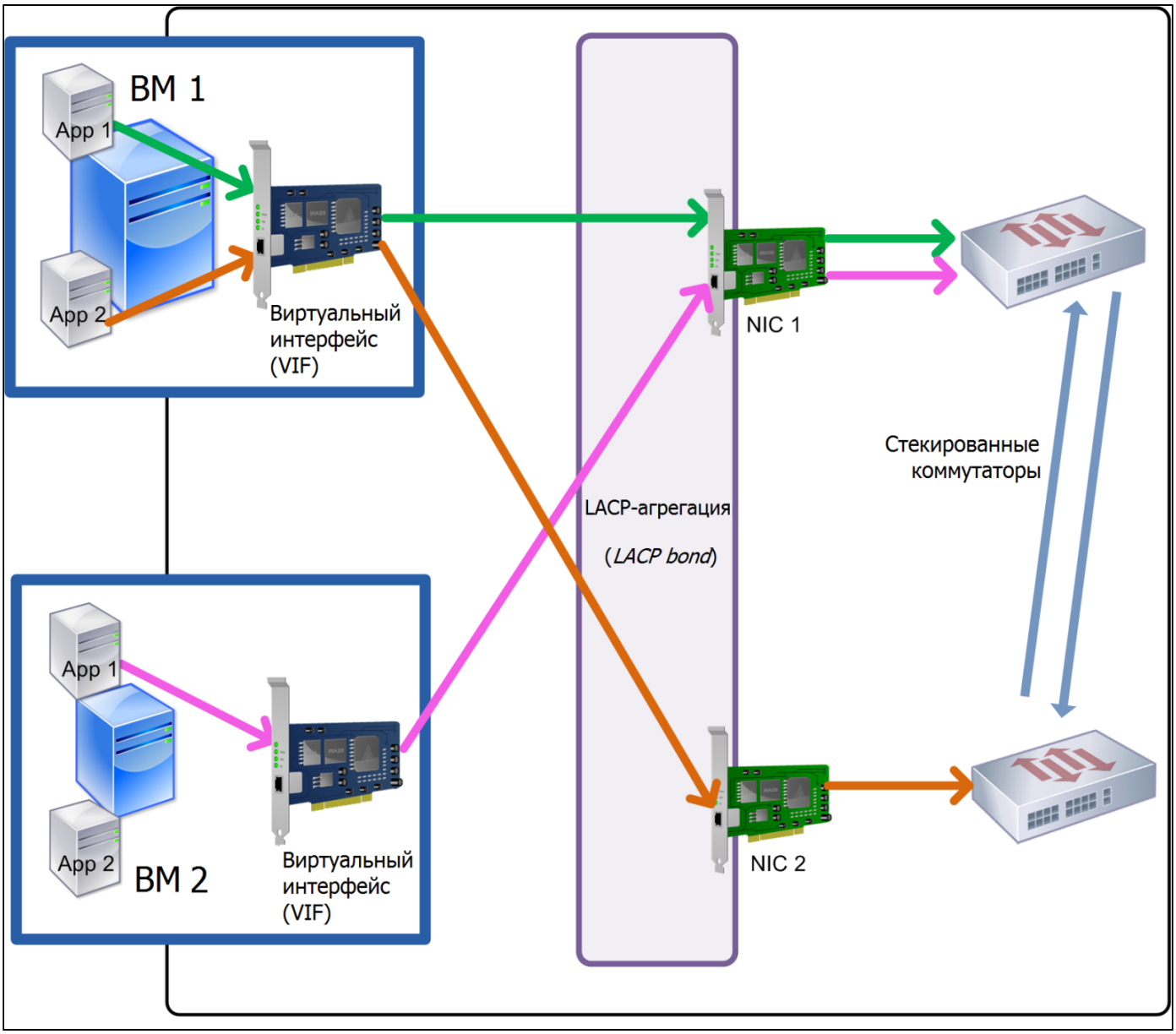
3.7.6.1.1. Балансировка нагрузки, основанная на IP-адресе и используемых портах источника и получателя

Этот тип хеширования используется по умолчанию при использовании LACP-агрегации.

Трафик, поступающий от одной виртуальной машины, может быть распределен по двум каналам при условии, что есть различия в исходном или целевом IP-адресе или номерах портов.

Если в ВМ исполняется несколько приложений, использующих различные IP-адреса или номера портов, данный тип хеширования распределяет трафик по нескольким каналам, давая гостевой системе возможность использования совокупной пропускной способности агрегированного интерфейса.

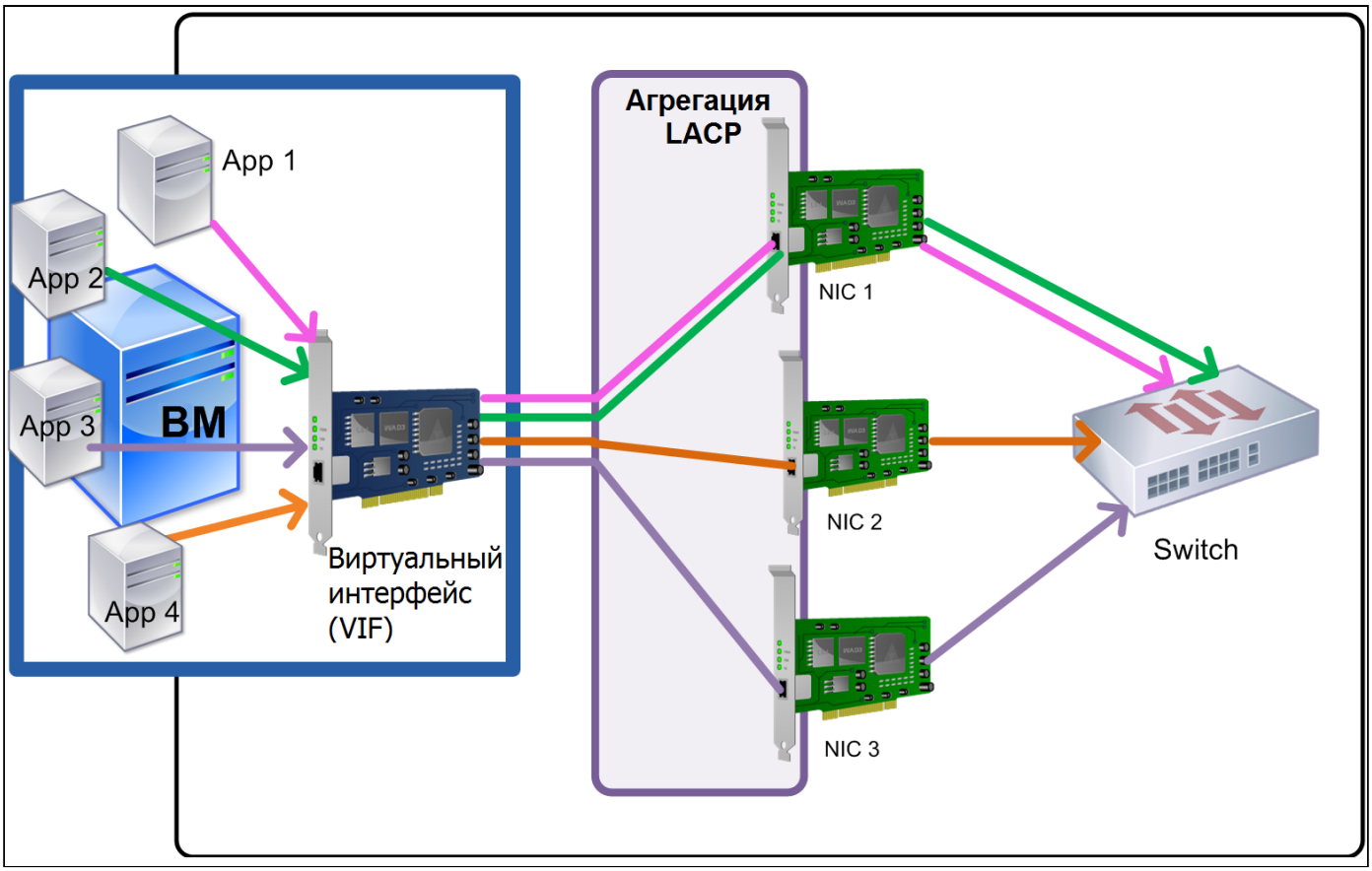
© 2025 Нума Технологии, ООО



Балансировка нагрузки, основанная на IP-адресе и используемых портах источника и получателя стек коммутаторов

Такой тип конфигурации агрегаций выгодно использовать при необходимости балансировать трафик двух различных приложений, исполняемых в одной ВМ.

© 2025 Нума Технологии, ООО



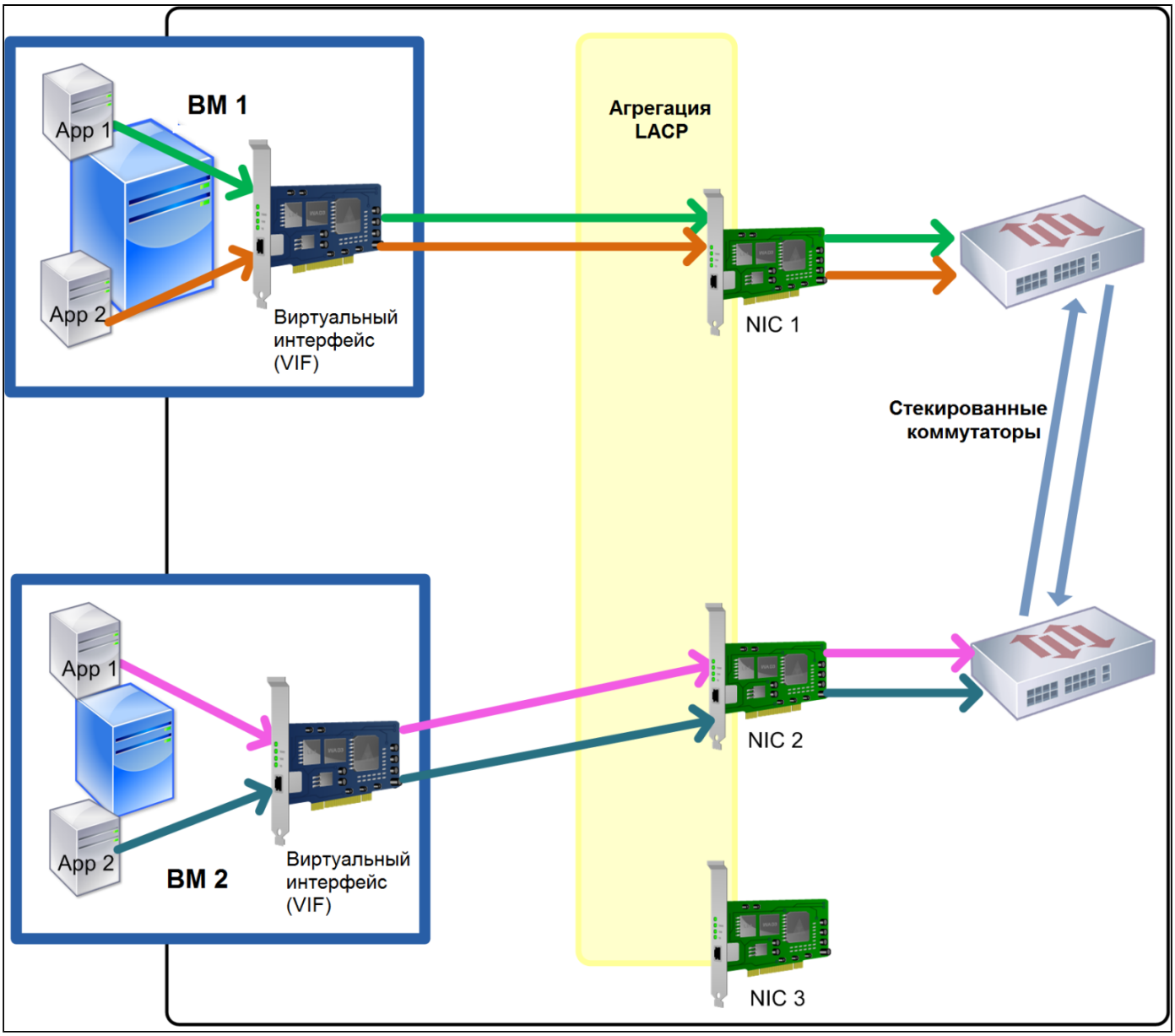
Балансировка нагрузки, основанная на IP-адресе и используемых портах источника и получателя (один коммутаторов)

Алгоритм балансировки для этого типа хеширования использует пять факторов для распределения трафика между сетевыми интерфейсами: IP-адрес источника, номер порта источника, IP-адрес назначения, номер порта назначения и MAC-адрес источника.

3.7.6.1.2. Балансировка нагрузки, основанная на MAC-адресе источника

Этот тип балансировки нагрузки работает хорошо, когда есть несколько виртуальных машин на одном сервере. Трафик балансируется на основе виртуального MAC-адреса виртуальной машины, с которой исходит трафик. Numa vServer отправляет исходящий трафик, используя тот же самый алгоритм, как в случае активно-активного агрегирования. Трафик от одной виртуальной не распределяется между несколькими сетевыми адаптерами. В результате этот тип хеширования не подходит для ситуаций, когда виртуальных интерфейсов меньше, чем физических сетевых адаптеров.

© 2025 Нума Технологии, ООО



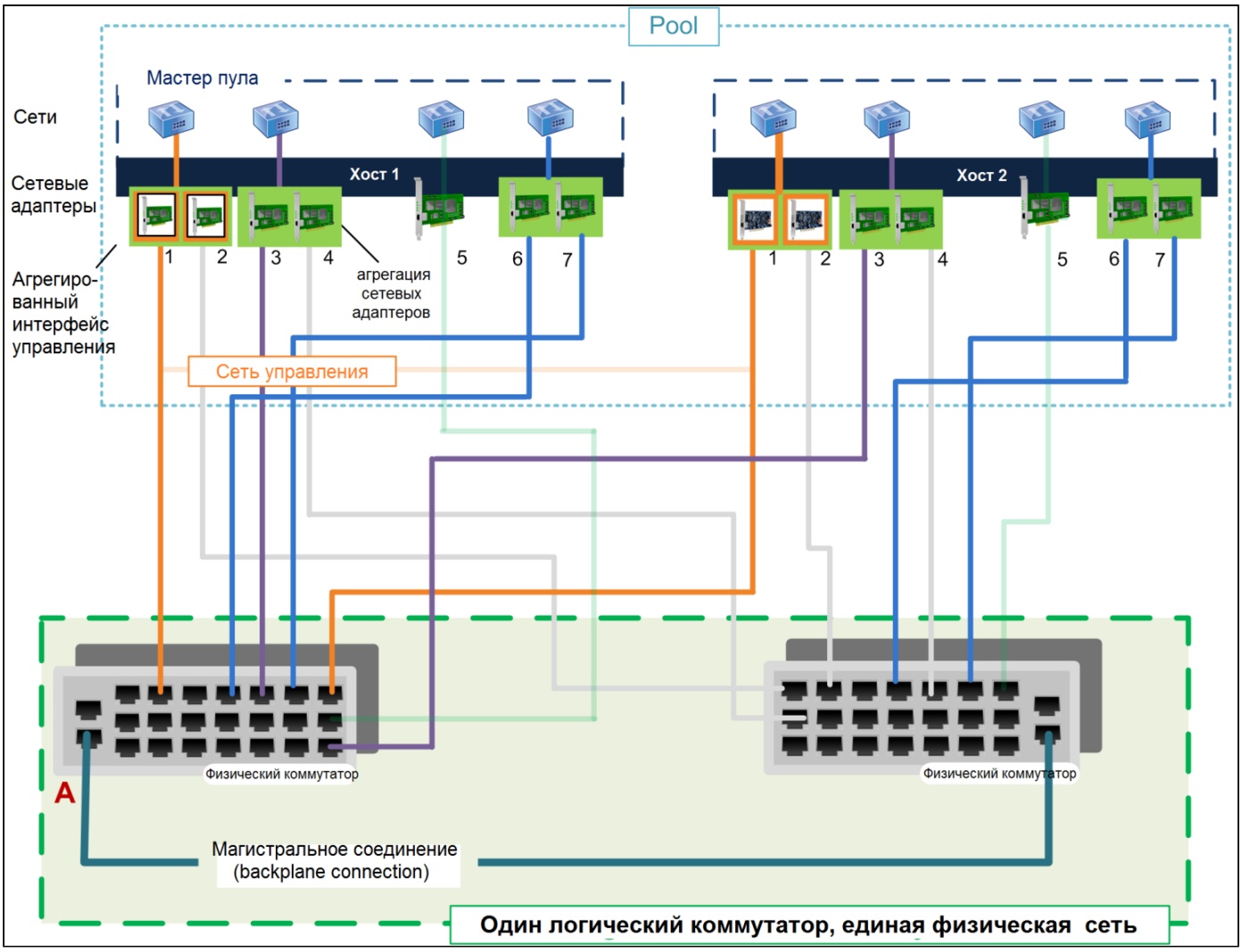
Балансировка нагрузки, основанная на MAC-адресе источника

3.7.7. Настройка коммутатора

В зависимости от требований избыточности можно подключить агрегацию сетевых адаптеров к одному или к нескольким стекированным коммутаторам. Если вы подключаете один из сетевых адаптеров ко второму резервному коммутатору, и сетевая карта или коммутатор выходит из строя, трафик переключается на другую сетевую карту. Добавление второго коммутатора предотвращает возникновение единой точки отказа в вашей конфигурации.

Используйте стековые коммутаторы, если вы хотите подключить агрегированные сетевые адаптеры к нескольким коммутаторам и настроили тип агрегации LACP. Термин «стековые коммутаторы» относится к ситуации, когда несколько физических коммутаторов сконфигурированы так, чтобы функционировать как один логический коммутатор. Коммутаторы в стеке должны быть соединены физически, и их ПО должно обеспечивать работу коммутаторов как единого логического коммутатора. Осуществляйте настройку стека в соответствии с документацией производителя оборудования.

© 2025 Нума Технологии, ООО



Вариант схемы соединения серверов и стека коммутаторов

3.7.7.1. Конфигурация коммутатора для агрегаций типа LACP

Несмотря на то, что некоторые детали конфигурации коммутаторов зависят от производителя, есть несколько ключевых пунктов, которые следует помнить, настраивая коммутаторы для использования с агрегациями типа LACP:

- сам коммутатор должен поддерживать LACP и стандарт IEEE 802.3ad;
- при создании LAG-группы на коммутаторе необходимо создать одну LAG-группу для каждой агрегации LACP на сервере;
- возможно, также следует добавить к LAG-группе идентификатор VLAN;
- каналы LACP на Numa vServer требуют, чтобы параметр режима Static Mode в LAG-группе был установлен в «Disabled» (отключено).

Как упоминалось ранее, наличие стекирования в коммутаторах является необходимым условием при подключении агрегации LACP к нескольким коммутаторам.

3.8. Первоначальная конфигурация сети после установки

Некоторые сетевые параметры сервера указываются ещё во время установки: IP-адрес (DHCP), сетевой адаптер, используемый в качестве интерфейса управления.

Если сервер содержит несколько сетевых адаптеров/интерфейсов, конфигурация сети после установки будет зависеть от того, какой из них был выбран для администрирования во время установки:

© 2025 Нума Технологии, ООО

- для каждого адаптера сервера создается отдельный ссылочный объект на физический сетевой интерфейс (PIF или PIF-объект);
- физическому сетевому интерфейсу сетевого адаптера, используемому в качестве интерфейса управления, присваиваются настройки IP-адреса, указанные во время установки;
- для каждого физического сетевого интерфейса создается сеть («Network 0», «Network 1» и т. д.);
- каждая сеть связана с одним PIF-объектом;
- настройки IP-адреса всех остальных физических интерфейсов остаются неустановленными.

В случае если сервер содержит единственный сетевой адаптер, после установки настройки будут следующими:

- будет создан один PIF-объект, соответствующий единственному сетевому адаптеру;
- PIF-объекту будут присвоены настройки IP-адресации, указанные во время установки, чтобы обеспечить возможность управления;
- физический сетевой интерфейс будет настроен в качестве интерфейса управления;
- будет создана единственная сеть «Network 0»;
- сеть «Network 0» будет подключена к PIF с целью обеспечения внешнего подключения к ВМ.

В обоих случаях полученные настройки сети обеспечат подключение xe CLI и любого иного управляющего ПО. Эта конфигурация также позволит создавать внешние сети для виртуальных машин, размещенных на сервере.

Физический сетевой интерфейс PIF, используемый для управления, является единственным физическим сетевым интерфейсом, которому присваиваются настройки IP-адреса во время установки Numa vServer. Создание внешних сетей для виртуальных машин достигается путем соединения физического сетевого интерфейса с виртуальным с помощью сетевого объекта, выполняющего роль виртуального Ethernet-коммутатора.

3.8.1. Изменение конфигурации сети

Изменить конфигурацию сети можно посредством изменения сетевого объекта. Для этого необходимо выполнить команду, затрагивающую либо сетевой объект, либо виртуальный сетевой интерфейс (VIF).

3.8.1.1. Изменение сетевого объекта

Изменять параметры сети, такие как размер фрейма (максимальный блок передачи), метка имени, описание имени и прочие значения, можно посредством команды:

```
1  xe network-param-set
```

и соответствующих параметров. Единственным обязательным параметром является `uuid`. Необязательные параметры включают в себя:

- `default_locking_mode` (см. раздел Упрощённая настройка режима блокировки виртуального сетевого интерфейса);
- `name-label` – название;
- `name-description` – описание;
- `MTU` – размер фреймов;
- `purpose` – добавление цели (см. раздел Назначение цели для сети);
- `other-config` – прочие настройки.

Если значение параметра не задано, то его значение приравнивается к нулю. Для установки пары «ключ-значение» в параметре адаптера, необходимо использовать синтаксическую конструкцию `map-param:key=value`.

3.8.2. Изменение времени задержки Up Delay трафика агрегации

Как было описано в разделе Агрегация сетевых интерфейсов, по умолчанию параметр задержки Up Delay равен 31000 мс, такое значение выбрано, чтобы избежать перебалансировки трафика в случае кратковременных отказов. Несмотря на то, что время ожидания может показаться очень большим, такая задержка необходима для всех режимов агрегации, а не только для активно-активного.

© 2025 Нума Технологии, ООО

Администратор может изменить время ожидания перед группировкой с помощью выполнения следующих команд:

- установка времени ожидания в миллисекундах:

```
xe pif-param-set uuid=<uuid главного интерфейса агрегации (PIF)> other-config:bond-updelay=<Время задержки в мс>
```

- чтобы изменения вступили в силу, необходимо отключить, а затем снова включить физический сетевой интерфейс:

```
xe pif-unplug uuid=<uuid главного интерфейса агрегации (PIF)>
```

```
xe pif-plug uuid=<uuid главного интерфейса агрегации (PIF)
```

3.9. Управление конфигурацией сети

Процедуры настройки сети в этом разделе различаются в зависимости от того, настраивается сеть на отдельном сервере или на сервере, который является частью пула ресурсов.

3.9.1. Создание сетей на автономном сервере

Так как внешние сети создаются для каждого физического сетевого интерфейса во время установки, создание дополнительной сети обычно может потребоваться только в случае:

- создания частной сети;
- поддержки дополнительных операций, таких как VLAN и объединение сетевых адаптеров.

Добавление новой сети с помощью командной строки:

1. Откройте консоль управления сервера.
2. Выполните команду для создания сети:

```
xe network-create name-label=<mynetwork>
```

После ввода команды на экране будет отображён UUID новой сети.

На данном этапе сеть не подключена к физическому интерфейсу, т.е. является внутренней.

3.9.2. Создание сетей в пуле ресурсов

Все серверы в рамках одного пула должны иметь одинаковое количество сетевых адаптеров (NIC), хотя это требование не является строгим.

Идентичность физической конфигурации сервера в рамках одного пула важна, потому что все серверы одного пула имеют общий набор сетей. Физические сетевые интерфейсы отдельных серверов подключаются к общим сетям пула по имени устройства. Например, все серверы в рамках пула с сетевым интерфейсом eth0 будут иметь соответствующий физический сетевой интерфейс, подключенный к общей сети пула Network 0. То же самое будет справедливо для серверов с интерфейсами eth1 и Network 1, так же, как и для иных адаптеров, присутствующих как минимум на одном сервере в пуле.

Если у одного из серверов количество сетевых адаптеров отличается от всех остальных в пуле, могут возникнуть сложности, так как не все сети пула будут действительны для всех его участников. Например, если серверы host1 и host2 находятся в одном пуле, и при этом у host1 четыре сетевых адаптера, а у host2 всего два, то для host2 будут действительны только сети, подключенные к физическим интерфейсам, соответствующим eth0 и eth1. Виртуальные машины на host1 с виртуальными сетевыми интерфейсами, подключенными к сетям, соответствующим eth0 и eth1 не смогут мигрировать на сервер host2.

© 2025 Нума Технологии, ООО

3.9.3. Создание виртуальных локальных сетей (VLAN)

Для серверов в рамках пула ресурсов можно воспользоваться командой `xe pool-vlan-create`. Эта команда создает VLAN и автоматически создает и подключает необходимые физические интерфейсы.

Для создания сети для использования с VLAN выполните следующие действия:

1. Откройте консоль управления сервера.
2. Выполните команду для создания сеть для использования с VLAN:

```
xe network-create name-label=network5
```

   На экране будет отображен UUID новой сети.
3. Для поиска UUID физического сетевого интерфейса, соответствующего физическому сетевому адаптеру, поддерживающему желаемый VLAN-тег используйте команду:

```
xe pif-list
```

   Будут показаны UUID и имена устройств всех физических интерфейсов, включая все существующие VLAN.
4. Создайте объект VLAN и укажите желаемый физический сетевой интерфейс и VLAN-тег:

```
xe vlan-create network-uuid=<network-uuid> pif-uuid=<pif-uuid> vlan=5
```

   На экране будет отображен UUID новой сети VLAN.
5. После создания новой сети можно подключить виртуальные сетевые интерфейсы ВМ к этой сети.

3.9.4. Агрегирование сетевых адаптеров автономного сервера

В данном разделе описывается порядок объединения интерфейсов сетевых адаптеров на сервере Numa vServer, не объединённых в пул с другими серверами, при помощи командной строки.

3.9.4.1. Агрегирование сетевых адаптеров

Для агрегации двух или четырёх сетевых адаптеров:

1. Создайте новую сеть для использования с объединенным сетевым адаптером:

```
xe network-create name-label=<bond0>
```

   На экране будет отображен UUID новой сети.
2. Узнайте идентификаторы UUID физических интерфейсов, которые предполагается агрегировать:

```
xe pif-list
```

3. Настройте активно-активный тип агрегации (это тип по умолчанию). Отделите параметры запятыми, укажите UUID только что созданной сети и UUID физических интерфейсов, которые необходимо объединить:

```
xe bond-create network-uuid=<network-uuid> pif-uuids=<pif-uuid-1>,<pif-uuid-2>,<pif-uuid-3>
```

© 2025 Нума Технологии, ООО

Введите два UUID, если вы объединяете два сетевых адаптера, и четыре UUID – если четыре. После выполнения команды будет выведен UUID агрегации.

4. Или настройте агрегацию типа «активно-пассивная» или типа LACP с использованием того же синтаксиса, указав необязательный параметр `mode` и задав для него значение `lacp` или `active-backup`:

```
xe bond-create network-uuid=<network-uuid> pif-uuids=<pif-uuid-1>,<pif-uuid-2>,<pif-uuid-3>
mode=<balance-slb | active-backup | lacp>
```

3.9.4.2. Управление MAC-адресом агрегации

При агрегировании физического сетевого интерфейса, используемого в данный момент в качестве интерфейса управления, роль интерфейса управления переносится на всю агрегацию. Если на сервере используется DHCP, то в большинстве случаев MAC-адрес агрегации будет совпадать с таковым у физического сетевого интерфейса, используемого в настоящий момент, а IP-адрес интерфейса управления останется неизменным.

MAC-адрес агрегации можно изменить, чтобы он отличался от MAC-адреса (текущего) адаптера интерфейса управления. Однако после объединения и изменения MAC/IP-адреса текущие сессии сети на сервере будут сброшены.

Управлять MAC-адресом агрегации можно двумя способами:

- в команде `xe bond-create` можно указать необязательный параметр `mac`. Этот параметр можно использовать, чтобы сделать MAC-адрес произвольным;
- если параметр `mac` не указан, будет использован MAC-адрес управляющего интерфейса, если он является одним из интерфейсов агрегации. Если в агрегацию входит не управляющий интерфейс, а другой, то агрегация использует MAC-адрес (а также IP-адрес) интерфейса управления. Если ни один из сетевых интерфейсов агрегации не является интерфейсом управления, агрегация использует MAC-адрес первого из указанных сетевых адаптеров.

3.9.4.3. Отключение агрегации сетевых адаптеров

При возврате сервера к неагрегированной конфигурации следует обратить внимание, что команда `xe bond-destroy` автоматически настроит интерфейс, указанный в параметре `primary-slave`, в качестве интерфейса управления. Впоследствии все виртуальные интерфейсы будут перемещены на него.

Термин primary-slave здесь соответствует физическому сетевому интерфейсу, настройки MAC- и IP-адресов которого были использованы при создании агрегации. При объединении двух сетевых адаптеров интерфейсом `primary-slave` будет являться:

- интерфейс управления (если он является одним из агрегируемых);
- любой другой сетевой адаптер с IP-адресом (если интерфейс управления не является одним из агрегируемых);
- первый указанный сетевой адаптер. Узнать какой это интерфейс можно, выполнив команду:

```
xe bond-list params=all
```

3.9.5. Агрегирование сетевых адаптеров в пуле

Данный раздел описывает процесс создания агрегаций сетевых адаптеров на серверах Numa vServer входящих в пул с помощью командной строки.

При возможности рекомендуется создавать агрегации сетевых адаптеров в процессе создания пула ресурсов, до добавления к пулу дополнительных серверов к пулу и создания ВМ. Это позволит автоматически дублировать настройки агрегации на серверы по мере их подключения к пулу и уменьшит объёмы работы.

Для добавления агрегации сетевых адаптеров к существующему пулу можно выбрать один из двух путей:

- с помощью CLI настроить агрегации на мастере пула, а затем на каждом рядовом члене пула;
- с помощью CLI настроить группы на мастере пула, чтобы он получил настройки от мастера.

© 2025 Нума Технологии, ООО

> **Предупреждение**
>
> Не пытайтесь агрегировать сети при включенной функции высокой доступности HA (High Availability). Процесс агрегирования нарушит текущие процессы функции HA и вызовет отключение серверов. После этого, скорее всего, не удастся выполнить их перезагрузку правильно, а для восстановления потребуется выполнить команду
>
> ```
> xe host-emergency-ha-disable
> ```

3.9.5.1. Добавление агрегаций сетевых адаптеров к новому пулу ресурсов

Для агрегации двух или четырёх сетевых адаптеров:

1. Выберите сервер, который должен стать мастером пула. По умолчанию любой сервер является мастером собственного безымянного пула. Для создания пула ресурсов с помощью командной строки, необходимо переименовать существующий безымянный пул:

```
xe pool-param-set name-label=<new-pool-name> uuid=<pool-uuid>
```

2. Процесс агрегирования сетевых адаптеров описан в разделе Агрегирование сетевых адаптеров автономного сервера;
3. Откройте консоль сервера, который необходимо добавить к пулу, и выполните команду:

```
xe pool-join master-address=<host1> master-username=root master-password=<password>
```

Данные сети и агрегации будут автоматически перенесены на новый сервер. Интерфейс управления автоматически переносится с сетевого адаптера сервера, где он был изначально настроен, на физический сетевой интерфейс, включенный в агрегацию (то есть интерфейс управления теперь поглощён агрегацией, вся она выполняет роль интерфейса управления).

Для поиска UUID настраиваемого сервера выполните следующую команду:

```
xe host-list
```

3.9.5.2. Добавление агрегаций сетевых адаптеров к существующему пулу ресурсов

> **Предупреждение**
>
> Не пытайтесь агрегировать сети при включенном HA. Процесс создания агрегации нарушит текущие процесс агента сервера и вызовет отключение сервера; после этого, скорее всего, не удастся выполнить их перезагрузку правильно, а для восстановления потребуется выполнить команду `xe host-emergency-ha-disable`.

В отсутствии графического интерфейса для объединения сетевых адаптеров самым быстрым способом создать агрегацию адаптеров, общую для всего пула, будет следующий: нужно создать эту агрегацию на сервере, являющемся мастером пула, а затем перезапустить прочие серверы пула.

В качестве альтернативы перезагрузки сервера можно использовать команду `systemctl restart xapi`.

В результате настройки агрегации и настройки VLAN на мастере пула будут переданы каждому серверу. Интерфейс управления каждого сервера придётся перенастраивать вручную.

Процесс агрегирования сетевых адаптеров описан в в разделе Агрегирование сетевых адаптеров автономного сервера.

© 2025 Нума Технологии, ООО

3.10. Настройка сетевого интерфейса, выделенного для соединения с хранилищем

С помощью интерфейса CLI можно присвоить сетевому интерфейсу IP-адрес и выделить его под определенные функции, например, под трафик сети хранения данных. Чтобы присвоить сетевому интерфейсу IP-адрес необходимо создать вторичный интерфейс (основной интерфейс с доступным IP-адресом, используемый Numa vServer для управляющего трафика, называется интерфейсом управления).

При необходимости выделить вторичный интерфейс под определенные функции, необходимо проверить конфигурацию сети и убедиться, что сетевой адаптер используется исключительно для необходимого трафика. Например, чтобы выделить сетевой интерфейс под трафик системы хранения, то сетевой интерфейс, запоминающее устройство, коммутатор и/или VLAN должны иметь такую конфигурацию, чтобы к запоминающему устройству, получающему трафик, доступ можно было получить только через выделенный сетевой интерфейс. Если физическая или IP-конфигурация не ограничивают трафик, который может быть пропущен через сетевой интерфейс системы хранения, то прочий трафик, как например управляющий трафик, можно пропустить через вторичный интерфейс.

При создании нового интерфейса для трафика системы хранения данных, необходимо присвоить ему IP-адрес, который будет расположен:

- в той же подсети, что и интерфейс системы хранения, если этот применимо;
- будет расположен в отдельной подсети от прочих вторичных интерфейсов или интерфейса управления.

При конфигурации вторичных интерфейсов следует обратить внимание, что каждый интерфейс должен быть расположен в отдельной подсети. Например, при необходимости выделить два дополнительных вторичных интерфейса под хранение, понадобятся IP-адреса в трёх разных подсетях: одна подсеть для интерфейса управления, вторая – для вторичного интерфейса №1 и третья – для вторичного интерфейса №2.

При использовании агрегирования интерфейсов с целью повысить отказоустойчивость передачи трафика системы хранения, рекомендуется рассмотреть вариант использования LACP на основе vSwitch.

> **Примечание**
>
> При выборе сетевого адаптера для использования с хранилищами на основе iSCSI или NFS, необходимо убедиться, что выделенный адаптер использует отдельную IP-подсеть, которая не маршрутизируется с интерфейса управления. Если это не обеспечено, то трафик системы хранения может быть направлен через интерфейс управления после перезапуска сервера, согласно порядку инициализации сетевых интерфейсов.

Чтобы присвоить функции сетевому адаптеру необходимо:

- убедиться, что физический сетевой интерфейс находится в отдельной подсети или что маршрутизация настроена согласно топологии имеющейся сети, чтобы обеспечить передачу необходимого трафика через выбранный физический сетевой интерфейс;
- установить IP-конфигурацию для физического сетевого интерфейса, внеся соответствующие величины в параметры режима, а при использовании статического IP-адреса – такие параметры как IP, маску сети, шлюз и DNS:

```
xe pif-reconfigure-ip mode=<DHCP | Static> uuid=<pif-uuid>
```

- присвоить значение `true` параметру `disallow-unplug`:

```
xe pif-param-set disallow-unplug=true uuid=<pif-uuid>
```

```
xe pif-param-set other-config:management_purpose="Storage" uuid=<pif-uuid>
```

При необходимости использования вторичного интерфейса для трафика системы хранения, который также может быть маршрутизирован с интерфейса управления (принимая во внимание, что такая конфигурация не является наилучшим решением), можно воспользоваться двумя способами:

© 2025 Нума Технологии, ООО

- после перезапуска хоста убедиться в правильности конфигурации вторичного интерфейса, а затем с помощью команд `xe pbd-unplug` и `xe pbd-plug` повторно инициализировать подключение системы хранения к хосту. В результате будет переустановлено соединение с системой хранения, а трафик будет направлен через нужный интерфейс;
- в качестве альтернативы можно использовать команду `xe pif-forget`, чтобы удалить интерфейс из базы данных и вручную настроить его в управляющем домене. Эта рекомендация является дополнительной и потребует навыка ручной конфигурации сетей Linux.

3.11. Использование сетевых адаптеров с поддержкой SR-IOV

Технология Single Root I/O Virtualization (SR-IOV) является технологией виртуализации PCI-устройств, которая позволяет одному PCI-устройству выполнять функцию нескольких аналогичных устройств на шине PCI. Само по себе физическое устройство называется физической функцией (Physical Function, PF), в то время как все остальные называются виртуальными функциями (Virtual Functions, VF). Целью является предоставление гипервизору возможности напрямую присваивать один или несколько виртуальных сетевых адаптеров виртуальной машине с помощью технологии SR-IOV: пользователь может использовать виртуальные адаптеры наравне со всеми прочими напрямую подключенными PCI-устройствами.

Присваивание одного или нескольких виртуальных адаптеров виртуальной машине позволяет ей напрямую использовать аппаратное обеспечение. После конфигурации, каждая ВМ ведет себя так, как если бы она напрямую использовала сетевой адаптер, что сокращает издержки на обработку и увеличивает производительность.

> **Предупреждение**
>
> Если виртуальной машине требуется мобильность, и она имеет присвоенные виртуальные адаптеры SR-IOV, то выполнение таких функций, как Live Migration, High Availability и Disaster Recovery невозможно. Это происходит из-за того, что ВМ напрямую связана с виртуальной функцией физического сетевого адаптера с поддержкой SR-IOV. Кроме того, сетевой трафик ВМ, направляемый через виртуальные сетевые адаптеры функции SR-IOV, минует vSwitch, что делает невозможным создание ACL или просмотр QoS.

SR-IOV имеет лучшую производительность, чем VIF. Он может обеспечить аппаратное разделение трафика между разными виртуальными машинами через один и тот же сетевой адаптер в обход сетевого стека Numa vServer.

3.11.1. Преимущества SR-IOV

Используя эту функцию, можно:

- включить SR-IOV на сетевых картах, которые поддерживают SR-IOV;
- отключить SR-IOV на сетевых картах, поддерживающих SR-IOV;
- управлять SR-IOV VFs как пулом ресурсов VF;
- назначить VF SR-IOV виртуальной машине;
- настроить VFs SR-IOV (например, MAC-адрес, VLAN, скорость);
- запустить тест для проверки поддержки SR-IOV.

3.11.2. Конфигурация системы для работы с SR-IOV

Для корректной работы SR-IOV необходима поддержка оборудованием следующих технологии:

- виртуализация ввода-вывода MMU (AMD-Vi и Intel VT-d);
- альтернативная интерпретация идентификатора маршрутизации (ARI);
- услуги по переводу адресов (ATS);
- службы контроля доступа (ACS).

© 2025 Нума Технологии, ООО

3.11.2.1. Ограничения при работе с SR-IOV

Технология SR-IOV следующие ограничения:

- для некоторых сетевых адаптеров, использующих устаревшие драйверы (например, семейство Intel I350), необходимо перезагрузить сервер, чтобы включить или отключить SR-IOV на этих устройствах;
- только гостевые ВМ с поддержкой аппаратной виртуализации (HVM) поддерживают работу с технологией SR-IOV;
- сеть уровня пула, имеющая разные типы сетевых карт, не поддерживается;
- VF SR-IOV и обычный VIF одного и того же сетевого адаптера могут не иметь возможности связываться друг с другом из-за аппаратных ограничений сетевого адаптера. Чтобы эти хосты могли обмениваться данными, убедитесь, что для связи используется шаблон VF для VF или VIF для VIF, а не VF для VIF;
- настройки качества обслуживания для некоторых VF SR-IOV не вступают в силу, поскольку они не поддерживают ограничение скорости сети;
- выполнение динамической миграции, приостановки и создание снимка состояния не поддерживается на виртуальных машинах, использующих SR-IOV VF;
- VF SR-IOV не поддерживают горячее подключение;
- для некоторых сетевых карт с устаревшими драйверами может потребоваться перезагрузка даже после перезапуска хоста, это указывает на то, что сетевая карта не может включить SR-IOV;
- аппаратное ограничение: функция SR-IOV полагается на контроллер для сброса функций устройства в исходное состояние в течение 100 мс по запросу гипервизора с использованием сброса функционального уровня (FLR);
- SR-IOV может использоваться в пуле, который использует механизм HA (высокая доступность). Виртуальные машины, которым назначены SR-IOV VF, перезапускаются, когда в пуле есть сервер, имеющий соответствующие ресурсы.

3.11.2.2. Настройка SR-IOV для устаревших драйверов

Обычно максимальное количество VF, которые может поддерживать сетевая карта, может быть определено автоматически. Для сетевых карт, использующих устаревшие драйверы (например, семейство Intel I350), ограничение определяется в файле конфигурации модуля драйвера. Может потребоваться корректировка лимита вручную. Чтобы установить его на максимум, необходимо:

- открыть файл редактором:

```
/etc/modprobe.d/igb.conf
```

- установить максимальное количество VF на 7 в поле `VFs-maxvfs-by-user`:

```
## VFs-param: max_vfs
## VFs-maxvfs-by-default: 7
## VFs-maxvfs-by-user: 7
options igb max_vfs=0
```

- сохранить изменения;
- выгрузить и загрузить драйвер для применения конфигурации:

```
rmmod igb && modprobe igb
```

> **Внимание!**
>
> Вносимое в файл конфигурации драйвера значение должно быть меньше или равно значению `VFs-maxvfs-by-default`.

Не рекомендуется изменять никакие другие строки в этом файле.

© 2025 Нума Технологии, ООО

3.11.2.3. Присвоение ВМ виртуального адаптера SR-IOV

- открыть CLI севера;
- выполнить команду `lspci`, чтобы отобразить список виртуальных функций (VF). Например:

```
07:10.0 Ethernet controller: Intel Corporation 82559 Ethernet Controller Virtual Function (rev 01)
```

В примере выше 07:10.0 является (bus:device.function) - адресом виртуального адаптера.

- виртуальный адаптер присваивается ВМ с помощью следующей команды:

```
xe vm-param-set other-config:pci=0/0000:<bus:device.function> uuid=<vm-uuid>
```

- запустить ВМ и установить в ОС драйвер соответствующей виртуальному адаптеру для конкретного устройства.

> **Примечание**
>
> Одной ВМ может быть присвоено несколько виртуальных адаптеров, однако один виртуальный адаптер не может использоваться несколькими ВМ.

3.12. Ограничение базовой скорости передачи данных (QoS limit)

Чтобы ограничить объём трафика, который ВМ может отправлять за секунду времени, можно присвоить значение базовой скорости передачи данных (Quality of Service limit) для виртуального сетевого интерфейса. Это позволяет установить максимальный уровень передачи исходящих пакетов данных в Кбайт/сек.

Значение QoS ограничивает уровень исходящих данных из виртуальной машины, и не ограничивает объём входящих данных. В зависимости от сетевого стека, настроенного для пула, можно установить значение параметра QoS для виртуального сетевого интерфейса виртуальной машины в одном из двух мест: либо на внешнем контроллере, совместимым с vSwitch, либо на сервер.

Таблица - Настройка QoS в зависимости от используемого сетевого стека

Сетевой стек	Доступные методы конфигурации
vSwitch	Внешний контроллер. Этот метод является предпочтительным методом настройки QoS на виртуальном интерфейсе, когда vSwitch выполняет роль сетевого стека; Командная строка. Возможно установить уровень передачи QoS с помощью команд, как показано в примере ниже.
Linux bridge	Командная строка. Установить уровень передачи QoS также можно с помощью командной строки, выполнив команды, описанные ниже.

> **Предупреждение**
>
> Когда vSwitch используется в качестве сетевого стека, можно непреднамеренно установить значение QoS как на внешнем контроллере, так и внутри сервера Numa vServer. В таком случае, Numa vServer ограничит исходящий трафик согласно более низкому из установленных значений.

Пример команд интерфейса командной строки для установки QoS. Чтобы ограничить виртуальный сетевой интерфейс до максимального уровня передачи в 100 Кбайт/с с помощью командной строки, необходимо воспользоваться следующей командой:

© 2025 Нума Технологии, ООО

```
xe vif-param-set uuid=<vif_uuid> qos_algorithm_type=ratelimit
```

```
xe vif-param-set uuid=<vif_uuid> qos_algorithm_params:kbps=100
```

Если используется внешний контроллер, рекомендуется установить ограничение скорости передачи в контроллере вместо выполнения этой команды CLI.

3.13. Изменение параметров конфигурации сети

В данном разделе рассматриваются возможности изменения сетевой конфигурации сервера Numa vServer. Это включает в себя:

- изменение имени хоста (hostname);
- добавление или удаление DNS-серверов;
- изменение IP-адреса;
- изменение сетевого адаптера, используемого в качестве интерфейса управления;
- добавление нового физического сетевого адаптера к серверу;
- включение ARP-фильтрации (блокировка порта коммутатора).

3.13.1. Изменение имени хоста

Системное имя хоста, также известное как DNS-имя, определяется в рамках общей базы данных пула и управляется с помощью следующей команды:

```
xe host-set-hostname-live host-uuid=<host_uuid> host-name=<host-name>
```

Базовое имя хоста управляющего домена изменяет в динамическом режиме и отображает действующее имя хоста.

3.13.2. DNS-серверы

Чтобы добавить или удалить DNS-сервер в конфигурации IP-адресации хоста Numa vServer, следует пользоваться командой `xe pif-reconfigure-ip`. Например, для физического сетевого интерфейса со статическим IP-адресом:

- настройте порядок поиска суффиксов DNS вашего домена для разрешения неполных доменных имен:

```
xe pif-param-set uuid=<pif-uuid_in_the_dns_subnetwork> other-config:domain=suffix.com
```

- настройте DNS-сервер для использования на хостах vServer:

```
xe pif-reconfigure-ip mode=static dns=<dnshost> ip=<ip> gateway=<gateway> netmask=<netmask>
uuid=<uuid>
```

- вручную настройте интерфейс управления на использование PIF, который находится в той же сети, что и ваш DNS-сервер:

```
xe host-management-reconfigure pif-uuid=<pif_in_the_dns_subnetwork>
```

© 2025 Нума Технологии, ООО

> **Примечание**
>
> Альтернативный способ добавления DNS-сервера:
>
> - `xe pif-reconfigure-ip mode=static dns=<dnshost> ip=<ip> gateway=<gateway> netmask=<netmask> uuid=<uuid>`
> - `resolvectl domain xenbr0 suffix.com`

3.13.3. Изменение конфигурации IP-адреса сервера

Конфигурацию сетевого интерфейса можно изменить с помощью командной строки. Чтобы изменить конфигурацию IP-адреса физического сетевого интерфейса следует воспользоваться командой `xe pif-reconfigure-ip`.

3.13.4. Изменение конфигурации IP-адреса в пуле ресурсов

Серверы Numa vServer в пуле ресурсов имеют один административный IP-адрес, используемый для управления, связи и взаимодействия с другими серверами в пуле. Процедура изменения IP-адреса интерфейса управления для мастера пула отличается от аналогичной процедуры для остальных хостов.

> **Предупреждение**
>
> Изменять IP-адрес и прочие параметры сервера необходимо с осторожностью. В зависимости от топологии сети и вносимых изменений, соединение с сетевой системой хранения данных может быть потеряно. Если это произойдет, систему хранения необходимо подключить заново с помощью команды `xe pbd-plug` командной строки. Рекомендуется мигрировать ВМ с сервера до внесения изменений в IP-конфигурацию.

Для изменения IP-адреса рядового участника пула следует:

- установить желаемый IP-адрес посредством интерфейса командной строки выполнив команду `xe pif-reconfigure-ip`. Например, для получения IP-адреса по DHCP:

```
1  xe pif-reconfigure-ip uuid=<pif_uuid> mode=DHCP
```

- выполнить команду `xe host-list`, чтобы убедиться, что участник пула был успешно подключен к мастеру, проверив, что все остальные серверы пула отображаются корректно.

```
1  xe host-list
```

Изменение IP-адреса мастера пула потребует дополнительных действий, поскольку каждый рядовой участник пула использует IP-адрес мастера для связи и взаимодействия с ним, и не будет знать, как связаться с мастером после изменения этого адреса.

По возможности для мастера пула необходимо использовать выделенный IP-адрес, который с малой вероятностью будет подвержен изменениям на протяжении всего срока службы пула.

Для изменения IP-адреса мастера пула следует выполнить следующую последовательность действий:

- установить желаемый IP-адрес посредством интерфейса командной строки выполнив команду `xe pif-reconfigure-ip`. Например, для получения IP-адреса по DHCP:

© 2025 Нума Технологии, ООО

```
xe pif-reconfigure-ip uuid=<pif_uuid> mode=DHCP
```

- после изменения IP-адреса мастера пула, все серверы рядовых участников перейдут в аварийный режим, по причине невозможности установить с ним связь. Чтобы принудительно подключить мастер к остальным членам пула и сообщить им его новый IP-адрес, необходимо с сервера-мастера выполнить следующую команду:

```
xe pool-recover-slaves
```

3.13.5. Смена интерфейса управления

В случае если Numa vServer установлен на сервере с несколькими сетевыми адаптерами, то один из сетевых интерфейсов адаптеров должен быть выбран в качестве интерфейса управления. Интерфейс управления используется для подключения к серверу клиента управления и для межсерверного взаимодействия.

Изменение сетевого адаптера, используемого в качестве интерфейса управления:

- чтобы определить, какой физический сетевой интерфейс соотнесен с сетевым адаптером, и должен использоваться в качестве интерфейса управления, выполнить следующую команду:

```
xe pif-list
```

Будет показан UUID каждого физического сетевого интерфейса.

- чтобы просмотреть IP-адрес для физического сетевого интерфейса, который будет использоваться в качестве интерфейса управления, выполнить команду `xe pif-param-list`. При необходимости изменить IP-адрес, выполнив команду `xe pif-reconfigure-ip`:

```
xe pif-param-list uuid=<pif_uuid>
```

- выполнить команду `xe host-management-reconfigure` для изменения сетевого интерфейса используемого в качестве интерфейса управления. Если этот сервер входит в состав пула, эту команду необходимо выполнить рядового участника пула:

```
xe host-management-reconfigure pif-uuid=<pif_uuid>
```

- для изменения интерфейса управления в пуле необходимо выполнить команду:

```
xe pool-management-reconfigure network-uuid=<network_uuid>
```

3.13.5.1. Отключение интерфейса управления

Чтобы полностью отключить удаленный доступ к административной консоли, необходимо выполнить команду:

```
xe host-management-disable
```

> **Предупреждение**
>
> После того как интерфейс управления был отключен, для выполнения административных задач, необходимо будет войти в физическую консоль управления на сервере.

© 2025 Нума Технологии, ООО

3.13.6. Добавление нового сетевого адаптера

После установки нового физического сетевого адаптера в сервер он не будет автоматически определён в системе. Для того что бы новый сетевой адаптер определился в системе необходимо выполнить команду `xe pif-scan`.

3.14. Использование блокировки порта коммутатора

Функция блокировки порта коммутатора Numa vServer позволяет контролировать трафик, отправляемый неизвестными, ненадежным или потенциально опасными ВМ посредством ограничения их способности имитировать наличие MAC-адресов и IP-адресов, которые не были им присвоены. Функции позволяет воспользоваться командами блокировки порта, чтобы заблокировать весь трафик в сети по умолчанию или определить конкретные IP-адреса, с которых отдельным ВМ будет разрешено отправлять трафик.

Блокировка порта коммутатора является функцией, разработанной для провайдеров общедоступных облачных услуг в средах подверженным внутренним угрозам. Эта функция может помочь провайдерам общедоступных облачных услуг, обладающих сетевой архитектурой, где каждая ВМ имеет открытый и связанный с Internet IP-адрес. Поскольку арендаторы облака всегда считаются ненадежными, применение таких мер безопасности, как защита от несанкционированного получения доступа к ресурсам сети за счёт использования чужого IP-адреса, может быть необходимым для защиты виртуальных машин от атак других арендаторов облака.

Использование блокировки порта коммутатора позволяет упростить конфигурацию сети, ограничив действия всех арендаторов и незарегистрированных пользователей одним уровнем сети (L2).

Одной из наиболее важных функций команд блокировки порта коммутатора является ограничение трафика, который может быть получен от ненадежного незарегистрированного пользователя, что, в свою очередь, ограничивает способность такого пользователя имитировать наличие MAC и IP-адреса, которым он на самом деле не обладает. В частности, можно использовать эти команды, чтобы предотвратить такие действия незарегистрированного пользователя, как:

- сообщение IP-адреса или MAC-адреса, который не входит в список разрешенных адресов, указанных администратором Numa vServer;
- перехват, несанкционированное получение или перебой трафика других ВМ.

3.14.1. Требования функции блокировки

Функция блокировки порта коммутатора Numa vServer поддерживается в сетевых стеках Linux bridge и vSwitch.

Если в среде активировано ролевое управление доступом (RBAC), пользователь, настраивающий блокировку порта коммутатора, должен быть авторизован в системе посредством учётной записи с функциями не ниже Оператора пула или Администратора пула. Если RBAC не активирован, пользователь должен быть авторизован в системе мастера пула посредством учётной записи с правами администратора.

При выполнении команд блокировки порта коммутатора, сеть может быть как онлайн, так и оффлайн.

В виртуальных машинах под управлением ОС Windows значок отключенной сети появляется только в том случае, если в гостевой системе установлены vServer VM Tools.

3.14.2. Примечания

Когда значения функции блокировки порта коммутатора не установлено, виртуальные интерфейсы имеют параметр `network_default`, а Сети – `unlocked`.

Конфигурация блокировки порта коммутатора не поддерживается, когда в контроллер программно-определяемых сетей или иные адаптеры.

Блокировка порта коммутатора не защитит от таких действий арендаторов облака, как:

- осуществление атаки на другого арендатора/пользователя на том же IP-уровне. Однако блокировка порта коммутатора может предотвратить атаки в рамках одного IP-уровня, если они осуществляются следующим образом:
  - действия под видом законного пользователя/арендатора облака;
  - попытка перехвата трафика, предназначенного другому пользователю;

© 2025 Нума Технологии, ООО

- истощение ресурсов сети;
- получение трафика, предназначенного другим ВМ посредством чрезмерной лавинной маршрутизации (для широковещательных MAC-адресов или MAC-адресов с неизвестным назначением).

И соответственно блокировка порта коммутатора не контролирует то, куда ВМ может отправлять трафик.

3.14.2.1. Примечания по реализации функции

Применить функцию блокировки порта коммутатора можно либо с помощью командной строки, либо с помощью ПО совместимого с API. Однако в крупных средах, где автоматизация играет первостепенную роль, наиболее типичным методом применения может являться использование API.

3.14.2.2. Принцип блокировки порта коммутатора

Функция блокировки порта коммутатора позволяет контролировать фильтрацию пакетов на одном или двух уровнях:

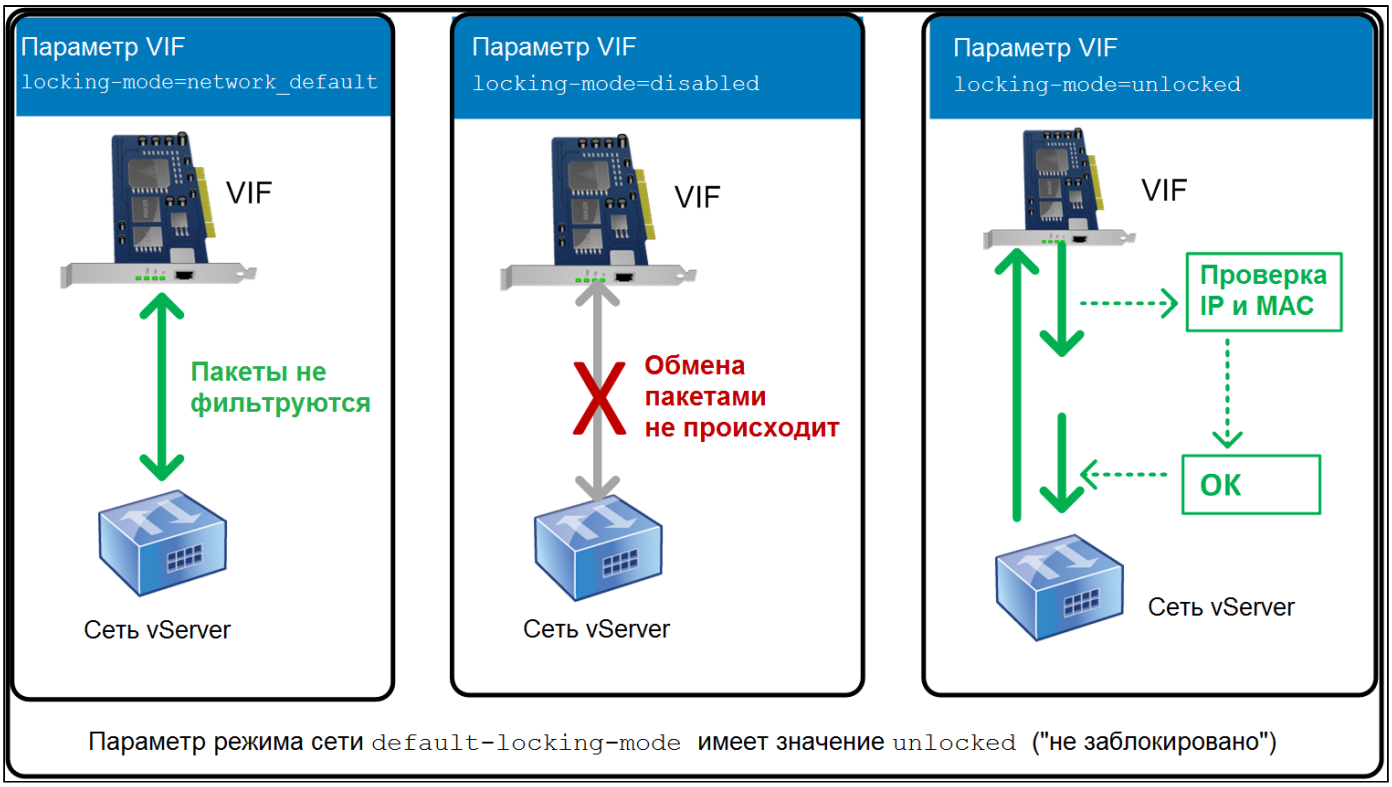
- на уровне виртуального сетевого интерфейса. То, каким образом должны фильтроваться пакеты данных, определяется установками виртуального сетевого интерфейса. Можно настроить виртуальный сетевой интерфейс так, чтобы в целом запретить виртуальной машине отправлять трафик, ограничить возможность виртуальной машины отправлением трафика, использующего только заданный IP-адрес, или разрешить виртуальной машине отправлять трафик на любой IP-адрес сети, подключенной к данному виртуальному сетевому интерфейсу;
- на уровне сети. То, каким образом должны фильтроваться пакеты данных, определяется сетью Numa vServer. Когда режим блокировки виртуального сетевого интерфейса установлен на `network_default`, это говорит о том, что, то какой трафик можно пропускать, определяется настройками блокировки на уровне сети.

Работа функции не зависит от того, какой сетевой стек используется. Однако Linux bridge не полностью поддерживает блокировку порта коммутатора в IPv6 сетях.

3.14.2.3. Варианты режима блокировки виртуального сетевого интерфейса

Функция блокировки порта коммутатора Numa vServer представляет собой режим блокировки с четырьмя вариантами настройки виртуального сетевого интерфейса. Эти варианты могут быть применимы только в том случае, когда виртуальный сетевой интерфейс подключен к работающей ВМ.

© 2025 Нума Технологии, ООО



Блокировка порта коммутатора

Рисунок выше показывает, как ведет себя виртуальный сетевой интерфейс (VIF) в трёх различных вариантах режима блокировки, когда параметр, отвечающий за режим блокировки самой сети (параметр `default-locking-mode`) находится в состоянии `unlocked`.

На первом изображении рисунка, виртуальный сетевой интерфейс настроен по умолчанию (`locking-mode=network_default`), поэтому трафик, исходящий от ВМ, не фильтруется.

На втором изображении, виртуальный сетевой интерфейс не отправляет и не получает пакеты трафика, поскольку режим блокировки `disabled` запрещает обмен трафиком.

На третьей изображении рисунка, виртуальный сетевой интерфейс находится в состоянии `unlocked`, поэтому он может отправлять только пакеты трафика с заданными MAC- и IP-адресами.

Подробнее значения параметра `locking-mode` описаны ниже:

- `network_default` («для сети по умолчанию»). Когда режим виртуальной сети установлен в значение `network_default`, сервер использует параметр сети `default-locking-mode` чтобы определить, следует ли фильтровать пакеты, проходящие через виртуальную сеть и как это делать. Соответственно, поведение отличается в зависимости то того, какое из значений параметра установлено для сети:
  - `default-locking-mode=disabled` («запрещено»), Numa vServer применяет правило фильтрации, по которому виртуальный сетевой интерфейс удаляет весь трафик;
  - `default-locking-mode=unlocked` («не заблокировано»), Numa vServer снимает все правила фильтрации по отношению к виртуальному сетевому интерфейсу. По умолчанию этот параметр режима блокировки установлен на значение `unlocked` («разблокирован»).

Режим блокировки сети по умолчанию не влияет на подключенные VIF, состояние блокировки которых отличается от `network_default`.

Предупреждение

Параметр `default-locking-mode` сети с подключенным активным виртуальным сетевым интерфейсом, не подлежит изменению.

© 2025 Нума Технологии, ООО

- `locked` («заблокирован). Numa vServer применяет правила фильтрации, согласно которым через виртуальный сетевой интерфейс может проходить трафик, отправленный только с определённых MAC- и IP-адресов или только на определённые MAC- и IP-адреса. В данном режиме, если не указано ни одного IP-адреса, виртуальная машина не может передавать трафик через данный виртуальный сетевой интерфейс (данной сети).

Чтобы указать IP-адреса, с которых VIF принимает трафик, используйте IP-адреса IPv4 или IPv6 с помощью параметров `ipv4_allowed` или `ipv6_allowed`. Однако если у вас настроен мост Linux, не вводите адреса IPv6.

Numa vServer позволяет вводить адреса IPv6, когда Linux bridge активен. Однако не может фильтровать на основе введенных адресов IPv6. Причина в том, что у Linux Bridge нет модулей для фильтрации пакетов протокола обнаружения соседей (NDP). Следовательно, полная защита не может быть реализована, и ВМ смогут выдавать себя за другие ВМ путем подделки пакетов NDP. В результате, если вы укажете хотя бы один адрес IPv6, то Numa vServer пропускает весь трафик IPv6 через VIF. Если вы не укажете адреса IPv6, то не пропускает трафик IPv6 в VIF.

- `unlocked` («не заблокирован»). Через виртуальный сетевой интерфейс может проходить весь трафик. То есть к трафику, проходящему через виртуальный сетевой интерфейс, фильтрация не применяется.
- `disabled` («запрещён»). Трафик вообще не может проходить через виртуальный сетевой интерфейс, то есть происходит его удаление.

3.14.2.4. Настройка блокировки порта коммутатора

В данном пункте описываются три различные процедуры:

- ограничение работы виртуальных сетевых интерфейсов использованием определенного IP-адреса;
- добавление IP-адреса к существующему списку ограничений (например, когда необходимо добавить IP-адрес к виртуальному сетевому интерфейсу);
- удаление IP-адреса из существующего списка ограничений.

Если режим виртуального сетевого интерфейса находится в состоянии `locked`, то он сможет использовать только адреса, указанные в параметрах `ipv4_allowed` или `ipv6_allowed`.

Потому как в некоторых относительно редких случаях, виртуальные сетевые интерфейсы могут иметь более одного IP-адреса, то возможно указать несколько IP-адресов для одного виртуального сетевого интерфейса.

Эти процедуры можно выполнить как до, так и после подключения виртуального сетевого интерфейса (или запуска виртуальной машины).

Чтобы ограничить работу виртуальных сетевых интерфейсов с определённым IP-адресом необходимо:

- перевести параметр режима `default-locking` в состояние `locked`, если этот режим в данный момент не используется, команда:

```
1  xe vif-param-set uuid=<vif-uuid> locking-mode=locked
```

Команда `xe vif-uuid` выведет UUID виртуального сетевого интерфейса, которому вам необходимо разрешить отправлять трафик. Чтобы получить UUID, выполните команду `xe vif-list` на сервере. Команда `xe vm-uuid` укажет виртуальную машину, в отношении которой выведена данная информация.

- чтобы указать IP-адреса, с которых виртуальной машине можно отправлять трафик, необходимо указать один или несколько желаемых IP-адресов версии IPv4. Например:

```
1  xe vif-param-set uuid=<vif-uuid> ipv4-allowed=<список ipv4-адресов через запятую>
```

- или указать один или несколько желаемых IP-адресов версии IPv6. Например:

```
1  xe vif-param-set uuid=<vif-uuid> ipv6-allowed=<список ipv6-адресов через запятую>
```

Через запятую можно указать несколько IP-адресов.

Выполнив предыдущую процедуру ограничения работы виртуальных сетевых интерфейсов с определённым IP-адресом, можно добавить к этому ограничению один или несколько IP-адресов, которые сможет использовать виртуальный сетевой интерфейс.

- чтобы добавить IP-адрес к существующему списку, следует указать IP-адрес версии IPv4. Например:

© 2025 Нума Технологии, ООО

```
xe vif-param-add uuid=<vif-uuid> param-name=ipv4-allowed param-key=<ipv4-адрес>
```

- или указать IP-адрес версии IPv6. Например:

```
xe vif-param-add uuid=<vif-uuid> name=ipv6-allowed param-key=<ipv6-адрес>
```

Если администратор ограничивает работу виртуального сетевого интерфейса использованием двух или более IP-адресов, то можно удалить один из таких IP-адресов из списка.

Чтобы удалить IP-адрес из существующего списка, необходимо указать IP-адрес версии IPv4, которые необходимо удалить. Например:

```
xe vif-param-remove uuid=<vif-uuid> param-name=ipv4-allowed param-key=<ipv4-адрес>
```

или указать IP-адрес версии IPv6, который необходимо удалить. Например:

```
xe vif-param-remove uuid=<vif-uuid> param-name=ipv6-allowed param-key=<ipv6-адрес>
```

3.14.2.5. Запрет ВМ отправлять или получать трафик из определенной сети

Описанная ниже процедура запрещает виртуальной машине пропускать трафик через виртуальный сетевой интерфейс. Эту процедуру можно использовать, чтобы запретить взаимообмен трафиком между виртуальной машиной и определенной сетью. Это предоставляет возможность более тонкого контроля, чем полный запрет на обмен трафиком с сетью.

Нет необходимости отключать виртуальный сетевой интерфейс, чтобы установить режим его блокировки; команда изменит правила фильтрования, не отключая его. В этом случае сетевое соединение по-прежнему присутствует, однако VIF отбрасывает все пакеты, которые виртуальная машина пытается отправить.

> **Примечание**
>
> Чтобы получить UUID виртуального сетевого интерфейса, необходимо выполнить команду `xe vif-list`. Поле `device` показывает номер устройства виртуального сетевого интерфейса.

Чтобы запретить виртуальному сетевому интерфейсу принимать трафик из сети, необходимо ввести команду:

```
xe vif-param-set uuid=<vif-uuid> locking-mode=disabled
```

3.14.2.6. Снятие ограничения работы виртуального сетевого интерфейса

Чтобы вернуться к разблокированному состоянию виртуального сетевого интерфейса, необходимо перевести режим `default-locking` виртуального сетевого интерфейса в состояние `unlocked` (если это состояние уже в данный момент не используется), выполнив следующую команду:

```
xe vif-param-set uuid=<vif_uuid> locking-mode=unlocked
```

© 2025 Нума Технологии, ООО

3.14.2.7. Упрощённая настройка режима блокировки виртуального сетевого интерфейса

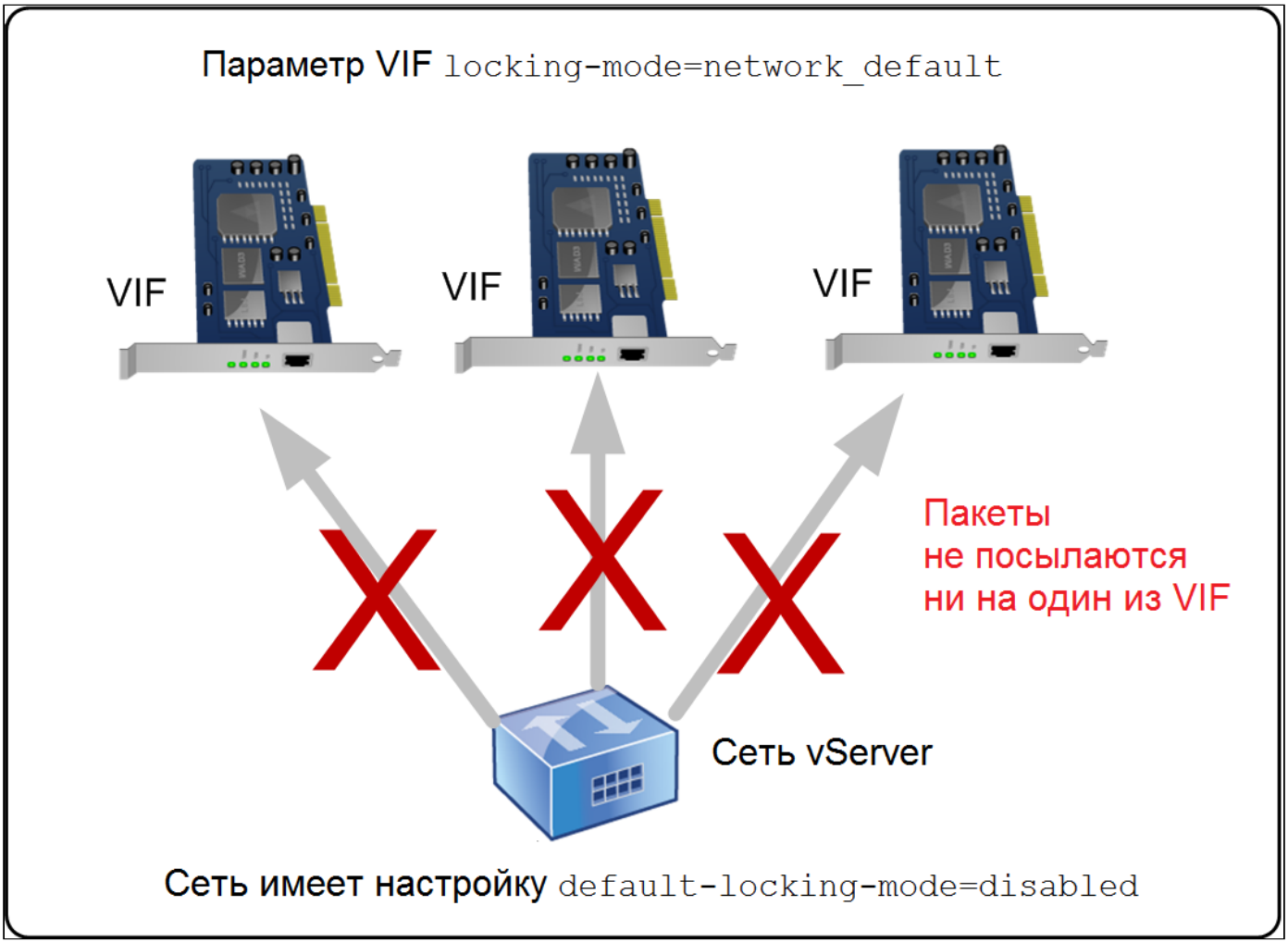
Вместо того чтобы выполнять команды режима блокировки виртуального сетевого интерфейса для каждого в отдельности, можно заблокировать все виртуальные сетевые интерфейсы по умолчанию. Чтобы добиться этого, необходимо внести изменения в фильтрацию пакетов трафика на уровне сети, благодаря которой сеть Numa vServer определяет и какие пакеты необходимо фильтровать, согласно процедуре, описанной в пп. Использование блокировки порта коммутатора.

В частности, настройка сетевого параметра `default-locking-mode` определяет поведение новых виртуальных сетевых интерфейсов с настройками по умолчанию. Если `locking-mode` виртуального сетевого интерфейса установлен по умолчанию (`default`), то виртуальный сетевой интерфейс обращается к сетевому режиму блокировки (`default-locking-mode`), чтобы определить, фильтруются ли пакеты трафика, проходящие через виртуальный сетевой интерфейс, а также то, каким образом происходит фильтрация:

- `unlocked` («разблокирован»). Numa vServer разрешает ВМ отправлять трафик на любой IP-адрес сети, подключенной к данному виртуальному сетевому интерфейсу;
- `disabled` («запрещён»). Numa vServer применяет правило фильтрации, по которому виртуальный сетевой интерфейс удаляет весь трафик.

По умолчанию параметр `default-locking-mode` установлен на `unlocked` для всех сетей.

Устанавливая режим блокировки виртуального сетевого интерфейса в состояние по умолчанию (`network_default`), можно использовать эту настройку в качестве базовой конфигурации (на уровне сети) для всех вновь созданных виртуальных сетевых интерфейсов, подключенных к определенной сети.



Блокировка виртуального сетевого интерфейса в пуле ресурсов

© 2025 Нума Технологии, ООО

Рисунок выше показывает, как виртуальный сетевой интерфейс, в случае если он настроен по умолчанию (`locking-mode=network_default`), руководствуется значением параметра `default-locking-mode` сети. Ко всей сети применен параметр `default-locking-mode=disabled` , поэтому виртуальные сетевые интерфейсы не могут пропускать трафик.

Чтобы изменить настройку режима блокировки по умолчанию для сети необходимо создать сеть и изменить параметр `default-locking-mode` , выполнив следующую команду:

```
xe network-param-set uuid=<network-uuid> default-locking-mode=[unlocked|disabled]
```

Чтобы получить идентификатор UUID сети, нужно выполнить команду `xe network-list` . Эта команда отобразит идентификаторы всех сетей на сервере, где была выполнена команда.

Чтобы узнать значение по умолчанию сетевого режима блокировки, следует выполнить одну из следующих команд:

```
xe network-param-get uuid=<network-uuid> param-name=default-locking-mode
```

или

```
xe network-list uuid=<network-uuid> params=default-locking-mode
```

3.14.2.8. Применение настроек сети для фильтрации трафика к виртуальному сетевому интерфейсу

Чтобы использовать настройки сети для фильтрации трафика к определенному VIF необходимо выполнить следующие шаги:

- перевести режим блокировки виртуального сетевого интерфейса в состояние `network_default` (если этот режим в данный момент уже не используется), выполнив следующую команду:

```
xe vif-param-set uuid=<vif_uuid> locking-mode=network_default
```

- перевести параметр `default-locking` в состояние `unlocked` (если этот режим в данный момент уже не используется), выполнив следующую команду:

```
xe network-param-set uuid=<network-uuid> default-locking-mode=unlocked
```

3.14.2.9. Назначение цели для сети

Назначение цели для сети может использоваться для добавления дополнительных функций. Например, возможность использовать сеть для создания соединений NBD.

Чтобы назначить цель необходимо выполнить команду:

```
xe network-param-add param-name=purpose param-key=<purpose> uuid=<network-uuid>
```

Для удаления цели из сети выполнить команду:

```
xe network-param-remove param-name=purpose param-key=<purpose> uuid=<network-uuid>
```

В настоящее время доступными значениями для сетевых целей являются `nbd` и `insecure_nbd` .

© 2025 Нума Технологии, ООО

3.15. Устранение неполадок сети

3.15.1. Обнаружение ошибок и неисправностей сети

Некоторые модели сетевых карт требуют обновления встроенного программного обеспечения от поставщика для надежной работы под нагрузкой или при включении определенных оптимизаций. Если вы видите поврежденный трафик на виртуальных машинах, попробуйте получить последнюю версию прошивки от вашего поставщика.

Если проблема все еще сохраняется, вы можете использовать CLI для отключения оптимизации приема или передачи разгрузки на физическом интерфейсе:

> **Предупреждение**
>
> Отключение оптимизации приема или передачи разгрузки может привести к потере производительности и увеличению загрузки ЦП.

- определить UUID физического интерфейса:

```
xe pif-list
```

- отключить разгрузку для передачи данных (TX) физического интерфейса:

```
xe pif-param-set uuid=<pif_uuid> other-config:ethtool-tx=off
```

- переподключить физический интерфейс или перезапустить сервер, чтобы изменения вступили в силу.

3.15.2. Аварийный перезапуск сети

Неправильные сетевые настройки могут вызвать потерю соединения с сетью, а сервер может стать недоступным при подключении по SSH. Аварийный перезапуск сети представляет собой простой механизм восстановления и перезагрузки сети сервера.

Эта функция доступна из интерфейса командной строки с помощью команды `xe-reset-networking`.

Неправильные настройки, вызывающие потерю соединения с сетью, могут также включать в себя переименование сетевых интерфейсов, объединение адаптеров или VLAN, или ошибки при изменении интерфейса управления (например, неправильно введённый IP-адрес).

Эта функция должна использоваться только в случае экстренной ситуации, так как она удаляет конфигурацию всех физических сетевых интерфейсов, агрегаций, VLAN и туннелей, имеющих отношение к данному серверу. Гостевые сети и виртуальные сетевые интерфейсы сохраняются. При выполнении этой функции, виртуальные машины будут принудительно выключены, поэтому рекомендуется перед выполнением команды, выключить виртуальные машины. Перед перезапуском, администратор может внести изменения в интерфейс управления и указать, какую IP-конфигурацию следует использовать: DHCP или статическую.

Если мастер пула требует перезапуска сети, она должна быть выполнена до перезапуска сетей всех остальных рядовых участников пула. Затем следует выполнить перезапуск сетей всех остальных серверов сети, чтобы обеспечить однородность сетевой конфигурации пула.

© 2025 Нума Технологии, ООО

> **Примечание**
>
> Если IP-адрес мастера пула (интерфейс управления) изменяется в результате сброса сети или `xe host-management-reconfigure`, примените команду сброса сети к другим серверам в пуле. Это необходимо для того, чтобы участники пула могли повторно подключиться к мастеру пула с его новым IP-адресом. В этой ситуации необходимо указать IP-адрес мастера пула.

> **Внимание!**
>
> Перезапуск сети НЕ поддерживается при включенной функции High Availability (HA). Чтобы при таком сценарии выполнить перезапуск конфигурации сети, необходимо сначала в ручную отключить HA, а затем выполнить команду перезапуска сети.

3.15.2.1. Проверка параметров сети после их сброса

Указав режим конфигурации для перезапуска сети, в интерфейсе командной строки отобразятся настройки, которые будут применены к серверу после перезагрузки. Это будет последней возможностью внести изменения перед применением команды аварийного перезапуска сети.

> **Примечание**
>
> Аварийный перезапуск сети также необходимо применить к остальным серверам пула, чтобы продублировать агрегации, VLAN и туннели в соответствии с новой конфигурации мастера пула.

3.15.2.2. Перезапуск сети с помощью интерфейса командной строки

В таблице ниже показаны доступные необязательные параметры, которые можно применить во время выполнения команды `xe-reset-networking`.

> **Предупреждение**
>
> Ответственность за правильность параметров, указанных для команды `xe-reset-networking`, лежит на администраторе. Необходимо внимательно проверить все указанные параметры. При указании неверных параметров связь с сетью будет потеряна. В такой ситуации рекомендуется повторно выполнить команду `xe-reset-networking`, не указывая никаких параметров.

Перезапуск сетевой конфигурации всего пула необходимо начинать с мастера пула, а затем переходить к перезапуску сети всех остальных серверах пула.

Таблица – Параметры xe-reset-networking

Параметр	Обязательный/ необязательный	Описание
-m, --master	необязательный	IP-адрес интерфейса управления мастера пула. Сбрасывает на последнее известное значение IP-адреса мастер пула
--device	необязательный	

© 2025 Нума Технологии, ООО

Параметр	Обязательный/ необязательный	Описание
		Имя устройства административного интерфейса. Сбрасывает на значение имени устройства, указанное при установке
-mode=static	необязательный	Позволяет использовать следующие четыре параметра для статической IP-конфигурации административного интерфейса. Если этот параметр не указан, по умолчанию используется значение параметра DHCP
--ip	обязательный, если mode=static	IP-адрес интерфейса управления сервера. Действителен только, если mode=static
--netmask	обязательный, если mode=static	Маска сети интерфейса управления. Действителен только, если mode=static
--gateway	необязательный	Шлюз интерфейса управления. Действителен только, если mode=static
--dns	необязательный	DNS-сервер интерфейса управления. Действителен только, если mode=static

3.15.2.3. Примеры аварийного сброса настроек на мастере пула

Ниже описаны примеры команд, которые могут быть применены к мастеру пула:

- сброс настроек сети для DHCP-конфигурации:

```
xe-reset-networking
```

- сброс настроек сети для статической IP-конфигурации:

```
xe-reset-networking --mode=static --ip=<ip-address> --netmask=<netmask> --gateway=<gateway> --
dns=<dns>
```

- сброс настроек сети для DHCP-конфигурации, если после первоначальной установки произошла смена интерфейса управления:

```
xe-reset-networking --device=<device-name>
```

- сброс настроек сети для статической IP-конфигурации, если после первоначальной установки произошла смена интерфейса управления:

```
xe-reset-networking --device=<device-name> --mode=static --ip=<ip-address> --netmask=<netmask> --
gateway=<gateway> --dns=<dns>
```

3.15.2.4. Примеры аварийного сброса настроек для рядового участника пула

Все примеры, приведённые в предыдущем пункте, также применимы и для рядовых серверов пула. Кроме того, можно указать IP-адрес мастера пула (что будет необходимым в случае его изменения). Ниже приведены примеры управления конфигурацией рядовых участников пула:

- сброс настроек сети для конфигурации DHCP:

```
xe-reset-networking
```

- сброс настроек сети для конфигурации DHCP при изменении IP-адреса мастера пула:

```
xe-reset-networking --master=<master-ip-address>
```

© 2025 Нума Технологии, ООО

- сброс настроек сети для статической IP-конфигурации, при условии, что IP-адрес мастера пула не менялся:

```
xe-reset-networking --mode=static --ip=<ip-address> --netmask=<netmask> --gateway=<gateway> --
dns=<dns>
```

- сброс настроек сети для DHCP-конфигурации, если после первоначальной установки произошла смена интерфейса управления и IP-адреса мастера пула:

```
xe-reset-networking --device=<device-name> --master=<master-ip-address>
```

© 2025 Нума Технологии, ООО

4. Администрирование системы хранения

В этом разделе описывается, как физическое оборудование для хранения данных сопоставляется с виртуальными машинами (ВМ) и программными объектами, используемыми API управления для выполнения задач, связанных с хранилищем. Подробные разделы по каждому из поддерживаемых типов хранилищ данных содержат следующую информацию:

- процедуры создания хранилища для ВМ с помощью интерфейса командной строки (CLI) с параметрами конфигурации устройств, зависящими от типа хранилища;
- создание снимков состояния для целей резервного копирования;
- рекомендации по управлению хранилищем;
- настройка параметров QoS для виртуального диска.

4.1. Хранилище данных

Хранилище данных (Storage Repsitory или SR) – это определенный целевой объект хранения, в котором хранятся образы виртуальных дисков (VDI) виртуальных машин. VDI является дисковой абстракцией, содержащей контент виртуального жесткого диска (HDD).

Образы VDI поддерживаются большим количеством различных типов хранилищ.

Хранилища Numa vServer имеют встроенную поддержку дисков, как локальных:

- IDE;
- SATA;
- SCSI;
- SAS.

Так и удалённых:

- iSCSI;
- NFS;
- CIFS/SMB;
- SAS;
- Fibre Channel.

Хранилища данных и VDI предоставляют поддержку усовершенствованных функций, таких как thin-provisioning (возможность экономичного выделения места для нужд хранения данных, далее по тексту термин даётся в англоязычном варианте либо как «экономичное выделение»), поддержка снимков состояния VDI (snapshots) и быстрого клонирования, которые будут выполняться на поддерживающих их подсистемах хранения. Для подсистем хранения, не поддерживающих эти операции непосредственно, предоставляется программный стек на основе спецификации механизма предоставления виртуального жесткого диска (Microsoft Virtual Hard Disk, VHD), реализующий эти операции программно.

Каждый сервер может использовать множество хранилищ данных и различные их типы одновременно. Хранилища данных могут быть общими для пула или выделенными для определенного сервера. Общее хранилище используется несколькими серверами в пуле ресурсов. Общее хранилище должно быть доступно по сети для каждого сервера в пуле. Рекомендуется иметь, по крайней мере, одно общее хранилище в пуле, подключенное в каждому серверу. Общее хранилище не может быть общим для нескольких пулов.

Команды управления хранилищами данных предоставляют операции для создания, удаления, изменения размеров, клонирования, присоединения и обнаружения содержащихся в них отдельных VDI (подробнее см. в разделе Команды управления хранилищами данных).

Для типов хранилищ на базе блочных устройств процесс создания нового хранилища подразумевает затирание любых существующих данных в указанном месте хранения.

© 2025 Нума Технологии, ООО

4.1.1. Образы виртуальных дисков (VDI)

Образы виртуальных дисков (VDI) являются абстрактными (логическими) объектами хранения, которые предоставляются виртуальным машинам как виртуальные жесткие диски (HDD). Образ VDI является основной единицей виртуализированного хранения в Numa vServer. Подобно хранилищам данных, образы VDI являются постоянными объектами на диске и существуют независимо от серверов. Фактическое представление данных на диске различается в зависимости от типа хранилища и управляется при помощи отдельного интерфейса программного модуля, называемого SM API (для каждого хранилища отдельно).

4.1.2. Физические блочные устройства (PBD)

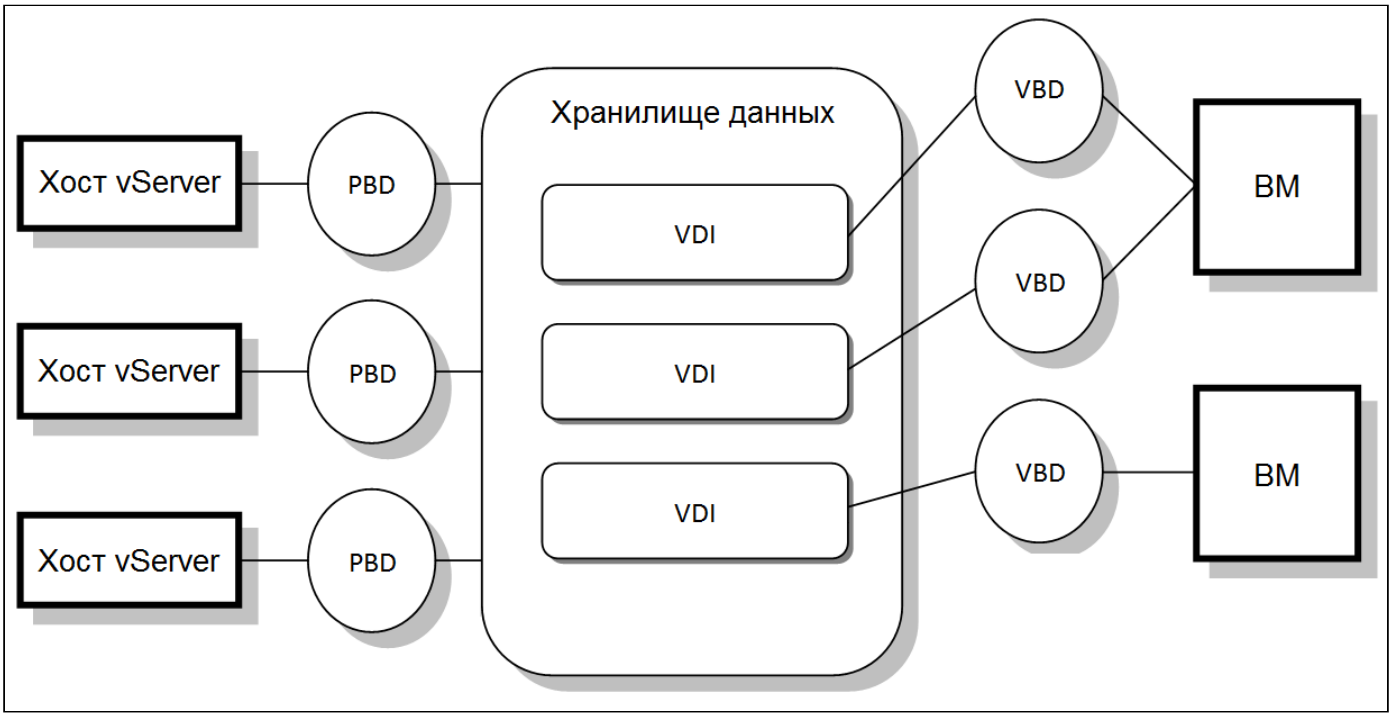
Физические блочные устройства (PBD) представляют собой интерфейс между физическим сервером и присоединённым хранилищем. PBD являются соединительными объектами, которые позволяют сопоставить хранилище с сервером. PBD хранят поля конфигурации устройства, которые используются для поделючения и взаимодействия с целевым хранилищем (storage target). Например, конфигурация устройства NFS включает IP-адрес сервера NFS и связанный путь, который Numa vServer использует для монтирования диска. Объекты PBD управляют присоединением данного хранилища к данному хосту Numa vServer.

4.1.3. Виртуальные блочные устройства (VBD)

Виртуальные блочные устройства (VBD), как и PBD, являются связующими объектами, позволяющими задавать соответствие между образами VDI и ВМ.

В дополнение к обеспечению механизма для присоединения (также названного подключением, англ. plugging) VDI к ВМ, VBD позволяет выполнить настройку параметров QoS, статистики и возможности загрузки с данного VDI.

4.1.4. Взаимосвязь объектов хранения



Взаимосвязь физических, логических и виртуальных элементов системы хранения

На рисунке выше показано, как связаны объекты хранения.

© 2025 Нума Технологии, ООО

4.1.4.1. Форматы виртуальных дисков

Существуют следующие типы сопоставления физического хранилища с VDI:

- VHD на базе логического тома на LUN (Logical Unit – логический блок, логическая единица, на которую разбивается контейнер хранилища данных). По умолчанию в Numa vServer систему хранения на базе блочных устройств добавляет менеджер логического тома (англ. Logical Volume Manager, LVM) на диск – либо на локально подключенное устройство (хранилище типа LVM), либо на LUN, присоединённый к SAN по протоколу Fibre Channel (хранилище типа LVMoHBA), iSCSI (хранилище типа LVMoISCSI) или SAS (хранилище типа LVMoHBA). Образы VDI представляются как отдельные тома с менеджерами LVM и хранятся в формате VHD для возможности экономичного выделения памяти (thin provisioning) для связанных узлов при создании снимков и клонировании.
- VHD на базе файла в файловой системе. Образы ВМ хранятся как файлы формата VHD с возможностью thin-provisioning в локальной (не совместно используемой) файловой системе (хранилища типа EXT), или в совместно используемой NFS (хранилище NFS).

4.1.4.2. Типы VDI

В общем случае создаётся VDI формата VHD. Администратор может решить использовать «сырой» («неразмеченный», англ. raw) тип при создании VDI (с помощью команд xe). Чтобы проверить, был ли VDI создан с `type=raw`, нужно проверить его map-параметр `sm-config`. С этой целью могут использоваться, соответственно, команды `xe sr-param-list` и `xe vdi-param-list`.

4.1.4.3. Создание не размеченного виртуального диска (raw) при помощи интерфейса CLI

1. Выполните следующую команду для создания VDI, указав UUID хранилища, в которое требуется поместить виртуальный диск:

```
xe vdi-create sr-uuid=<sr-uuid> type=user virtual-size=<virtual-size> name-label=<VDI_name> sm-config:type=raw
```

2. Присоедините новый виртуальный диск к ВМ и используйте в ней обычные инструменты для создания и форматирования разделов (или используйте новый диск иным образом). Можно использовать команду `xe vbd-create` для создания нового VBD для сопоставления виртуального диска с вашей ВМ.

4.1.4.4. Преобразование между форматами VDI

Невозможно сделать прямое преобразование между форматом VHD и raw. Вместо этого можно создать новый VDI (неразмеченный – raw, как описано выше, или VHD), а затем скопировать данные в него из существующего тома. Рекомендуется использовать xe CLI, чтобы быть уверенным, что новый VDI имеет виртуальный размер не меньше копируемого VDI (путем проверки его поля виртуального размера, например, при помощи команды `xe vdi-param-list`). Затем можно присоединить этот новый VDI к ВМ и использовать в ней предпочитаемые инструменты (стандартные инструменты управления дисками в Windows или команда `dd` в Linux), для выполнения прямого блочного копирования данных. Если новый том является томом VHD, важно использовать инструмент, который поможет избежать записи пустых секторов на диск. Это действие может гарантировать оптимальное использование пространства в базовом хранилище – в этом случае подход копирования на основе файлов может быть более подходящим.

4.1.4.5. Образы виртуальных дисков на основе VHD

Образы VHD могут быть объединены в цепочку, что позволяет двум VDI совместно использовать общие данные. В случаях, когда клонируется ВМ с VHD, полученные ВМ совместно используют общие дисковые данные во время клонирования. Каждая ВМ продолжает вносить свои собственные изменения в собственную отдельную версию VDI с механизмом copy-on-write, CoW. Эта функция позволяет быстро клонировать основанные на VHD ВМ из шаблонов, упрощая и ускоряя настройку и развертывание новых ВМ.

Это приводит к созданию со временем деревьев объединённых в цепочку образов VDI, так как ВМ и связанные с ними образы виртуальных дисков клонируются. Когда один из VDI в цепочке удаляется, Numa vServer рационализирует другие VDI в ней для удаления ненужных образов. Этот процесс объединения (англ. coalescing) работает асинхронно. Объем освобожденного дискового пространства и время, необходимое для выполнения процесса, зависят от размера VDI и объема общих данных.

© 2025 Нума Технологии, ООО

Формат VHD, используемый в Numa vServer хранилищами на основе LVM или файлов, использует механизм экономичного выделения места thin-provisioning. Файл образа автоматически расширяется (блоками, по 2 Мбайта) по мере того, как ВМ записывает данные на диск. Для VHD на базе файла это имеет значительное преимущество: файлы образа ВМ занимают не больше пространства в физической системе хранения, чем реально требуется для записанных на них данных. В случае VHD, основанного на LVM, объём логического контейнера должен быть изменён до виртуального размера VDI, однако при создании снимка или клона неиспользуемое место на диске CoW-экземпляра исправляется.

Различие между описанными двумя вариантами поведения может быть характеризовано следующим образом:

- для VHD, основанных на LVM, «разностные» узлы в цепочке используют ровно столько данных, сколько было записано на диск, но узлы-«листья» такой древоподобной структуры (то есть клоны VDI) занимают виртуальный диск полностью. Узлы-«листья», представляющие собой снимки VDI, продолжают занимать минимальное требуемое пространство, когда не используются, и для сохранения своего размера могут быть присоединены в режиме «только для чтения». Когда узлы-снимки присоединяются в режиме «чтение и запись», они будут полностью «растянуты» на всё свободное пространство диска при присоединении и возвращены к реальным размерам при отсоединении;
- в случае VHD на базе файлов все узлы используют лишь объёмы памяти, соразмерные объёмам записанных данных, и размеры файлов, соответствующих узлам-«листьям», растут в соответствии с темпами активной записи. Если для новой ВМ выделяется VDI на 100 Гбайт, и устанавливается ОС, файл VDI физически будет иметь размер, равный совокупному объёму данных ОС, записанных на диск, плюс небольшие издержки метаданных.

При клонировании ВМ на основе единственного шаблона VHD каждая дочерняя ВМ формирует цепочку, где записаны новые изменения к новой ВМ, а старые блоки считываются непосредственно из родительского шаблона. Если новая ВМ была преобразована в дальнейшем в шаблон и из него появляется ещё больше клонов, получающаяся цепочка приведёт к ухудшению производительности. Numa vServer поддерживает максимальную длину цепочки 30, но обычно не рекомендуется приближаться к этому пределу без серьезных оснований. При наличии сомнений лучше скопировать ВМ, используя команду vm-copy, которая автоматически сбросит длину цепочки в «0».

4.1.4.5.1. Замечания по объединению VHD

Только один подобный процесс объединения может быть активен в хранилище в каждый момент времени. Поток этого процесса запускается на главном хосте (мастере) хранилища.

Если имеет место критическая работа ВМ мастера пула и медленный случайный ввод-вывод из-за этого процесса, можно предпринять следующие шаги:

- переместить ВМ на другой хост (миграция);
- установить дисковый приоритет ввода-вывода в более высокий уровень и скорректировать настройки планировщика (см. раздел Настройки QoS для виртуальных дисков).

4.1.5. Форматы хранилищ

Новые хранилища могут быть созданы через интерфейс CLI командой `xe sr-create`. Эта команда создаёт новое хранилище данных на аппаратных средствах хранения (потенциально уничтожая любые уже существующие данные на них) и создает программный объект «хранилище» и соответствующую запись PBD, позволяя виртуальным машинам использовать хранилище. К успешно созданному хранилищу автоматически подключается PBD. Если для хранилища установлен флаг `shared=true`, запись PBD создаётся и подключается для каждого сервера Numa vServer в пуле.

При создании хранилища с поддержкой протокола IP (iSCSI или NFS), можно сконфигурировать под его нужды сетевой адаптер/интерфейс, обрабатывающий управляющий трафик, или новый сетевой адаптер. вы можете настроить один из следующих сетевых адаптеров в качестве сети хранения: NIC, который обрабатывает трафик управления, или новый NIC для трафика хранения. Процесс присвоения IP-адреса сетевому интерфейсу (адаптеру) описан в разделе Настройка сетевого интерфейса, выделенного для соединения с хранилищем.

Все типы хранилищ в Numa vServer поддерживают изменение размеров VDI, быстрое клонирование и снимки состояний. Хранилища на основе LVM (локальные, iSCSI или HBA) обеспечивают thin-provisioning для снимков состояния и скрытых родительских узлов. Другие типы хранилищ (EXT3, EXT4, NFS) имеют полную поддержку thin-provisioning, в том числе для активных виртуальных дисков.

© 2025 Нума Технологии, ООО

> **Внимание!**
>
> Когда VHD VDI не присоединены, например, в случае снимка VDI, они сохраняются по умолчанию с поддержкой thin-provisioning. Если вы пытаетесь повторно подключить VDI, убедитесь, что на диске достаточно места для превращения его в диск с неэкономичным выделением (thick-provisioning) при попытке присоединить его. Клоны VDI будут поддерживать `thick-provisioning`.

Максимальные поддерживаемые размеры VDI описаны в таблице ниже.

Таблица – Поддерживаемые максимальные размеры VDI

Формат хранилища данных	Максимальный размер VDI
EXT3	2 Тбайта
LVM	2 Тбайта
NFS	2 Тбайта
LVMoFCOE	2 Тбайта
LVMoiSCSI	2 Тбайта
LVMoHBA	2 Тбайта

4.1.5.1. Локальный LVM

Хранилища типа локальный LVM представляют собой диски в локально присоединенной группе томов. Рекомендуется присоединять только одно локальное хранилище на сервер.

По умолчанию Numa vServer использует локальный диск на том физическом хосте, на котором он установлен. Менеджер логического тома (LVM) Linux используется для управления хранением ВМ. Образы VDI представляются в формате VHD на логическом томе LVM указанного размера.

4.1.5.1.1. Особенности работы с LVM

Реализованные в Numa vServer возможности создания снимков состояния и быстрого клонирования для хранилищ типа LVM влекут неотъемлемые потери производительности. Когда требуется оптимальная производительность, Numa vServer поддерживает создание из образов VDI в неразмеченном формате (raw) в дополнение к формату VHD по умолчанию. Функциональность снимка состояния Numa vServer не поддерживается на raw-образах VDI.

> **Примечание**
>
> Нетранспортабельные снимки, использующие по умолчанию провайдер Windows VSS, будут работать с любым типом из VDI.

> **Предупреждение**
>
> Не следует делать снимок ВМ, имеющей присоединенные диски с типом `type=raw`. Это может привести к созданию частичного снимка. В этой ситуации можно идентифицировать такой снимок VDI путём проверки поля `snapshot-of` и затем удалить его.

© 2025 Нума Технологии, ООО

4.1.5.1.2. Создание локального хранилища на основе LVM

Хранилище на основе LVM создаётся по умолчанию при установке сервера.

Для создания локального хранилища LVM на `/dev/<раздел-диска>` используется следующая команда:

```
xe sr-create host-uuid=<host-uuid> content-type=user name-label=<sr-name> shared=false device-config:device=/dev/<раздел-диска> type=lvm
```

где `device` – имя устройства на локальном сервере для использования в хранилище. Вы также можете предоставить список имен, разделенных запятыми.

4.1.5.2. Локальный EXT3

Использование EXT3 позволяет выполнять экономичное выделение места (thin-provisioning) на локальных хранилищах. Однако типом хранилища по умолчанию является LVM, поскольку он обеспечивает постоянную производительность записи и предотвращает чрезмерное выделение ресурсов хранилища (англ. overcommitting). Если вы используете EXT3, то можете заметить снижение производительности в следующих случаях:

- при выполнении операций жизненного цикла ВМ (создание, приостановка и возобновление ВМ);
- при создании больших файлов в файловой системе ВМ.

Локальное хранилище на основе EXT3 должно быть сконфигурировано с помощью интерфейса CLI.

4.1.5.2.1. Создание локального хранилища на основе EXT3 (ext)

Для создания локального хранилища EXT3 на `/dev/<раздел-диска>` используется следующая команда:

```
xe sr-create host-uuid=<host-uuid> content-type=user name-label=<sr-name> shared=false device-config:device=/dev/<раздел-диска> type=ext
```

где `device` – имя устройства на локальном сервере для использования в хранилище. Вы также можете предоставить список имен, разделенных запятыми.

4.1.5.3. Udev

Тип udev представляет устройства, подключенные как образы VDI при помощи диспетчера устройств udev.

Numa vServer имеет два хранилища типа udev, которые представляют собой съемные хранилища: первое используется для CD или DVD-диска в физическом приводе CD-ROM или DVD-ROM сервера Numa vServer, второе – для USB-устройства, подключенного к USB-порту Numa vServer. Образы VDI, соответствующие этим носителям, подключаются и отключаются в соответствии с установкой и отсоединением CD-дисков и USB-накопителей.

4.1.5.4. ISO

Тип ISO обрабатывает образы CD, хранящиеся в виде файлов в формате ISO. Этот тип хранилищ полезен для создания общих библиотек ISO.

Доступны следующие типы ISO-хранилищ:

- nfs_iso: тип хранилища NFS ISO обрабатывает образы компакт-дисков, хранящиеся в виде файлов в формате ISO, доступных как общий ресурс NFS;
- cifs: тип хранилища для общего доступа к файлам Windows (SMB/CIFS). Обрабатывает образы компакт-дисков, хранящихся в виде файлов в формате ISO, доступных в качестве общего ресурса Windows (SMB/CIFS).

© 2025 Нума Технологии, ООО

Если вы не укажете тип хранилища при создании, Numa vServer использует сведения из параметра конфигурации `location` для определения типа.

Для хранилищ, в которых хранится библиотека ISO-образов, параметр `content-type` (тип контента) должен быть установлен в значение `iso`. Например:

```
xe sr-create host-uuid=<host-uuid> content-type=iso type=iso name-label=<sr-name> device-config:location=<path-to-mount>
```

Для монтирования ISO-хранилища можно использовать NFS или SMB.

Рекомендуется использовать SMB версии 3.0 для монтирования ISO-хранилища на файловом сервере Windows. Версия 3.0 выбрана по умолчанию, потому что она более безопасна и надежна, чем SMB версии 1.0. Однако есть возможность использовать SMB версии 1.0. Например:

```
xe sr-create content-type=iso type=iso shared=true device-config:location=<path-to-mount> device-config:username=<username> device-config:cifspassword=<password> device-config:type=cifs device-config:vers=<Choose either 1.0 or 3.0> name-label=<sr-name>
```

4.1.5.5. Программная поддержка iSCSI

Numa vServer поддерживает общие хранилищв на iSCSI LUN. Поддержка реализуется при помощи iSCSI-инициатора Open-iSCSI (программное обеспечение) или при помощи поддерживаемого адаптера шины хоста (англ. Host Bus Adapter, HBA) iSCSI. Шаги, которые необходимо выполнить для использования iSCSI HBA, идентичны шагам для Fibre Channel HBA (см. раздел Удаление записей устройств SAS, FC или iSCSI основанных на HBA).

Поддержка общего iSCSI при помощи программного обеспечения инициатора iSCSI реализована на основе Менеджера томов Linux (LVM) и обеспечивает те же преимущества производительности, которые обеспечивают LVM VDI в случае локального диска. Общее хранилище iSCSI с использованием программного инициатора сервера могут поддерживать живую миграцию ВМ: ВМ могут быть запущены на любых серверах пула и перемещаться между ними без существенной потери времени.

Хранилища iSCSI полностью используют LUN, определённый в процессе создании хранилища, и не могут охватывать более одного LUN. Поддержка CHAP предоставляется для аутентификации пользователя как во время инициализации пути данных, так и на этапах обнаружения LUN (LUN discovery phases).

> **Примечание**
>
> Размер блока iSCSI LUN должен составлять 512 байт

4.1.5.5.1. Настройка iSCSI для хостов Numa vServer

Все инициаторы и цели iSCSI должны иметь уникальное имя, чтобы гарантировать их уникальную идентификацию в сети. Инициатор имеет адрес инициатора iSCSI, а цель имеет целевой адрес iSCSI. В совокупности они дают так называемые квалифицированные имена iSCSI (iSCSI Qualified Names, IQN).

Сервера Numa vServer поддерживают наличие единственного инициатора iSCSI, который автоматически создается и настраивается с помощью случайного IQN во время установки сервера. Один инициатор может использоваться для соединения с несколькими целями iSCSI одновременно.

Цели iSCSI обычно обеспечивают управление доступом с помощью списков IQN инициатора iSCSI. Все цели iSCSI/LUN, к которым обращается сервер Numa vServer, должны быть настроены на разрешение доступа IQN инициатора сервера. Точно так же целевые LUN, которые будут использоваться в качестве общего iSCSI-хранилища, должны быть настроены на разрешение доступа для IQN всех серверов пула.

© 2025 Нума Технологии, ООО

> Примечание
>
> Целевые объекты iSCSI, которые не обеспечивают управление доступом, обычно по умолчанию ограничивают доступ LUN к одному инициатору для обеспечения целостности данных. Если iSCSI LUN используется в качестве общего хранилища на нескольких серверах в пуле, убедитесь, что для указанного LUN включен доступ с несколькими инициаторами

Значение IQN сервера Numa vServer можно настроить с помощью следующей команды при использовании программного инициатора iSCSI:

```
xe host-param-set uuid=<host-uuid> other-config:iscsi_iqn=<new_initiator_iqn>
```

> Внимание!
>
> 1. У каждой цели iSCSI и инициатора обязательно должно быть уникальное IQN. Если используется неуникальный (групповой) идентификатор IQN, может произойти повреждение данных или отказ в доступе к LUN.
> 2. Не следует изменять IQN сервера Numa vServer с подключенными iSCSI-хранилищем. Это может привести к сбоям подключения с новымм целямм или существующим хранилищем.

4.1.5.6. Программное хранилище FCoE

Программное обеспечение FCoE обеспечивает стандартную структуру, к которой поставщики оборудования могут подключить свои сетевые адаптеры с поддержкой FCoE и получить те же преимущества, что и аппаратный FCoE. Эта функция исключает необходимость использования дорогих адаптеров HBA.

Перед созданием программного хранилища FCoE вручную выполните настройку, необходимую для предоставления LUN серверу. Эта настройка включает в себя настройку структуры FCoE и выделение LUN для общедоступного имени вашей сети SAN (PWWN). После завершения этой настройки доступный LUN подключается к CNA сервера как устройство SCSI. Затем устройство SCSI можно использовать для доступа к LUN, как если бы оно было локально подключенным устройством SCSI. Для получения информации о настройке физического коммутатора и массива для поддержки FCoE см. документацию, предоставленную поставщиком.

> Примечание
>
> Программное обеспечение FCoE может использоваться с Open vSwitch и Linux bridge в качестве серверной сети

4.1.5.6.1. Настройка программного хранилища FCoE

Перед созданием программного хранилища FCoE необходимо убедиться, что к серверу подключены сетевые карты с поддержкой FCoE.

Команда для создания программного хранилища FCoE:

```
xe sr-create type=lvmofcoe name-label=<sr-name> shared=true device-config:SCSIid=<SCSI_id>
```

4.1.5.7. Аппаратные контроллеры шин сервера (Hardware HBA)

Этот подраздел описывает различные операции, требуемые для управления аппаратными контроллерами шин (HBA) SAS, Fibre Channel и iSCSI сервера Numa vServer.

© 2025 Нума Технологии, ООО

4.1.5.7.1. Пример настройки QLogic iSCSI HBA

Полное руководство по конфигурированию HBA для Fibre Channel QLogic и iSCSI см. на официальном веб-сайт QLogic.

Как только HBA физически установлен на сервере Numa vServer, можно использовать следующие шаги для конфигурирования HBA:

1. Настроить сетевую конфигурацию протокола IP для HBA. В этом примере предполагается использовать порт 0 (port 0) для DHCP и HBA. Необходимо определить надлежащие значения для использования статической IP-адресации или многопортового HBA.
2. Добавить постоянную iSCSI-цель для порта 0 HBA.
3. Использовать команду `xe sr-probe` для запуска повторного сканирования контроллера HBA и вывода на экран списка доступных LUN.

4.1.5.7.2. Удаление записей устройств SAS, FC или iSCSI на основе HBA

> **Примечание**
>
> Данный шаг не является обязательным и должен выполняться лишь опытными администраторами при необходимости

Каждый LUN на основе HBA имеет соответствующую глобальную запись пути устройства в разделе `/dev/disk/by-scsibus` в формате `<SCSIid>-<adapter>:<bus>:<target>:<lun>` и стандартный путь к устройству в `/dev`. Для удаления записи о LUN, который больше не планируется использовать в качестве хранилища, выполните следующие действия:

1. Используйте команды `xe sr-forget` или `xe sr-destroy` для хранилищ, которые требуется удалить из базы данных сервера Numa vServer (см. раздел Удаление хранилища).
2. Удалите конфигурацию зонирования в пределах SAN для нужного LUN на сервере.
3. Используйте команду `xe sr-probe` для определения значений ADAPTER, BUS, TARGET и LUN, соответствующих удаляемому LUN.
4. Удалите записи устройства следующей командой:

```
echo "1" > /sys/class/scsi_device/<adapter>:<bus>:<target>:<lun>/device/delete
```

> **Предупреждение**
>
> Убедитесь, что вы уверены какой именно LUN удаляете. Случайное удаление LUN, необходимого для работы сервера, например, загрузочного или корневого устройства, делает сервер непригодным для использования.

4.1.5.8. Общее хранилище типа LVM

Общее хранилище типа LVM представляет диски как логические тома в группе томов, созданной в LUN на основе iSCSI (FC или SAS).

> **Примечание**
>
> Размер блока iSCSI LUN должен составлять 512 байт

© 2025 Нума Технологии, ООО

4.1.5.8.1. Создание общего LVM поверх хранилища iSCSI с использованием программного инициатора iSCSI (lvmoiscsi)

Таблица – Параметры конфигурации устройства для хранилищ lvmoiscsi

Имя параметра	Описание	Обязательность
target	IP-адрес или имя хоста цели iSCSI в SAN, где размещен SR. Это также может быть список значений, разделенных запятыми, для подключения к нескольким целям.	Да
targetIQN	Квалифицированное имя iSCSI (IQN) цели в iSCSI SAN, где размещено хранилище, или `*` для подключения ко всем IQN.	Да
SCSIid	Идентификатор шины SCSI целевого LUN	Да
chapuser	Имя пользователя, которое будет использоваться для аутентификации CHAP	Нет
chappassword	Пароль, который будет использоваться для аутентификации CHAP	Нет
port	Номер сетевого порта, на который посылается запроса к целевому хранилищу	Нет
usediscoverynumber	Определенный индекс записи iSCSI для использования	Нет
incoming_chapuser	Имя пользователя, которое фильтр iSCSI будет использовать для аутентификации на хосте	Нет
incoming_chappassword	Пароль, который фильтр iSCSI будет использовать для аутентификации на хосте	Нет

Для создания общего хранилища типа LVMoiSCSI на определенном LUN iSCSI используйте следующую команду:

```
1  xe sr-create host-uuid=<vhost-uuid> content-type=user name-label=<sr-name> shared=true device-
   config:target=<target_ip=> device-config:targetIQN=<target_iqn> device-config:SCSIid=<scsi_id>
   type=lvmoiscsi
```

4.1.5.8.2. Создание совместно используемого LVM поверх хранилища на базе Fibre Channel/Fibre Channel over Ethernet/iSCSI HBA или SAS (lvmohba)

Хранилища типа LVMoHBA создаются и управляются через интерфейс CLI.

Для создания общего хранилища LVMoHBA выполните следующие шаги на каждом сервере в пуле:

1. Зонируйте один или несколько LUN для каждого сервера в пуле. Детали процесса зависят от используемого оборудования SAN.
2. Используйте команду `xe sr-probe` для определения глобального пути устройства LUN HBA. Команда `xe sr-probe` принудительно осуществляет пересканирование установленных HBA в системе для обнаружения любых новых LUN, призонированных к хосту. Команда возвращает список свойств для каждого найденного LUN. Укажите параметр `host-uuid`, чтобы убедиться, что пересканирование происходит на требуемом хосте.

   Глобальный путь устройства, возвращённый в свойстве <path>, является общим для всех серверов в пуле и поэтому должен использоваться в качестве значения для параметра `device-config:device` при создании хранилища.

© 2025 Нума Технологии, ООО

Если присутствует несколько LUN, используйте имя поставщика, размер LUN, серийный номер LUN или идентификатор SCSI из свойства <path> для однозначной идентификации требуемого LUN:

© 2025 Нума Технологии, ООО

Команда

```
xe sr-probe type=lvmohba host-uuid=<host-uuid>
```

Пример вывода

```
xe sr-probe type=lvmohba host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31

    Error code: SR_BACKEND_FAILURE_90
    Error parameters: , The request is missing the device parameter, \
    <?xml version="1.0" ?>
    <Devlist>
        <BlockDevice>
            <path>
                /dev/disk/by-id/scsi-360a98000686669496734463876653 36f
            </path>
            <vendor>
                HITACHI
            </vendor>
            <serial>
                730157980002
            </serial>
            <size>
                80530636800
            </size>
            <adapter>
                4
            </adapter>
            <channel>
                0
            </channel>
            <id>
                4
            </id>
            <lun>
                2
            </lun>
            <hba>
                qla2xxx
            </hba>
        </BlockDevice>
        <Adapter>
            <host>
                Host4
            </host>
            <name>
                qla2xxx
            </name>
            <manufacturer>
                QLogic HBA Driver
            </manufacturer>
            <id>
                4
            </id>
        </Adapter>
    </Devlist>
```

© 2025 Нума Технологии, ООО

3. На мастере пула создайте хранилище, задав глобальный путь устройства в соответствии с путём, возвращённым в свойстве <path> в качестве результата команды `sr-probe`. PBD будут созданы и включены для каждого хоста в пуле автоматически:

```
xe sr-create host-uuid=<host-uuid> content-type=user name-label=<sr-name> shared=true device-config:SCSIid=<device_scsi_id> type=lvmohba
```

4.1.5.9. NFS и SMB

Общие ресурсы на серверах NFS (которые поддерживают NFSv4 или NFSv3) или на серверах SMB (которые поддерживают SMB 3.0) можно сразу использовать в качестве хранилищ для виртуальных дисков. VDI хранятся только в формате Microsoft VHD. Кроме того, поскольку эти хранилища могут быть общими, VDI, хранящиеся на общих хранилищах, позволяют:

- запускать ВМ на любых серверах в пуле;
- использовать миграцию ВМ между серверами в пуле с использованием динамической миграции (без заметного простоя).

> **Примечание**
>
> 1. Поддержка SMB 3.0 ограничивается возможностью подключения к общему ресурсу по протоколу 3.0. Дополнительные функции, такие как прозрачная отработка отказа, зависят от доступности функций в вышестоящем ядре Linux и не поддерживаются в Numa vServer.
> 2. Для NFSv4 поддерживается только тип аутентификации AUTH_SYS

VDI, хранимые на файловых хранилищах, имеют thin-provisioning (экономичное выделение места хранения). Дисковое пространство для файла образа выделяется по мере того, как ВМ записывает данные на диск. Этот подход имеет значительное преимущество в том, что файлы образов ВМ занимают столько места в хранилище, сколько требуется. Например, если для ВМ выделен VDI объемом 100 ГБ и установлена ОС, файл VDI отражает только размер данных ОС, записанных на диск, а не все 100 ГБ.

Файлы VHD также могут быть объединены в цепочку, что позволяет двум VDI совместно использовать общие данные. В случаях, когда клонируется файловая ВМ клонирована, полученные ВМ совместно используют общие данные на диске во время клонирования. Каждая ВМ продолжает вносить свои собственные изменения в изолированную версию VDI с копированием при записи. Эта функция позволяет быстро клонировать файловые ВМ из шаблонов, обеспечивая очень быструю подготовку и развертывание новых ВМ.

> **Примечание**
>
> Максимальная поддерживаемая длина цепочек VHD — 30.

Реализации файловых хранилищ и VHD в Numa vServer предполагают, что они имеют полный контроль над каталогом хранилища на файловом сервере. Администраторы не должны изменять содержимое каталога хранилища, так как это может привести к повреждению содержимого VDI.

> **Примечание**
>
> Поскольку VDI на файловых хранилищах создаются как thin-provisioning, администраторы должны убедиться, что на файловых хранилищах достаточно дискового пространства для всех необходимых VDI. Серверы Numa vServer не проверяют наличие пространства, необходимого для VDI на файловых хранилищах.
>
> Убедитесь, что вы следите за свободным пространством на вашем хранилище. Если использование хранилища достигнет 100%, дальнейшие записи с ВМ завершаются неудачей. Эти неудачные записи могут привести к зависанию или сбою ВМ.

© 2025 Нума Технологии, ООО

4.1.5.9.1. Настройка общего хранилища NFS

> **Примечание**
>
> Если вы попытаетесь подключить NFS-хранилище только для чтения, то действие завершится ошибкой: «SR_BACKEND_FAILURE_461 — Невозможно выполнить запись в файловую систему для SR».

Чтобы создать NFS-хранилище, необходимо указать имя хоста или IP-адрес сервера NFS. Можно создать хранилище на любом допустимом пути назначения, используя команду `xe sr-probe` для отображения списка допустимых путей назначения, экспортированных сервером.

В тех случаях, когда Numa vServer используется с хранилищем начального уровня, он осторожно ожидает подтверждения всех записей перед передачей подтверждений на ВМ. Этот подход требует заметных затрат производительности и может быть решен путем настройки хранилища для представления точки монтирования хранилища как асинхронного режима экспорта. Асинхронные экспорты подтверждают записи, которых фактически нет на диске.

> **Внимание!**
>
> Сервер NFS должен быть настроен на экспорт указанного пути на всех серверах в пуле. Если эта настройка не выполнена, создание хранилища и подключение PBD завершатся неудачей.

Реализация NFS в Numa vServer по умолчанию использует TCP. Если ситуация позволяет, можно настроить реализацию на использование UDP в сценариях, где может быть выигрыш в производительности. Для этого при создании хранилища необходимо указать параметр `device-config:useUDP=true`.

Например, для создания совместно используемого хранилища NFS на `192.168.1.10:/export1` используйте следующую команду:

```
xe sr-create content-type=user name-label=<sr-name> shared=true device-config:server=192.168.1.10
device-config:serverpath=/export1 type=nfs nfsversion=<"3", "4">
```

Для создания NFS-хранилища без общего доступа выполните следующую команду:

```
xe sr-create host-uuid=<host-uuid> content-type=user name-label=<sr-name> device-
config:server=192.168.1.10 device-config:serverpath=/export1 type=nfs nfsversion=<"3", "4">
```

4.1.5.9.2. Настройка общего хранилища SMB

Чтобы создать общее SMB-хранилище, укажите имя хоста или IP-адрес сервера SMB, полный путь экспортируемого общего ресурса и соответствующие учетные данные.

Например, чтобы создать общее SMB-хранилище с адресом и путем `192.168.1.10:/share1`, используйте следующую команду:

```
xe sr-create content-type=user name-label=<shared-sr-name> shared=true device-config:server=//
192.168.1.10/share1 device-config:username=<valid_username> device-config:password=<valid_password>
type=smb
```

Чтобы создать необщее SMB-хранилище, используйте следующую команду:

© 2025 Нума Технологии, ООО

```
xe sr-create host-uuid=host_uuid content-type=user name-label=<non-shared-sr-name> device-config:server=//192.168.1.10/share1 device-config:username=<valid_username> device-config:password=<valid_password> type=smb
```

4.1.5.10. LVM поверх аппаратных HBA

Хранилище типа LVM поверх аппаратных HBA представляет диски как VHD на логических томах в группе томов, созданной на HBA LUN, который обеспечивает, например, аппаратную поддержку iSCSI или FC.

Серверы Numa vServer поддерживают SAN (storage area networks) Fibre Channel (FC) через адаптеры HBA от Emulex или QLogic. Все настройки FC, необходимые для предоставления LUN FC серверу, должны быть выполнены вручную, включая устройства хранения, сетевые устройства и адаптеры HBA на сервере. Как только вся конфигурация FC будет настроена, HBA представит серверу SCSI-устройство, работающее «поверх» FC LUN. Затем устройство SCSI можно будет использовать для получения доступа к LUN FC, как если бы это было локально подключенное устройство SCSI.

Для вывода списка поддерживаемых в настоящий момент на сервере SCSI-устройств с поддержкой LUN используйте команду `xe sr-probe`. Эта команда принудительно запускает сканирование на наличие новых SCSI-устройств с споддержкой LUN. Значение пути, возвращаемое `xe sr-probe` для SCSI-устройств с поддержкой LUN, согласовано на всех серверах с доступом к LUN. Поэтому это значение должно использоваться при создании общих хранилищ, доступных всем серверам в пуле.

Те же функции применимы к iSCSI HBA от QLogic.

См. раздел Создание хранилищ для получения дополнительной информации о создании общих хранилищ.

> **Внимание**
>
> Numa vServer для Fibre Channel не поддерживает прямое сопоставление LUN с ВМ. LUN на основе HBA должны быть сопоставлены с сервером и указаны для использования в хранилище. VDI в хранилище предоставляются ВМ как стандартные блочные устройства.
>
> Размер блока LVM по HBA LUN должен быть 512 байт. Для использования хранилища с физическими блоками 4 КБ хранилище также должно поддерживать эмуляцию блоков распределения по 512 байт (логический размер блока должен быть 512 байт).

4.1.6. Создание и настройка хранилищ данных

В этом разделе описываются процессы создания хранилищ различных типов и предоставления доступа к ним серверам Numa vServer. Также описываются различные операции, необходимые для управления хранилищами, включая живую миграцию VDI.

4.1.6.1. Создание хранилищ

В этом разделе объясняется, как создать хранилища разных типов и сделать их доступными для сервера Numa vServer. Приведенные примеры охватывают создание хранилищ с помощью команд xe в CLI.

Создание нового хранилища данных для использования в Numa vServer включает два основных шага, выполняемых с помощью CLI:

1. Проверьте тип хранилища, чтобы определить значения всех требуемых параметров.
2. Создайте хранилище. Для инициализации объектов хранилища и связанных с ними объектов PBD включите PBD и активируйте хранилище.

Эти шаги отличаются в зависимости от типа создаваемого хранилища. В случае успеха команда `xe sr-create` возвращает UUID созданного хранилища.

© 2025 Нума Технологии, ООО

Хранилище можно уничтожить, если они больше не используются, чтобы освободить физическое устройство. Хранилище также могут быть деактивированы для отсоединения хранилища от одного сервера Numa vServer и присоединения к другому (см.раздел Удаление хранилища).

4.1.6.2. Сканирование хранилища

Команду `xe sr-probe` можно использовать следующими способами:

- для определения неизвестных параметров для использования при создании хранилища;
- чтобы вернуть список существующих хранилищ.

В обоих случаях `xe sr-probe` работает путём определения типа хранилища и одного или нескольких параметров `device-config` для этого типа хранилищ. Если предоставлен неполный набор параметров, `xe sr-probe` сообщает об ошибке, указывающее на отсутствие параметров и возможные варианты для отсутствующих параметров. Когда предоставлен полный набор параметров, команда возвращает список существующих хранилищ. Весь вывод `xe sr-probe` возвращается в виде XML.

Например, известный iSCSI-цель может быть проверен путем указания его имени или IP-адреса. В результате сканирования будет возвращён набор IQN, доступных на цели:

Команда

```
xe sr-probe type=lvmoiscsi device-config:target=<target-ip>
```

Пример вывода

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10

    Error code: SR_BACKEND_FAILURE_96
    Error parameters: , The request is missing or has an incorrect target IQN parameter, \
    <?xml version="1.0" ?>
    <iscsi-target-iqns>
        <TGT>
            <Index>
                0
            </Index>
            <IPAddress>
                192.168.1.10
            </IPAddress>
            <TargetIQN>
                iqn.192.168.1.10:filer1
            </TargetIQN>
        </TGT>
    </iscsi-target-iqns>
```

© 2025 Нума Технологии, ООО

При повторном сканировании той же цели и указание как имени/IP-адреса, так и требуемого IQN будет возвращён набор SCSIid (LUN), доступных на target/IQN.

Команда

```
xe sr-probe type=lvmoiscsi device-config:target=<target-ip> device-config:targetIQN=iqn.<target-ip>:filer1
```

Пример вывода

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 device-config:targetIQN=iqn.192.168.1.10:filer1
    Error code: SR_BACKEND_FAILURE_107
    Error parameters: , The SCSIid parameter is missing or incorrect, \
    <?xml version="1.0" ?>
    <iscsi-target>
        <LUN>
            <vendor>
                IET
            </vendor>
            <LUNid>
                0
            </LUNid>
            <size>
                42949672960
            </size>
            <SCSIid>
                14945540000000000000000002000000b70200000f000000
            </SCSIid>
        </LUN>
    </iscsi-target>
```

© 2025 Нума Технологии, ООО

Повторное сканирование одной и той же цели с предоставлением всех трёх параметров возвращает список хранилищ, существующих на LUN (если таковые имеются).

Команда

```
xe sr-probe type=lvmoiscsi device-config:target=<target-ip>  \
    device-config:targetIQN=<target-ip>:filer1 \
    device-config:SCSIid=<SCSIid>
```

Пример вывода

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10  \
    device-config:targetIQN=192.168.1.10:filer1 \
    device-config:SCSIid=149455400000000000000000002000000b70200000f000000

    <?xml version="1.0" ?>
    <SRlist>
        <SR>
            <UUID>
                3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
            </UUID>
            <Devlist>
                /dev/disk/by-id/scsi-149455400000000000000000002000000b70200000f000000
            </Devlist>
        </SR>
    </SRlist>
```

Таблица ниже содержит параметры для каждого типа хранилищ с указанием, какие из параметров сканируются.

Таблица – Параметры хранилищ

Тип хранилища	Параметр конфигурации устройства, в порядке зависимости	Может ли быть сканирован	Требуется ли для sr-create
lvmoiscsi	target	Нет	Да
	Chapuser	Нет	Нет
	chappassword	Нет	Нет
	targetIQN	Да	Да
	SCSIid	Да	Да
lvmohba	SCSIid	Да	Да
NetApp	Target	Нет	Да
	Username	Нет	Да
	Password	Нет	Да
	Chapuser	Нет	Нет
	chappassword	Нет	Нет
	Aggregate	Нет*	Да
	FlexVols	Нет	Нет
	Allocation	Нет	Нет
	Asis	Нет	Нет

© 2025 Нума Технологии, ООО

Тип хранилища	Параметр конфигурации устройства, в порядке зависимости	Может ли быть сканирован	Требуется ли для sr-create
nfs	Server	Нет	Да
	serverpath	Да	Да
lvm	Device	Нет	Да
ext	Device	Нет	Да
EqualLogic	target	Нет	Да
	username	Нет	Да
	password	Нет	Да
	chapuser	Нет	Нет
	chappassword	Нет	Нет
	storagepool	Нет**	Да

> Примечание
>
> * – сканирование Aggregate возможно только во время выполнения `xe sr-create`. Должно быть сделано так, чтобы aggregate мог быть определен в точке, в которой было создано хранилище.
> ** – сканирование пула хранилища возможно только во время `xe sr-create`. Должно быть сделано так, чтобы пула мог быть определен в точке, в которой было создано хранилище.

4.1.6.3. Удаление хранилища

Хранилище может быть удален временно или навсегда. Существуют следующие способы:

- отсоединить: разрывает связь между хранилищем и пулом или сервером (отключение PBD). Хранилище (и его VDI) становятся недоступными. Содержимое VDI и метаинформация, используемая виртуальными машинами для доступа к VDI, сохраняются. Отсоединение можно использовать, когда необходимо временно отключить хранилище, например, для обслуживания. Отсоединенное хранилище можно позже снова присоединить.
- забыть: сохраняет содержимое хранилища на физическом диске, но информация, которая подключает виртуальную машину к ее VDI, навсегда удаляется. Например, позволяет повторно подключить хранилище к другому серверу Numa vServer, не удаляя его содержимое.
- уничтожить: полностью удаляет содержимое хранилища с физического диска.

Для того что бы уничтожить или забыть PBD, подключенный к хранилищу, он должен быть отключен от сервера.

1. Отключите PBD, чтобы отсоединить хранилище от соответствующего сервера Numa vServer:

```
xe pbd-unplug uuid=<pbd_uuid>
```

2. Используйте команду `xe sr-destroy`, чтобы удалить хранилище. Данная команда уничтожает и удаляет хранилище и соответствующий PBD из базы данных сервера Numa vServer и удаляет содержимое хранилища с физического диска:

```
xe sr-destroy uuid=<sr_uuid>
```

3. Используйте команду `xe sr-forget`, чтобы забыть хранилище. Данная команда удаляет хранилище и соответствующий PBD из базы данных сервера Numa vServer, но оставляет фактическое содержимое хранилища нетронутым на физическом носителе:

```
xe sr-forget uuid=<sr_uuid>
```

© 2025 Нума Технологии, ООО

> **Примечание**
>
> Удаление программного объекта, соответствующего хранилищу, может занять некоторое время, пока «сборщик мусора» не удалит его.

4.1.6.4. Повторный ввод хранилища в работу

Чтобы повторно ввести в работу ранее забытое хранилище, создайте PBD и вручную подключить PBD к соответствующим серверам Numa vServer для активации хранилища.

Следующий пример описывает порядок действий для повторного ввода в работу хранилища типа lvmoiscsi:

1. Просканируйте (probe) существующее хранилище для определения его UUID:

```
xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 device-
config:targetIQN=192.168.1.10:filer1 device-
config:SCSIid=149455400000000000000000002000000b70200000f000000
```

2. Выполните команду `xe sr-introduce` для хранилища, UUID которого был выведен на предыдущем шаге командой `xe sr-probe`. Команда возвращает UUID нового хранилища:

```
xe sr-introduce content-type=user name-label=<Example Shared LVM over iSCSI SR> shared=true
uuid=<valid_sr_uuid> type=lvmoiscsi
```

3. Создайте для данного хранилища новый PBD. Команда возвращает UUID нового PBD:

```
xe pbd-create type=lvmoiscsi host-uuid=<valid_uuid> sr-uuid=<valid_sr_uuid> device-
config:target=<192.168.0.1> device-config:targetIQN=<192.168.1.10:filer1> device-
config:SCSIid=<149455400000000000000000002000000b70200000f000000>
```

4. Подключите PBD для присоединения к хранилищу:

```
xe pbd-plug uuid=<pbd_uuid>
```

5. Проверьте статус подключения PBD. Если подключение успешно, то свойство `currently-attached` будет равно `true` («истина»):

```
xe pbd-list sr-uuid=<sr_uuid>
```

> **Примечание**
>
> Шаги 3–5 должны быть выполнены для каждого сервера в пуле

4.1.6.5. Расширение LUN

Чтобы увеличить размер LUN, выделенного для сервера Numa vServer:

1. Увеличьте размер LUN в хранилище.
2. На Numa vServer выполните команду:

© 2025 Нума Технологии, ООО

```
xe sr-scan sr-uuid=<sr_uuid>
```

Эта команда повторно сканирует SR, что позволяет дополнить его ёмкость.

> **Предупреждение**
>
> Уменьшение размера LUN в массиве хранения может привести к потере данных

4.1.6.6. Живая миграция VDI

Живая миграция (англ. live migration) VDI позволяет администратору перемещать VDI ВМ без выключения ВМ. Эта функция позволяет выполнять такие административные операции как:

- перемещение ВМ из низкоскоростного локального хранилища в более быстрое, отказоустойчивое хранилище, основанное на массиве (array-backed);
- перемещение ВМ из среды разработки в производственную среду;
- перемещение между уровнями системы хранения (storage tiers), когда ВМ ограничена объёмом хранилища;
- выполнение обновлений массива хранения.

4.1.6.6.1. Ограничения и предостережения

На живую миграцию VDI распространяются следующие ограничения и предостережения:

- на целевом хранилище должно быть доступно достаточное дисковое пространство;
- образы VDI, имеющие более одного снимка, не могут быть перемещены.

4.1.6.7. «Холодная» миграция образов VDI между хранилищами (offline-миграция)

VDI, связанные с ВМ, могут быть скопированы с одного SR на другой для соответствия требованиям обслуживания или многоуровневой конфигурации хранилища.

4.1.6.7.1. Копирование отдельных образов виртуальных дисков на выбранное хранилище

Для копирования отдельных VDI между хранилищами можно использовать команды xe в CLI:

1. Выключите ВМ.
2. Используйте соответствующую команду CLI для идентификации UUID VDI, которые нужно переместить. Если ВМ имеет DVD-привод, то его параметр `vdi-uuid` будет выведен как `<not in database>` и может быть проигнорирован:

```
xe vbd-list vm-uuid=<valid_vm_uuid>
```

> **Внимание!**
>
> Команда `xe vbd-list` выводит на экран идентификаторы UUID VBD и VDI. Обязательно запишите VDI UUID, а не VBD UUID

© 2025 Нума Технологии, ООО

3. Для каждого требуемого VDI выполнить команду `xe vbd-destroy`.

```
xe vbd-destroy uuid=<vbd_uuid>
```

> **Предупреждение**
>
> При использовании команды `xe vbd-destroy` для отсоединения VDI, заданных идентификаторами UUID, обязательно нужно убедиться, что параметр VBD `other-config:owner` установлен в значение true. Если это так, следует установить его в значение false, поскольку команда `xe vbd-destroy` с параметром `other-config:owner=true` уничтожит также связанный с VBD образ VDI.

4. Скопируйте каждый из образов VDI ВМ командой `xe vdi-copy` для перемещения их в требуемое хранилище:

```
xe vdi-copy uuid=<valid_vdi_uuid> sr-uuid=<valid_sr_uuid>
```

5. Используйте команду `xe vbd-create`, указав для параметра `uuid` значения UUID VDI из нового хранилища.
6. Удалите исходные VDI:

```
vdi-destroy uuid=<vdi_uuid>
```

4.1.6.8. Преобразование локальных хранилищ на основе Fibre Channel в общее хранилище

Для подобного преобразования следует выполните следующие действия:

1. Убедитесь, что все серверы в пуле имеют LUN хранилища (см. раздел Сканирование хранилища для получения подробностей по использованию команды `xe sr-probe` для проверки наличия LUN на каждом сервере).
2. Преобразуйте хранилище в общее:

```
xe sr-param-set shared=true uuid=<local_fc_sr_uuid>
```

4.1.6.9. Автоматическое освбождение места в пространстве при удалении снимков состояния

При удалении снимков состояния с Numa vServer пространство, выделенное на хранилище на основе LVM, автоматически освобождается, и перезагрузка ВМ не требуется. Эта функция известна как онлайн-слияние (Online Coalesce).

> **Примечание**
>
> Функция онлайн-слияния применима только к хранилищам на основе LVM (LVM, LVMoISCSI и LVMoHBA) и не применима к хранилищам EXT или NFS, поведение которых остаётся неизменным

В некоторых случаях автоматическое восстановление пространства может не работать. Мы рекомендуем использовать офлайн-слияние в следующих сценариях:

- в условиях, когда пропускная способность ввода-вывода ВМ значительна;

© 2025 Нума Технологии, ООО

• в условиях, когда пространство не восстанавливается даже по истечении определенного промежутка времени после удаления снимка.

> **Примечание**
>
> Запуск офлайн-слияния ведёт к некоторому простою ВМ из-за выполнения операций приостановки и возобновления.
>
> Перед запуском инструмента удалите все ненужные снимки и клоны ВМ. Инструмент восстанавливает столько места, сколько возможно, учитывая оставшиеся снимки и клоны. Если необходимо восстановить всё пространство, удалите все снимки и клоны.
>
> Все диски ВМ должны располагаться в общем или локальном хранилище для одного сервера. ВМ с дисками в обоих типах хранилища не могут быть объединены.

4.1.6.9.1. Освобождение места в пространстве при помощи офлайн-слияния

> **Примечание**
>
> Функция офлайн-слияния применима только к хранилищам, основанным на LVM (LVM, LVMoISCSI и LVMoHBA) и не применима к хранилищам на основе EXT или NFS, поведение которых остается неизменным

1. Откройте консоль на сервере и выполните следующую команду:

Команда

```
xe host-call-plugin host-uuid=<host-uuid> plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=<VM-uuid>
```

Пример ввода

Например, если UUID ВМ – «9bad4022-2c2d-dee6-abf5-1b6195b1dad5», а идентификатор UUID сервера – «b8722062-de95-4d95-9baa-a5fe343898ea», выполните следующую команду:

```
xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2c2d-dee6-abf5-1b6195b1dad5
```

2. Данная команда приостанавливает ВМ (если она ещё не выключена), инициирует процесс освобождения пространства и затем возобновляет работу ВМ.

© 2025 Нума Технологии, ООО

> **Примечание**
>
> Перед запуском офлайн-слияния рекомендуем завершить или приостановить работу ВМ вручную посредством CLI. Если вы запустите процесс слияния на работающей ВМ, то данный процесс автоматически приостановит работу ВМ, выполнит требуемые операции слияния VDI и возобновит работу ВМ.
>
> Если объединяемые VDI находятся на общем хранилище, необходимо запустить офлайн-слияния на сервере, являющимся мастером пула.
>
> Если объединяемые VDI находятся на локальном хранилище, запустить офлайн-слияния на сервере, к которому подключено локальное хранилище.

4.1.6.10. Настройка планировщика ввода-вывода на диске

Вы можете настроить планировщик дискового ввода-вывода и параметры приоритета дискового ввода-вывода, чтобы изменить производительность ваших дисков.

> **Примечание**
>
> Возможности дискового ввода-вывода, описанные в данном разделе, не применимы к хранилищам EqualLogic, NetApp или NFS

Для общей производительности планировщик дискового ввода-вывода (англ. Disk IO Scheduler, по умолчанию используется планировщик Noop) применяется на всех новых типах хранилищ. Планировщик ввода-вывода Noop обеспечивает наиболее справедливую производительность для ВМ, конкурирующих за доступ к одному устройству.

1. Настройте планировщик диска с помощью команды:

```
xe sr-param-set other-config:scheduler=<noop|cfq|anticipatory|deadline> uuid=<sr_uuid>
```

2. Отключите и снова подключите соответствующий PBD, чтобы параметр планировщика вступил в силу.

```
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
```

При использовании механизма QoS для диска (см. раздел Настройки QoS для виртуальных дисков) необходимо переопределить настройку по умолчанию и присвоить параметру `other-config:scheduler` (выбор планировщика для хранилища) значение `cfq`.

4.1.6.11. Настройки QoS для виртуальных дисков

Виртуальные диски имеют настройки приоритета запросов ввода-вывода (QoS) (необязательная опция). В данном разделе описано, как применить эти настройки к существующим виртуальным дискам.

Перед настройкой любых параметров QoS для VBD следует обеспечить хранилище соответствующим дисковым планировщиком (см. раздел Настройка планировщика ввода вывода на диске). Для хранилищ, которым требуется поддержка QoS, параметр планировщика должен быть установлен в значение `cfq`.

© 2025 Нума Технологии, ООО

> **Внимание**
>
> После установки для требуемого хранилища параметра планировщика в значение `cfq` убедитесь, что PBD было переподключено, чтобы изменения для планировщика вступили в силу

Для общего хранилища, где несколько серверов обращаются к одному и тому же LUN, настройка QoS применяется к VBD, обращающимся к LUN с одного и того же сервера. Эти настройки не применяются к серверам в пуле.

4.1.6.11.1. Настройка параметров запроса дискового ввода-вывода

Эти настройки можно применить к существующим виртуальным диска с помощью команды `xe vbd-param-set` со следующими параметрами:

- `qos_algorithm_type` – этот параметр должен быть установлен в значение `ionice` (единственный тип алгоритма QoS, поддерживаемый для виртуальных дисков в данной версии Numa vServer).
- `qos_algorithm_param` – используйте этот параметр для установки пар ключ-значение. Для виртуальных дисков параметр `qos_algorithm_param` использует ключ `sched` (тип плана QoS) и, в зависимости от значения, также требует ключ `class`.

Возможные значения параметра `qos_algorithm_param:sched`:

- `sched=rt` или `sched=real-time` – устанавливает приоритет параметра планирования в реальном времени, что требует установки значения параметра `class`;
- `sched=idle` – соответствует режиму бездействия планировщика QoS (idle priority), не требующему установки значения какого-либо параметра `class`;
- `sched=anything` – соответствует приоритету планирования по принципу «лучшей попытки» (best effort), требующему установки значения параметра `class`.

Возможные значения для параметра `qos_algorithm_param:class`:

- одно из следующих ключевых слов: `highest`, `high`, `normal`, `low`, `lowest`;
- целое число между 0 и 7, где `7` соответствует самому высокому приоритету, а `0` – самому низкому. Например, запрос ввод-вывода с приоритетом `5` будет обработан раньше запроса с приоритетом `2`.

Например, следующие команды устанавливают виртуальное блочное устройство виртуального диска для использования приоритета `5` (реального времени):

```
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_type=ionice
```

```
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:sched=rt
```

```
xe vbd-param-set uuid=<vbd_uuid> qos_algorithm_params:class=5
```

```
xe sr-param-set uuid=<sr_uuid> other-config:scheduler=cfq
```

```
xe pbd-unplug uuid=<pbd_uuid>
```

```
xe pbd-plug uuid=<pbd_uuid>
```

© 2025 Нума Технологии, ООО

4.1.6.12. Многоканальные соединения в системе хранения (multipathing)

Поддержка динамической многоканальности (multipathing) доступна для хранилищ на основе Fibre Channel и iSCSI.

Настройка multipathing обеспечивает избыточность для трафика удаленного хранилища в случае частичной потери подключения. Многопутевой режим направляет трафик хранилища на устройство хранения по нескольким путям для избыточности и повышения пропускной способности. Вы можете использовать до 16 путей к одному LUN. Многопутевой режим представляет собой конфигурацию «активный-активный».

По умолчанию multipathing использует либо циклическую балансировку нагрузки (round-robin). Во время нормальной работы на всех маршрутах есть активный трафик, что приводит к повышению пропускной способности.

Многоканальное соединение можно включить через CLI. Перед включением убедитесь, что следующие утверждения верны:

- Убедитесь, что на сервере хранения действительно доступно несколько целей.

Например, серверная часть хранилища iSCSI запрашивает `sendtargets` на данном портале должен возвратить более одной цели, как в примере ниже:

```
iscsiadm -m discovery --type sendtargets --portal 192.168.0.161

192.168.0.161:3260,1 iqn.strawberry:litchie
192.168.0.204:3260,2 iqn.strawberry:litchi
```

- Только для iSCSI домен управления (dom0) имеет IP-адрес в каждой подсети, используемой многопутевым хранилищем.

Убедитесь, что для каждого пути к хранилищу есть сетевая карта, а для каждой сетевой карты настроен IP-адрес. Например, если вам нужны четыре пути к хранилищу, у вас должно быть четыре сетевых адаптера, на каждом из которых настроен IP-адрес.

4.1.6.12.1. Включение multipathing

Для включения многоканального соединения для системы хранения выполните следующие шаги:

1. Отключите все PBD на сервере:

```
xe pbd-unplug uuid=<pbd_uuid>
```

где `pbd_uuid` можно найти с помощью команды `xe pbd-list`

2. Установите для параметра `other-config:multipathing` значение `true`:

```
xe host-param-set other-config:multipathing=true uuid=<host_uuid>
```

3. Установите для параметра `other-config:multipathhandle` значение `dmp`:

```
xe host-param-set other-config:multipathhandle=dmp uuid=<host_uuid>
```

4. Если существующие на сервере хранилища работают в одноканальном режиме, но имеют возможность многоканального использования:
   - перенесите или приостановите любые работающие ВМ с виртуальными дисками в затронутых хранилищах;
   - отключите и повторно включите все влияющие на хранилища PBD, чтобы повторно подключить их, используя многоканальное соединение:

```
xe pbd-unplug uuid=<pbd_uuid>
xe pbd-plug uuid=<pbd_uuid>
```

© 2025 Нума Технологии, ООО

4.1.6.12.2. Отключение multipathing

Для отключения многоканального соединения:

1. Отключите VBD, установив на хосте параметр `other-config:multipathing` в значение `false`.
2. Затем повторно включите физические блочные устройства, как это описано выше. Параметр `other-config:multipathing` изменять не следует, поскольку это будет сделано автоматически.

Поддержка многоканальности в Numa vServer основывается на наборе компонентов `multipathd components` модуля ядра Linux, называемого `device-mapper`. Активация и деактивация многоканальных подключенных узлов осуществляется автоматически Storage Manager API. В отличие от стандартных инструментов `dm-multipathd tools` в Linux, узлы `device-mapper` не создаются для всех LUN в системе автоматически: новые узлы вводятся в действие лишь в случаях, когда LUN активно используются уровнем управления системы хранения. В связи с этим нет нужды использовать какой-либо инструмент `dm-multipath` командной строки для запроса или обновления табличных узлов `device-mapper` на сервере Numa vServer. Если необходимо запросить состояние таблиц `device-mapper` вручную или вывести список активных многоканальных узлов `device-mapper` в системе, следует использовать утилиту `mpathutil`:

- `mpathutil status` - запрос статуса;
- `mpathutil list` - вывод списка.

> **Предупреждение**
>
> Из-за несовместимостей с интегрированной архитектурой управления многоканальности, стандартная утилита командной строки `dm-multipath` не должна использоваться с Numa vServer. Следует использовать инструмент командной строки `mpathutil` для того, чтобы запросить состояние узлов на сервере

Поддержка многоканальности в массивах EqualLogic не охватывает многоканальность ввода-вывода системы хранения (Storage IO multipathing) в традиционном смысле этого термина. Управление многоканальными соединениями должно происходить на уровне сетей/агрегаций сетевых интерфейсов. Обратитесь к документации EqualLogic для получения информации о настройках механизмов обеспечения отказоустойчивости сети для хранилищ на основе EqualLogic или LVMoISCSI.

© 2025 Нума Технологии, ООО

5. Администрирование пользователей

В Numa vServer реализовано управление доступом на основе ролей для контроля доступа к серверным узлам и ресурсным пулам Numa vServer и контроля действий пользователей.

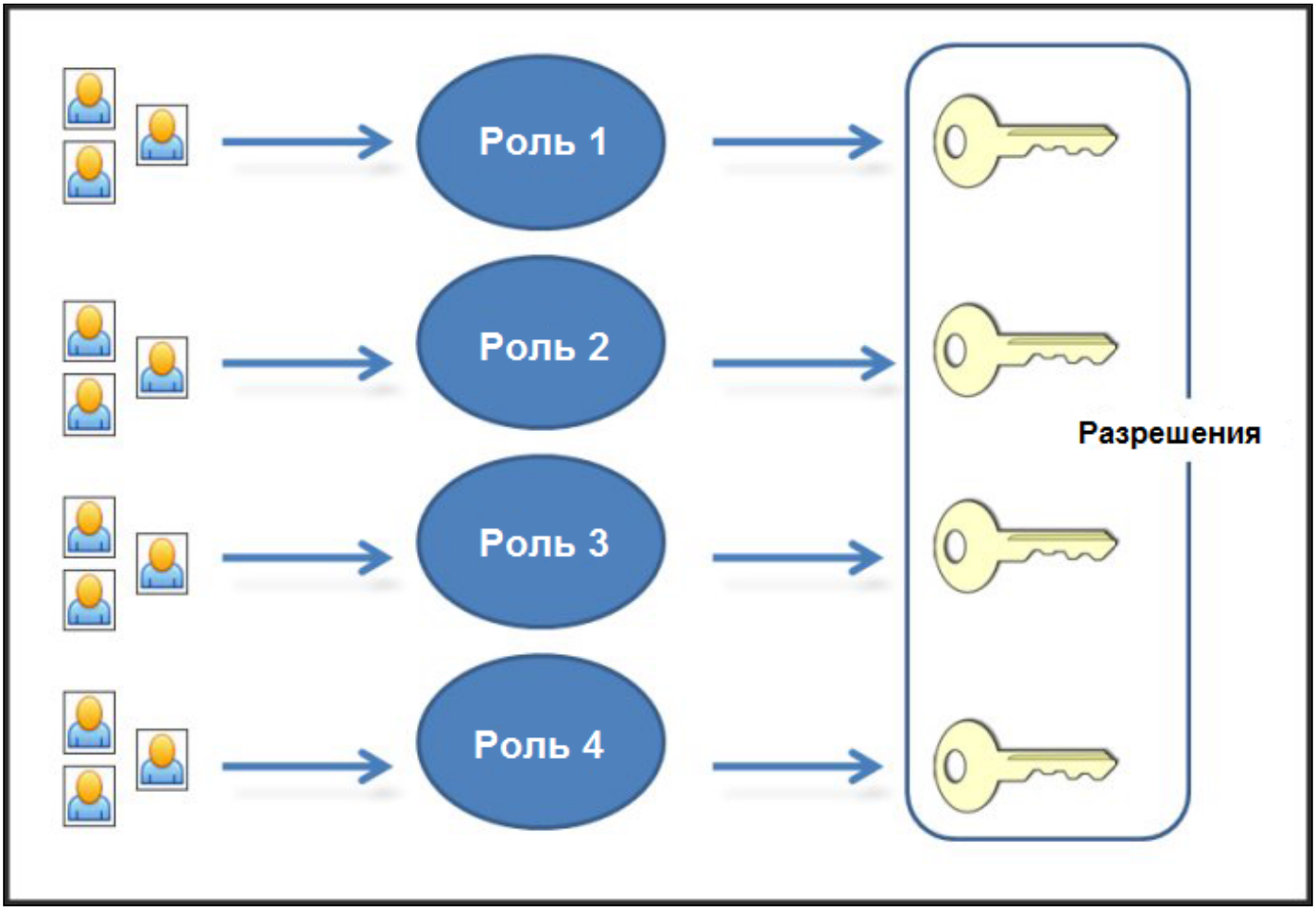
5.1. Локальный суперпользователь

По умолчанию в Numa vServer предустановлен один пользователь root с ролью локального суперпользователя (Local Super User, LSU).

Локальный суперпользователь (LSU) или root – это особая учетная запись пользователя, обладающая всеми правами и полномочиями для администрирования Numa vServer. Аутентификация с этой учётной записью проверяется только средствами Numa vServer, а не внешней службы аутентификации, поэтому локальный суперпользователь сможет войти и управлять системой даже при сбое соединения с сервером службы аутентификации. Локальный суперпользователь всегда может получить доступ к серверному узлу Numa vServer локально или по SSH (при условии, что доступ по SSH не отключен).

5.2. Управление доступом на основе ролей

Подсистема управления доступом на основе ролей (Role Based Access Control, RBAC) позволяет назначить пользователям роли и полномочия для управления доступом к Numa vServer. Также RBAC предоставляет функцию журнала аудита.



RBAC зависит от внешних служб аутентификации, таких как:

© 2025 Нума Технологии, ООО

- Active Directory, FreeIPA. Для работы с данными службами необходимо присоединить ресурсный пул или серверный узел Numa vServer к домену и добавить учетные записи, прежде чем администратор сможет непосредственно назначать роли.
- Модуль PAM. Данный тип службы создает локальных пользователей и назначает им роли доступа.

> **Примечание**
>
> При создании новых пользователей Numa vServer не назначает автоматически созданным учетным записям роли согласно RBAC. Таким образом, эти учетные записи не будут иметь доступа к пулу до тех пор, пока им не будет назначена соответствующая роль.

5.2.1. Пользовательские роли

Numa vServer поддерживает шесть ролей пользователей:

- Администратор пула (Pool Admin) – пользователь с полными правами доступа, как у локального суперпользователя.
- Оператор пула (Pool Operator) – пользователю доступны все операции, кроме добавления/удаления пользователей и изменения их ролей. Данная роль предназначена, в основном, для управления серверными узлами и пулом (создание хранилищ, настройка пулов, управление сетями и т. д.).
- Администратор виртуальных машин с расширенными полномочиями (VM Power Admin) – пользователю доступны создание и управление виртуальными машинами. Эта роль ориентирована на создание и обслуживание виртуальных машин, которые используются администраторами и операторами ВМ.
- Администратор виртуальных машин (VM Admin) – роль, схожая с предыдущей, но не позволяющая производить миграцию виртуальных машин или создавать снимки состояния ВМ.
- Оператор виртуальных машин (VM Operator) – по аналогии с ролью администратора ВМ, но не имеет полномочий на создание/удаление ВМ, однако позволяет запускать/останавливать операции жизненного цикла ВМ.
- Только для чтения (Read Only) – роль, позволяющая просматривать пул и данные о производительности.

Всем пользователям Numa vServer должны быть назначены соответствующие им роли. Пользователю может быть назначено множество ролей. В этом случае пользователь будет иметь объединение всех их разрешений.

> **Примечание**
>
> В данной версии Numa vServer отсутствует возможность добавления или удаления ролей.

> **Предупреждение**
>
> Нельзя назначить роль Pool Admin группе служб аутентификации, содержащей более 500 членов, если предполагается, что в дальнейшем эти пользователи будут иметь доступ по SSH.

Для знакомства с полномочиями, доступными для каждой роли, и получения более подробной информации об операциях, доступных для каждого разрешения (см. раздел Описание ролей и разрешений RBAC).

5.2.2. Описание ролей и разрешений RBAC

Таблица ниже суммирует полномочия доступные для каждой роли. Более подробные сведения представлены в таблице Дополнительные сведения о полномочиях ролей.

Таблица – Полномочия для базовых ролей

© 2025 Нума Технологии, ООО

Полномочие	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator
Назначение и изменение ролей пользователей	X				
Резервное копирование/ восстановление сервера	X				
Импорт/экспорт OVF-/OVA-контейнеров и образов дисков ВМ	X				
Установка количества ядер на сокет	X	X	X	X	
Преобразование виртуальных машин с помощью диспетчера преобразований	X				
Блокировка портов коммутатора	X	X			
Настройка multipathing	X	X			
Отключение активных пользователей от управления (завершение сеанса работы)	X	X			
Создание и снятие оповещений для пользователей	X	X			
Отмена заданий любого пользователя	X	X			
Управление пулом	X	X			
Живая миграция	X	X	X		
Хранилище для живой миграции	X	X	X		
Расширенные операции по управлению ВМ	X	X	X		
Создание и удаление ВМ	X	X	X	X	
Изменение подключенных CD образов в ВМ	X	X	X	X	X
Изменение состояния питания ВМ	X	X	X	X	X
Доступа к консоли ВМ	X	X	X	X	X
Отмена собственных задач	X	X	X	X	X
Чтение журнала аудита	X	X	X	X	X
Подключение к пулу и чтение метаданных пула	X	X	X	X	X
Настройка vGPU	X	X			
Просмотр конфигурации vGPU	X	X	X	X	X
Доступ к конфигурационному диску (только для ВМ CoreOS)	X				
Управление контейнером	X				
Запланированные моментальные снимки	X	X	X		
Запланированные снимки	X	X			
	X	X			

© 2025 Нума Технологии, ООО

Полномочие	Pool Admin	Pool Operator	VM Power Admin	VM Admin	VM Operator
Настройка проверки работоспособности					
Просмотр результатов и настроек проверки работоспособности	X	X	X	X	X
Настройка отслеживания измененных блоков	X	X	X	X	
Просмотр списка измененных блоков	X	X	X	X	X

Пользователю с ролью read-only доступны следующие полномочия:

- Отмена собственных задач
- Чтение журнала аудита
- Подключение к пулу и чтение метаданных пула
- Просмотр конфигурации vGPU
- Просмотр результатов и настроек проверки работоспособности

Таблица – Дополнительные сведения о полномочиях ролей

Полномочие	Детали	Примечание
Назначение и изменение ролей пользователей	добавить/удалить пользователей назначить/удалить роль включение и отключение интеграции с AD (присоединение к домену)	Предупреждение. Эта роль позволяет пользователю отключить интеграцию с Active Directory
Доступ к серверной консоли через SSH	доступ с локальной консоли сервера или через SSH	При локальном администрировании администратор может произвольно изменить конфигурацию всей системы, в том числе назначения ролей
Резервное копирование/ восстановление сервера	резервное копирование и восстановление серверов резервное копирование и восстановление метаданных пула	Возможность восстановления резервной копии позволяет восстановить изменения конфигурации ролей
Импорт/экспорт OVF-/OVA-контейнеров и образов дисков ВМ	импорт OVF- и OVA-контейнеров импорт образов дисков экспорт виртуальных машин как OVF-/OVA-контейнеров	
Установка количества ядер на сокет	установка количества ядер на сокет для виртуальных процессоров ВМ	Это разрешение позволяет пользователю указать топологию для виртуальных процессоров ВМ
Преобразование виртуальных машин с помощью диспетчера преобразований	преобразование виртуальных машин VMware в виртуальные машины Numa vServer	Это разрешение позволяет пользователю преобразовывать ВМ из VMware в Numa vServer путем копирования образов виртуальных машин VMware в среду Numa vServer
Блокировка портов коммутатора	контроль трафика в сети	Это разрешение позволяет пользователю по умолчанию блокировать весь трафик в сети или определять конкретные IP-адреса, с которых виртуальной машине разрешено отправлять трафик
Настройка multipathing	включение/отключение multipathing	
	возможность отключения вошедших в систему пользователей	

© 2025 Нума Технологии, ООО

Полномочие	Детали	Примечание
Отключение активных пользователей от управления (завершение сеанса работы)		
Создание и снятие оповещений для пользователей	конфигурация предупреждений, когда использование ресурсов пересекает определенные пороги удаление оповещений	Предупреждение. Пользователь с этим разрешением может отклонить оповещения для всего пула Примечание. Возможность просмотра предупреждений является частью подключения к пулу и чтения всех метаданных пула
Отмена заданий любого пользователя	отмена любого запущенного задания пользователя	Это разрешение позволяет пользователю запрашивать у Numa vServer отмену выполняемой задачи, инициированной любым пользователем
Управление пулом	установить свойства пула (название, SR по умолчанию) включить, отключить и настроить механизм HA установить приоритеты перезапуска механизма HA для каждой ВМ конфигурация DR и выполнение DR failover, failback и test failover включить, отключить и настроить балансировку рабочей нагрузки (WLB) добавить и удалить сервер из пула аварийная смена мастера аварийная смена адреса мастера аварийное восстановление подчинённых хостов назначить нового мастера управление пулами настройка свойств сервера настройка ведения журнала на сервере включение и отключение серверов завершение работы, перезагрузка и включение серверов перезапуск набора инструментов отчеты о состоянии системы динамическая миграция всех виртуальных машин на сервере на другой сервер из-за режима обслуживания или высокой доступности настройка интерфейс управления сервером и вторичных интерфейсов отключение управление сервером	Это разрешение включает в себя все действия, необходимые для поддержки пула Примечание. Если интерфейс управления не работает, никакие пользователи не могут проходить проверку подлинности, кроме локальных пользователей

© 2025 Нума Технологии, ООО

Полномочие	Детали	Примечание
	удаление crashdumps добавление, редактирование и удаление сетей добавление, редактирование и удаление PBD/PIF/VLAN/Bonds/SR добавление, редактирование и удаление секретов	
Живая миграция	перенос виртуальных машин с одного хоста на другой, когда виртуальные машины находятся в хранилище, совместно используемом обоими хостами	
Хранилище для живой миграции	миграция с одного хоста на другой, если виртуальные машины не находятся в хранилище, совместно используемом двумя хостами перемещение виртуальных дисков (VDI) из одного SR в другой SR	
Расширенные операции по управлению ВМ	настройка памяти ВМ (через динамическое управление памятью) создание снимка виртуальной машины с памятью, создание снимков виртуальной машины и откат виртуальных машин миграция виртуальных машин запуск виртуальных машин, в том числе с указанием физического сервера возобновление работы ВМ	Это разрешение предоставляет уполномоченному достаточно прав для запуска ВМ на другом сервере, если они не удовлетворены выбранным сервером Numa vServer
Создание и удаление ВМ	создание и удаление ВМ клонирование/копирование виртуальных машин добавление, удаление и настройка виртуальных дисков/CD устройств добавление, удаление и настройка виртуальных сетевых устройств импорт/экспорт файлов XVA изменение конфигурации виртуальных машин резервное копирование и восстановление сервера	Примечание. Роль VM Admin может импортировать файлы XVA только в пул с общим SR. Роль VM Admin не имеет достаточных прав для импорта файла XVA на хост или в пул без общего хранилища
Изменение подключенных CD образов в ВМ	установка/извлечение CD	
Изменение состояния питания ВМ	запуск виртуальных машин выключение виртуальных машин перезагрузка виртуальных машин	Это разрешение не включает start_on, resume_on и migrate, которые являются частью разрешения расширенных операций виртуальной машины

© 2025 Нума Технологии, ООО

Полномочие	Детали	Примечание
	приостановка виртуальных машин	
	возобновление работы виртуальных машин	
Доступ к консоли ВМ	взаимодействие с консолью виртульных машин	Это разрешение не позволяет пользователю просматривать серверную консоль
Отмена собственных задач	позволяет пользователю отменять собственные задачи	
Чтение журнала аудита	позволяет просматривать журнал аудита	
Подключение к пулу и чтение метаданных пула	подключение к пулу	
	просмотр метаданных пула	
	просмотр данных о производительности	
	просмотр зарегистрированных пользователей	
	просмотр пользователей и ролей	
	просмотр сообщений	
	регистрация и получение событий	
Настройка vGPU	настройка политики размещения в пуле	
	назначение виртуального графического процессора виртуальной машине	
	удаление виртуального графического процессора виртуальной машины	
	изменение разрешенных типов виртуальных графических процессоров	
	создание, удаление и назначение групп GPU	
Просмотр конфигурации vGPU	просмотр графических процессоров, политик размещения графических процессоров и назначений vGPU	
Доступ к конфигурационному диску (только для ВМ CoreOS)	доступ к драйверу конфигурации виртуальной машины	
	изменение параметров облачной конфигурации	
Управление контейнером	запуск	
	остановка	
	пауза	
	резюме	
	доступ к информации о контейнере	
Запланированные моментальные снимки	создание и удаление моментальных снимков виртуальных машин	
Запланированные снимки	добавление виртуальных машин в расписания снимков	

© 2025 Нума Технологии, ООО

Полномочие	Детали	Примечание
	удаление виртуальные машины из расписания снимков добавление расписания снимков	
изменение расписания снимков удаление расписания снимков		
Настройка проверки работоспособности	включение проверки работоспособности отключение проверки работоспособности обновление настроек проверки работоспособности ручная загрузка отчета о состоянии сервера	
Просмотр результатов и настроек проверки работоспособности	просмотр результатов проверки работоспособности просмотр настроек регистрации проверки работоспособности	
Настройка отслеживания измененных блоков	включение отслеживания измененных блоков отключение отслеживания измененных блоков уничтожение данных связанных со снимками и сохранение метаданных	
получение информации о соединении NBD для VDI		
Просмотр списка измененных блоков	сравнение двух снимков VDI и перечисление блоков, которые изменились	

5.3. Аутентификация пользователей с использованием модуля PAM

Внешняя система аутентификации PAM позволяет создавать локальных пользователей Для включения внешней системы аутентификации PAM введите команду:

```
xe pool-enable-external-auth auth-type=PAM service-name=<любое-имя>
```

Все запросы аутентификации Numa vServer будут проходить через механизм управления доступом на основе ролей (RBAC). RBAC позволяет тонко настраивать разрешения любых дополнительных пользователей или групп, которые доступны через внешнюю аутентификацию.

Для добавления пользователей:

1. Создайте локального пользователя:

```
useradd <username>
```

2. Задайте пользователю пароль:

© 2025 Нума Технологии, ООО

```
passwd <username>
```

Политика паролей

В Numa vServer реализована парольная политика со следующими критериями:

- минимальная сложность пароля с использованием символов не менее чем из 3 следующих категорий: прописные буквы английского алфавита от 'A' до 'Z', строчные буквы английского алфавита от 'a' до 'z', десятичные цифры от 0 до 9, спецсимволы ('~', '!', '@', '#', '$', '%', '^', '&', '*', '(', ')', '-', '+', '=', '_', '{','}', '[', ']', '\', '/', '|', ':', ';', '»', '', '"', '.', '?', '<', '>', '«');
- минимальное количество символов при создании новых паролей: в пределах от 6 до 8 символов (по умолчанию);
- время действия пароля, в пределах от 60 до 180 дней;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи субъекта доступа – от 3 до 10 попыток

3. Создайте субъект доступа:

```
xe subject-add subject-name=<username>
```

Команда выведет uuid субъекта.

4. Присвойте субъекту роль:

```
xe subject-role-add uuid=<subject-uuid> role-name=<role-name>
```

Роли пользователей

Для вывода списка ролей пользователей введите:

```
xe role-list
```

Подробнее про роли пользователей и их полномочия см. в разделах Управление доступом на основе ролей и Описание ролей и разрешений RBAC.

5. Выведите список субъектов и убедитесь, что созданнный пользователь есть в списке.

```
xe subject-list
```

5.4. Аутентификация пользователей с использованием Active Directory

Использование сервера Active Directory для аутентификации позволяет пользователям войти в Numa vServer, используя свои учетные данные домена ОС Windows.

Субъект в терминологии Numa vServer соответствует записи на сервере каталогов AD/LDAP/FreeIPA (соответствующей пользователю или группе). Когда внешняя аутентификация доступна, учетные данные используются для создания сеанса. Сначала проверяются учетные данные локального

© 2025 Нума Технологии, ООО

пользователя (в случае, если сервер каталогов недоступен), а затем список субъектов. Чтобы разрешить доступ к чему-то, необходимо создать запись для пользователя или группы, которым будет предоставлен этот доступ. Для этого используются команды xe, которые описаны далее.

Numa vServer позволяет использовать авторизационные данные Active Directory для учетных записей Numa vServer. Для этого, Numa vServer отправляет учетные данные Active Directory на контроллер домена Active Directory.

При добавлении в Numa vServer пользователи и группы Active Directory становятся субъектами Numa vServer. Когда субъект зарегистрирован в Numa vServer, пользователи/группы проходят проверку подлинности в Active Directory при входе в систему. Таким образом, отпадает необходимость квалифицировать имя пользователя с именем домена.

> **Примечание**
>
> По умолчанию, если домен пользователя не был уточнён (например, в виде «MyDomain\MyUser» или «myuser@mydomain.com»), Numa vServer попытается осуществить вход пользователей в серверы аутентификации Active Directory, используя домен, подключенный в настоящее время. Исключением из этого правила является учетная запись LSU, которая всегда аутентифицируется сначала локально (то есть на Numa vServer).

Процесс внешней аутентификации происходит следующим образом:

1. Учетные данные, при подключении к серверу, передаются на контроллер домена Active Directory для аутентификации.
2. Контроллер домена проверяет полномочия. Если они являются недействительными, аутентификация тут же прекращается.
3. Если учетные данные действительны, контроллер Active Directory запрашивает получение идентификатора и группы согласно учетным данным.
4. Если идентификатор субъекта совпадает с одним из хранящихся в Numa vServer, аутентификация успешно завершается.

При подключении к домену разрешается аутентификация в Active Directory для пула. Однако когда пул подключен к домену, только пользователи из этого домена (или домена, с которым он имеет доверенные отношения) могут подключаться к этому пулу.

> **Предупреждение**
>
> Ручная настройка конфигурации DNS физического интерфейса сети с настроенным сервисом DHCP может привести к сбоям в интеграции Active Directory и, следовательно, к сбоям в аутентификации пользователей.

5.4.1. Настройка аутентификации Active Directory

Numa vServer поддерживает использование серверов Active Directory, начиная с версии Windows 2008.

Для аутентификации в Active Directory серверного узла Numa vServer необходимо, чтобы использовались одни и те же DNS как для Active Directory сервера (настроенного для разрешения в совместимости), так и для серверного узла Numa vServer. В некоторых конфигурациях сервер Active Directory может сам предоставить сервис DNS. Это может быть достигнуто либо с помощью DHCP, чтобы предоставить IP-адрес и список DNS-серверов в Numa vServer, либо путем установки значений в объектах физического интерфейса.

> **Внимание!**
>
> Доменные имена серверных узлов Numa vServer должны быть уникальными в течение всего времени нахождения Numa vServer в домене.

Следует обратить внимание на следующие особенности:

- Numa vServer записывает входы в AD с использованием данного имени сервера в базу данных AD. Поэтому, если два сервера узла имеют одинаковое имя и подключены к одному и тому же домену, второй перезапишет вход в AD первого, независимо от того, находятся они в

© 2025 Нума Технологии, ООО

одном или разных пулах, в результате чего аутентификация на первом перестанет работать. Можно использовать одно и то же доменное имя на двух серверных узлах Numa vServer, пока они подключены к разным AD доменам;

- серверные узлы могут находиться в разных часовых поясах. Для обеспечения корректной синхронизации можно использовать одни и те же NTP-сервера для пула Numa vServer и для Active Directory сервера;
- пулы со смешанной аутентификацией не поддерживаются (то есть невозможно иметь пул, где одни сервера настроены для использования Active Directory, а другие – нет);
- интеграция Active Directory в Numa vServer происходит с использованием протокола Kerberos для соединения с серверами Active Directory. Как следствие, Numa vServer не поддерживает взаимодействие с серверами Active Directory без участия Kerberos;
- чтобы внешняя аутентификация с использованием Active Directory проводилась успешно, важно, чтобы системное время на серверных узлах Numa vServer было синхронизировано с системными часами на сервере Active Directory. Это проверяется, когда Numa vServer присоединяется к домену Active Directory, и если разница превышает допустимые значения, то аутентификация завершится ошибкой.

> **Примечание**
>
> Доменные имена должны состоять исключительно из букв и цифр длиной не менее одной буквы и не более 63 символов.

При добавлении в пул нового серверного узла после того, как был включен механизм аутентификации Active Directory, администратору будет предложено настроить на добавляемом сервере Active Directory. При появлении запроса на ввод учетных данных следует ввести учетные данные Active Directory с правами, достаточными для добавления серверов в этом домене.

5.4.2. Интеграция Active Directory

Необходимо убедиться в том, что сетевые порты для исходящего трафика, перечисленные в таблице ниже, открыты в настройках межсетевого экрана Numa vServer.

Таблица – Порты, необходимые для интеграции Active Directory

Порт	Протокол	Назначение
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB поверх TCP
464	UDP/TCP	Изменение пароля машины
3268	TCP	Global Catalog Search

> **Примечание**
>
> Для просмотра правил межсетевого экрана используется команда:

```
iptables -nL
```

© 2025 Нума Технологии, ООО

5.4.3. Управление паролем учетной записи компьютера для интеграции AD

Как и на клиентских машинах под управлением Windows, Numa vServer автоматически обновляет пароль учетной записи компьютера. Numa vServer обновляет пароль каждые 30 дней или в соответствии с политикой обновления пароля учетной записи компьютера на сервере AD.

5.4.4. Включение и отключение внешней системы аутентификации с использованием AD

Для включения внешней аутентификации с помощью Active Directory выполните следующую команду:

```
xe pool-enable-external-auth auth-type=AD service-name=<full-qualified-domain>
config:user=<username> config:pass=<password>
```

Указанный пользователь должен иметь привилегии для добавления и удаления компьютеров или рабочих станций, что по умолчанию разрешено администраторам доменов.

Если в сети, используемой Active Directory и серверными узлами Numa vServer, не используется DHCP, можно использовать следующие подходы к настройке DNS:

- настроить порядок поиска суффиксов домена DNS для работы с адресами, не являющимися FQDN:

```
xe pif-param-set uuid=<pif-uuid_in_the_dns_subnetwork> “other-config:domain=suffix1.com
suffix2.com suffix3.com”
```

- назначить DNS-сервер для серверов Numa vServer:

```
xe pif-reconfigure-ip mode=static dns=<dnshost> ip=<ip> gateway=<gateway> netmask=<netmask>
uuid=<uuid>
```

- вручную назначить для интерфейса управления PIF-объект из той же сети, что и DNS-сервер:

```
xe host-management-reconfigure pif-uuid=<pif_in_the_dns_subnetwork>
```

> **Примечание**
>
> Внешняя аутентификация является параметром, задаваемым отдельно для каждого серверного узла. Тем не менее, рекомендуется включать или отключать это параметр для всего пула – в этом случае при обработке сбоя на любом сервере и выполнении любых требуемых откатов состояний будет гарантироваться, что установленная конфигурация подходит для всего пула.

Для проверки параметров серверного узла и определения состояния внешней аутентификации можно использовать команду `xe host-param-list`, проверяя значения соответствующих полей.

Для отключения внешней аутентификации используется команда:

```
xe pool-disable-external-auth
```

© 2025 Нума Технологии, ООО

5.5. Удаленное управление Numa vServer

Пользователи с помощью команд xe могут удаленно управлять сервером, используя аргументы `-u` (имя пользователя, username), `-pw` (пароль пользователя, password), `-s` (IP-адрес Numa vServer, над которым выполняется действие).

Например:

```
xe vm-install -u user -pw Qazwsx102938* -s 10.150.100.100
```

5.6. Пользовательская аутентификация

Для разрешения доступа пользователя к серверному узлу Numa vServer необходимо добавить запись о субъекте доступа для этого пользователя, либо для группы, в которой он находится (вложенность групп проверяется в обычном порядке, например, если добавить разрешение для группы A, содержащей группу B, то пользователь из группы B будет иметь это разрешение).

Для управления разрешениями пользователей в Active Directory можно создать единую группу, а затем работать с ней, добавляя и удаляя пользователей. Можно добавлять и удалять отдельных пользователей, или сочетать использование отдельных пользователей и групп. Список субъектов может управляться с помощью интерфейса командной строки, как описано ниже.

При аутентификации пользователя, учетные данные сначала проверяются на соответствие учетной записи локального суперпользователя, что позволяет восстановить систему, если сервер AD вышел из строя. Если учетные данные (имя пользователя, пароль) не совпадают, то запрашивается аутентификация на сервере AD – если соединение с сервером AD происходит успешно, информация пользователя будет передана туда и проверен на соответствие списку субъектов, имеющемуся там. Если совпадение не будет найдено, либо не получится установить соединение с сервером AD, в доступе пользователю будет отказано. Проверка по списку субъектов считается успешной, если пользователь или его группа (возможно, в составе вложенной группы) имеются в списке субъектов доступа.

> **Внимание**
>
> При использовании групп Active Directory для предоставления доступа для пользователей с ролью Администратора пула, которым необходим доступ к хосту по SSH, число пользователей в группе Active Directory не должно превышать 500.

5.6.1. Управление пользовательским доступом к серверному узлу

Для добавления в список AD субъекта доступа к серверному узлу существует команда:

```
xe subject-add subject-name=<entity name>
```

В качестве entity name может использоваться имя пользователя или название группы, которому (которой) требуется предоставить доступ. Также можно в необязательном порядке указать домен (например, «<testad\user1>», а не просто «<user1>»), если это требуется для однозначности.

Для запрета пользователю доступа к серверному узлу необходимо выполнить следующую последовательность действий:

- найти идентификатор субъекта пользователя. Это пользователь или группа, содержащая пользователя (удаление группы запрещает доступ всем пользователям этой группы, если они не были также указаны в списке субъектов непосредственно). Для нахождения идентификатора необходимо использовать команду возвращающую список пользователей:

  ```
  xe subject-list
  ```

  Для облегчения поиска имеется возможность задавать фильтры для выводимых результатов поиска. Следующая команда выведет (при условии наличия) информацию о пользователе user1 в домене testad:

© 2025 Нума Технологии, ООО

```
xe subject-list other-config:subject-name='<testad\user1>'
```

- используя найденный идентификатор (UUID), можно удалить запись о разрешении доступа пользователю при помощи команды:

```
xe subject-remove subject-uuid=<subject-uuid>
```

Для принудительного завершения текущей сессии конкретного пользователя используется команда:

```
xe session-subject-identifier-logout subject-identifier=<subject-id>
```

Для принудительного завершения текущих сессий всех пользователей, работающих в системе в настоящий момент, используется команда:

```
xe session-subject-identifier-logout-all
```

Если принудительно не завершить сессии пользователей, доступ которым был запрещён, они будут иметь доступ к серверному до завершения своей сессии.

5.7. Вывод из домена Active Directory

> **Примечание**
>
> Когда администратор принимает решение покинуть домен (то есть отключить проверку подлинности Active Directory и отсоединить пул или сервер от этого домена), все пользователи, прошедшие аутентификацию в пуле или на сервере с учетными данными Active Directory, будут отключены.

Чтобы покинуть домен AD, следует выполнить команду:

```
xe pool-disable-external-auth
```

Указав идентификатор UUID пула, если требуется.

> **Примечание**
>
> Вывод севера из домена не влечёт удаление серверных записей из базы данных Active Directory.

© 2025 Нума Технологии, ООО

5.8. Использование RBAC через интерфейс CLI

Для вывода списка доступных ролей в Numa vServer используется команда:

Команда

```
xe role-list
```

Пример вывода

```
xe role-list

uuid( RO): 0165f154-ba3e-034e-6b27-5d271af109ba
name ( RO): pool-admin
description ( RO): The Pool Administrator role has full access to all
features and settings, including accessing Dom0 and managing subjects,
roles and external authentication

uuid ( RO): b9ce9791-0604-50cd-0649-09b3284c7dfd
name ( RO): pool-operator
description ( RO): The Pool Operator role manages host-  and pool-wide resources,
including setting up storage, creating resource pools and managing patches, and
high availability (HA).

uuid( RO): 7955168d-7bec-10ed-105f-c6a7e6e63249
name ( RO): vm-power-admin
description ( RO): The VM Power Administrator role has full access to VM and
template management and can choose where to start VMs and use the dynamic memory
control and VM snapshot features

uuid ( RO): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
name ( RO): vm-admin
description ( RO):  The VM Administrator role can manage VMs and templates

uuid ( RO): fb8d4ff9-310c-a959-0613-54101535d3d5
name ( RO): vm-operator
description ( RO):  The VM Operator role can use VMs and interact with VM consoles

uuid ( RO): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
name ( RO): read-only
description ( RO): The Read-Only role can log in with basic read-only access
```

Список ролей статичен, нельзя добавить новые роли, удалить или изменить старые.

Для отображения списка текущих субъектов доступа используется команда `xe subject-list`, возвращающая список пользователей, их идентификаторы и роли, если такие присутствуют в системе.

5.8.1. Добавление субъекта в систему RBAC

Для того чтобы включить существующих в AD пользователей в систему RBAC, необходимо создать экземпляр субъекта в Numa vServer, либо для пользователя AD непосредственно – либо напрямую для одного из пользователей, прописанных в AD, либо для одной из содержащих его групп:

```
xe subject-add subject-name=<AD user/group>
```

© 2025 Нума Технологии, ООО

5.8.2. Назначение роли созданному субъекту

Для назначения субъекту роли используется его идентификатор UUID:

```
xe subject-role-add uuid=<subject_uuid> role-uuid=<role_uuid>
```

или имя:

```
xe subject-role-add uuid=<subject_uuid> role-name=<role_name>
```

Пример. Следующая команда назначает пользователю с идентификатором UUID, равным `b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4`, роль «Pool Administrator»:

```
xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name=pool-admin
```

5.8.3. Изменение роли субъекта доступа

Изменение роли пользователя, в частности, необходимо для снятия с него текущей роли (поскольку в любой момент времени хотя бы одна роль должна быть назначена). Используются следующие команды:

```
xe subject-role-remove uuid=<subject_uuid> role-name=<role_name_to_remove>
```

```
xe subject-role-add uuid=<subject_uuid > role-name=<role_name_to_add>
```

Чтобы убедиться, что новая роль вступила в силу, пользователь должен выйти из системы и снова пройти авторизацию (чтобы иметь возможность сделать это для другого пользователя принудительно, необходимо иметь разрешение на отсоединение активных пользователей (Logout Active User Connections), что доступно только Администраторам пула или Операторам пула).

После добавления или удаления субъекта с ролью Администратора пула может возникнуть задержка на несколько секунд для SSH-сессий, связанных с этим субъектом, на всех хостах пула.

5.9. Аудит RBAC

Журнал аудита RBAC записывает все операции, предпринятые вошедшим в систему пользователем. Запись аудита будет явно содержать идентификатор субъекта и имя пользователя, ассоциированное с сессией, которая вызвала операцию.

В случае успешного выполнения какой-либо операции, фиксируется факт успеха; если операция не удалась, записывается также код ошибки.

Всегда фиксируется факт запроса выполнения операций, для осуществления которых субъект не имеет разрешения.

5.9.1. Команды CLI, связанные с журналом аудита

Следующая команда выгружает в файл все имеющиеся записи файла аудита RBAC пула. Если необязательный параметр `since` присутствует, то выгружаются только записи позднее указанной в этом параметре метки времени/даты.

```
xe audit-log-get [since=<timestamp>] filename=<output_filename>
```

Следующая команда позволяет выгрузить все записи аудита для пула:

© 2025 Нума Технологии, ООО

```
xe audit-log-get filename=/var/data/auditlog-pool-actions.out
```

Для получения записей журнала аудита пула, датированных позднее точной миллисекундной метки, используется команда:

```
xe audit-log-get since=2019-09-24T17:56:20.530Z filename=/var/data/auditlog-pool-actions.out
```

Для получения записей журнала аудита пула, датированных позднее метки с точностью до минуты, используется команда:

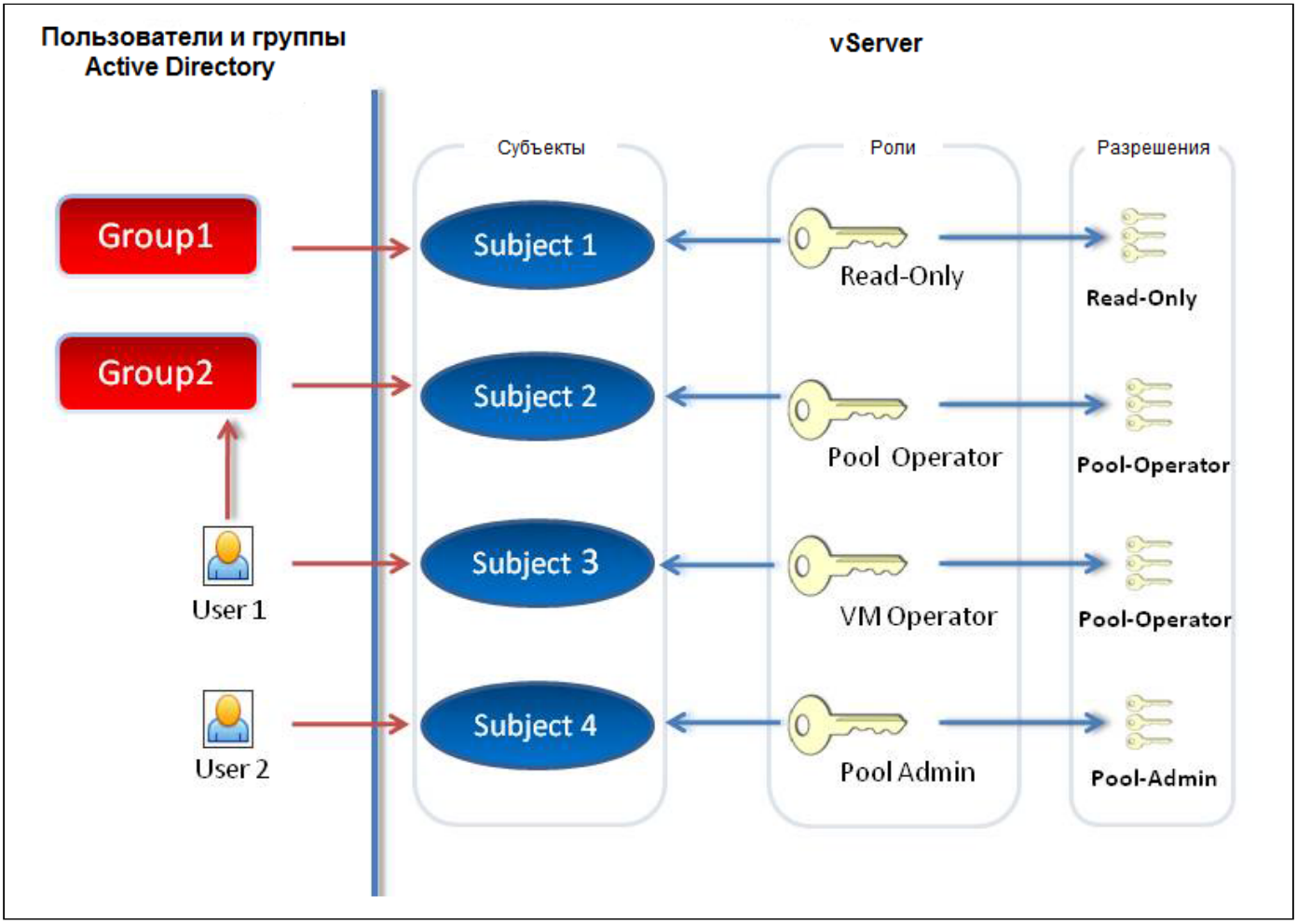
```
xe audit-log-get since=2019-09-24T17:56Z filename=/var/data/auditlog-pool-actions.out
```

5.10. Расчёт ролей для сессии в Numa vServer

Роль каждого конкретного субъекта в каждой сессии работы рассчитывается следующим образом.

- субъект проходит аутентификацию через сервер Active Directory для того, чтобы проверить, какие содержащие субъект группы также имеются в списках AD;
- Numa vServer заверяет набор ролей, отведённых субъекту и содержащим его группам;
- субъект, входящий в несколько групп, наследует все доступные им разрешения.

Схема получения окончательного набора ролей для сессии показана на рисунке ниже.



На этой иллюстрации, поскольку Subject2 (из группы Group2) является Оператором пула и пользователь User1 является членом группы Group2, когда Subject3 (пользователь User1) пытается войти, он наследует роли как Subject3 (роль «Оператор ВМ»), так и группы Group2 (роль «Оператор

© 2025 Нума Технологии, ООО

пула»). Поскольку роль «Оператор пула» выше по числу разрешений, в результате ролью субъекта Subject3 (User1) становится «Оператор пула», а не «Оператор ВМ».

© 2025 Нума Технологии, ООО

6. Обеспечение высокой доступности (high availability)

6.1. Описание механизма высокой доступности

Механизм обеспечения высокой доступности (далее – Механизм HA) является набором автоматических характеристик, спроектированных для учёта ситуаций (проблем), которые делают серверы недоступными, а также для безопасного восстановления функционирования пула после таких ситуаций. Механизм HA применяется для автоматического восстановления административного контроля над пулом в случае, если мастер пула становится недоступным или его работа становится нестабильной.

> ⚠ Обязательное использование механизма HA
>
> Механизм HA должен ВСЕГДА использоваться в системах с многоканальным подключением к хранилищу (multipathing) и агрегацией сетевых интерфейсов. При этом настройка Multipathing и агрегированных сетевых интерфейсов должна производиться до активации высокой доступности.

6.1.1. Примеры применения механизма HA

Механизм HA используется при нестабильной работе или недоступности сервера (например, при физических разрывах передачи данных по сети или неполадок аппаратного обеспечения хоста). В этом случае запущенные ВМ прекращают работу на текущем сервере и возобновляют работу на другом стабильном сервере. Для удобства последовательного запуска сервисов ВМ могут распределяться в группы по приоритетам запуска (это даёт возможность сначала запускать административные ВМ, затем зависящие от них ВМ. Например, запускать сервер DHCP раньше, чем зависящий от него сервер SQL). При этом можно избежать сценария, когда ВМ начинают работу (автоматически или вручную) на новом сервере, а предыдущий их сервер восстанавливает работу, что может привести к запуску экземпляров ВМ на разных серверах с высокой вероятностью порчи и потери данных ВМ.

Также механизм HA защищает от переполнения пула. Пул считается переполненным (overcommitted), если работающие ВМ не могут перезапуститься на одном из прочих серверов пула вследствие достижения в пуле критического количества отказов хостов. Данный показатель задаётся администратором.

© 2025 Нума Технологии, ООО

Подробнее про защиту от переполнения пула

Переполнение происходит, если не хватает свободной оперативной памяти в пуле для запуска ВМ, испытывающих отказ. Могут существовать другие малозаметные изменения, ухудшающие работу HA: изменения в виртуальных блочных устройствах (VBD) и сетях могут повлиять на выбор хоста, на котором будет перезапущена ВМ. В настоящий момент Numa vServer не может контролировать все действия, которые ведут к нарушению требований работы HA. При нарушении работы HA высылается асинхронное уведомление.

Numa vServer в реальном времени разрабатывает и осуществляет план обеспечения отказоустойчивости серверов в пуле (failover plan), определяющий действия в случае отказа некоторого количества серверов пула за некоторое заданное время. Важным для понимания является параметр максимального некритического количества отказов хостов (host failures to tolerate). Например, если пул ресурсов состоит из 6 серверов и некритическое количество отказов равняется 3, то пул рассчитывает план обеспечения отказоустойчивости, который позволяет при отказе любых трёх серверов продолжить работу ВМ на других серверах. Если отказывает большее количество, пул считается переполненным. План динамически пересчитывается с учётом анализа операций рабочего цикла и миграций ВМ. Если в процессе изменений (например, добавления новых ВМ в пул) появляется опасность переполнения пула, то система может выслать предупреждение (например, по электронной почте).

Предупреждение о переполнении

Если при старте или продолжении работы ВМ пул переполняется (overcommitted), система предупреждает об этом. Это предупреждение отображается при отсутствии доступного графического интерфейса в терминал API. Если заданы соответствующие настройки, сообщение может быть отправлено администратору по электронной почте. Затем будет предложено закончить операцию или продолжить ее. Продолжение операции приведет к переполнению пула. Количество информации, используемой ВМ с различными приоритетами, будет отображено в пуле и на хостах.

Изоляция сервера

В случае если происходит отказ сервера, теряется структура коммутации сети или возникает проблема с управляющим стеком, сервер самоизолируется (самоограживается) для того, чтобы исключить запуск одних ВМ на двух серверах одновременно. После запуска изоляции сервер немедленно перезагружается, а работа всех ВМ прекращается. Остальные серверы регистрируют остановку ВМ и далее ВМ перезагружаются в соответствии с определенными для них приоритетами. Изолированный сервер начинает процесс перезагрузки и после перезапуска пытается войти заново в пул ресурсов.

6.2. Требования к конфигурации механизма HA

6.2.1. Конфигурация инфраструктуры

Для настройки механизма HA необходимо наличие:

- пула из не менее чем 3 серверов (обеспечивает высокую доступность на уровне сервера в рамках одного пула ресурсов);
- статические IP-адреса для всех серверов;
- общее хранилище, доступное по протоколам iSCSI, NFS, SMB или Fibre Channel, для создания служебных томов (heartbeat SR) объемом 365 Мб или более.

  Механизм высокой доступности создаёт два тома на heartbeat SR:

  - том объёмом 4 Мбайт на heartbeat;
  - том объёмом 256 Мбайт для хранения метаданных мастера пула, которые будут использованы в случае отказа мастера.

Примечания

a. Для большей надежности настоятельно рекомендуется для heartbeat SR использовать общие хранилища данных на основе протоколов NFS или iSCSI, которые не используются в других целях.
b. Хранилище, подключенное с использованием протоколов SMB или iSCSI, при проверке подлинности с использованием CHAP не может использоваться в качестве heartbeat SR.
c. В случае использования хранилищ на основе NetApp или EqualLogic необходимо вручную задать адрес дискового устройства (LUN) NFS или iSCSI в массиве данных для использования в качестве хранилища под heartbeat SR.

© 2025 Нума Технологии, ООО

- для максимальной надежности рекомендуется использовать выделенный сетевой интерфейс для сети управления высокой доступностью.

6.2.2. Конфигурация ВМ

Чтобы виртуальная машина была защищена механизмом высокой доступности, она должна быть мобильной. Это означает, что:

- виртуальные диски ВМ должны быть в общем хранилище. Можно использовать любой тип общего хранилища. Только для диска на основе iSCSI, NFS или Fibre Chanel, который предполагается использовать для heartbeat SR, требуется номер логического устройства (Logical Unit Number, LUN). Опционально эти диски также могут быть использованы в качестве обычных виртуальных дисков;
- ВМ могут использовать живую миграцию;
- у ВМ отсутствует соединение с физическими DVD-приводом и USB-устройствами;
- у ВМ есть собственные виртуальные сетевые интерфейсы в сети пула.

> **Примечание**
>
> При включенном механизме HA настоятельно рекомендуется заранее агрегировать интерфейс управления на серверах пула, а также использовать многопоточные (multipath) хранилища в основе heartbeat SR.

При создании VLAN и агрегированных интерфейсов они могут оказаться не подключенными. В этой ситуации ВМ не будут под защитой механизма HA. В этом случае нужно использовать команду `xe pif-plug` для ввода VLAN и PIF-объектов агрегаций сервера в действие, благодаря чему ВМ смогут стать мобильными. Точно определить, почему ВМ не являются мобильными, можно, используя команду `xe diagnostic-vm-status` для анализа существующих ограничений.

6.3. Активация механизма высокой доступности в пуле

Для включения механизма HA для выбранного пула выполните следующую последовательность действий:

1. Убедитесь, что пул состоит не менее чем из трех серверов.
2. Проверьте, что к пулу присоединено совместимое общее хранилище данных. Совместимыми являются хранилища на основе протоколов iSCSI, NFS или Fibre Channel (подробнее см. Создание и настройка хранилищ данных).
3. Для каждой виртуальной машины, которую необходимо защитить, установите приоритет перезапуска и порядок запуска:

```
xe vm-param-set uuid=<vm_uuid> ha-restart-priority=<restart|best-effort> order=<число>
```

> **Приоритет и порядок запуска ВМ**
>
> Подробнее про:
>
> - приоритет запуска ВМ
> - порядок запуска ВМ

4. Включите механизм HA в пуле и при необходимости укажите время ожидания:

```
xe pool-ha-enable heartbeat-sr-uuids=<sr-uuid> ha-config:timeout=<время-в-секундах>
```

где `heartbeat-sr-uuids` – UUID общего хранилища;
`timeout` – это период, в течение которого сеть или хранилище недоступны узлам в пуле.

© 2025 Нума Технологии, ООО

Если не указать `timeout` при включении высокой доступности, то `timeout` по умолчанию будет 30 секунд. Если какой-либо сервер не может получить доступ к сети или хранилищу в течение времени ожидания, он самостоятельно перезапустится.

5. Выполните команду, которая вернет максимальное количество отказов хоста, допустимое с точки зрения механизма HA:

```
xe pool-ha-compute-max-host-failures-to-tolerate
```

Допустимое (некритическое) количество отказов определяется моментом отправки тревоги: система пересчитывает план отказоустойчивости в зависимости от изменения состояния пула и таким образом система определяет объём памяти пула для определения количества некритических отказов для надежной работы защищенных ВМ. Система сигнализирует о тревоге, если расчетный уровень падает ниже заданного для `ha-host-failures-to-tolerate`.

6. Задайте значение параметра допустимого количества отказов в пуле. Оно должно быть не более рассчитанного на предыдущем шаге значения:

```
xe pool-param-set ha-host-failures-to-tolerate=<допустимое-число-отказов-серверов> uuid=<pool-uuid>
```

> ⚠ Обратите внимание
>
> При активации механизма HA некоторые операции, которые могут негативно сказаться на плане перезапуска ВМ (например, извлечение сервера из пула), могут бездействовать.

6.4. Отключения механизма высокой доступности в пуле

Для отключения механизма высокой доступности в пуле выполните команду:

```
xe pool-ha-disable
```

6.5. Приоритет запуска и перезапуска ВМ

Виртуальные машины могут иметь приоритеты запуска `protected` (защищенная), `best-effort` (лучшая попытка) или `unprotected` (незащищенная). Приоритет задается через параметр `ha-restart-priority` в настройках виртуальной машины. Поведение перезапуска для виртуальных машин в каждом приоритете отличается.

Для задания значение свойства `ha-restart-priority` виртуальной машины выполните команду:

```
xe vm-param-set uuid=<vm_uuid> ha-restart-priority=<restart|best-effort|пустая-строка>
```

> ⚠ Обратите внимание
>
> Если в пуле возникают сбои сервера и число допустимых сбоев падает до нуля, защищенным виртуальным машинам не гарантируется запуск. В таких случаях генерируется системное предупреждение. Если происходит другой сбой, все виртуальные машины, для которых установлен приоритет `protected`, ведут себя в соответствии с приоритетом `best-effort`.

© 2025 Нума Технологии, ООО

> **Примечание**
>
> Механизм высокой доступности никогда не останавливает и не мигрирует работающие виртуальные машины для освобождения ресурсов в пуле для запуска виртуальных машин с приоритетами `protected` и `best-effort`.

6.5.1. Приоритет protected

Механизм высокой доступности гарантирует запуск защищённой виртуальной машины при сбое сервера или при ее отключении, при условии, что пул не переполнен и ВМ является мобильной.

Если защищенная виртуальная машина не может быть запущена (например, при переполнении пула), механизм высокой доступности будет пытаться запустить виртуальную машину до тех пор, пока ВМ не запустится на освободившихся или дополнительных ресурсах пула.

Значение: `ha-restart-priority=restart`

6.5.2. Приоритет best-effort

При сбое виртуальных машин с приоритетом `best-effort`, механизм высокой доступности будет пытаться запустить ВМ на другом сервере, но попытки запуска начнутся только после того как будут запущены защищенные ВМ.

Попытка запуска выполняется один раз, если она не удалась, то ВМ остается в выключенном состоянии и попытки запуска больше не выполняются.

Значение: `ha-restart-priority=best-effort`

6.5.3. Приоритет unprotected

Если незащищенная виртуальная машина или сервер, на котором она работает, остановлена, механизм высокой доступности не будет пытаться перезапустить виртуальную машину.

Значение: `ha-restart-priority=<пустая-строка>`

6.6. Порядок запуска ВМ

Порядок запуска – это порядок, в котором серверы с включенным механизмом HA будут пытаться перезапустить защищенные ВМ при возникновении сбоя. Порядок запуска задается в параметре `order` для каждой защищенной ВМ с помощью команды:

```
xe vm-param-set uuid=<vm_uuid> order=<число>
```

где `order` – целое число. Значение по умолчанию равно 0, что является наивысшим приоритетом. Защищенные ВМ со значением `order=0` перезапускаются первыми. Чем выше значение свойства `order`, тем позже в последовательности перезапускается виртуальная машина.

Задать параметр order можно каждой ВМ, но механизм HA использует этот параметр только для защищенных ВМ.

6.7. Вывод ВМ из механизма высокой доступности

Для вывода ВМ из механизма высокой доступности выполните:

© 2025 Нума Технологии, ООО

```
xe vm-param-set ha-always-run=false uuid=<vm-uuid>
```

При необходимости можно снова включить высокую доступность для виртуальной машины, установив для параметра `ha-restart-priority` значение `restart` или `best-effort`.

```
xe vm-param-set uuid=<vm-uuid> ha-restart-priority=<restart|best-effort>
```

6.8. Восстановление недоступного сервера

Если по какой-то причине сервер не может получить доступ к файлу состояния высокой доступности, то возможно он стал недоступен. Для восстановления недоступного сервера сначала деактивируйте высокую доступность следующей командой:

```
xe host-emergency-ha-disable --force
```

Если сервер был мастером пула, он должен возобновить работу с деактивированной высокой доступностью. Подчиненные серверы соединяются заново и автоматически деактивируют высокую доступность. Если сервер был подчиненным участником пула и не может соединиться с мастером, принудительно перезагрузите сервер как мастер пула и/или направьте к новому мастеру:

```
xe pool-emergency-transition-to-master uuid=<host-uuid>
```

```
xe pool-emergency-reset-master master-address=<new-master-hostname-or-ip-address>
```

После успешного перезапуска всех серверов активируйте высокую доступность снова:

```
xe pool-ha-enable heartbeat-sr-uuid=<sr-uuid>
```

6.9. Выключение сервера при активированном механизме высокой доступности

Если происходит завершение работы или перезагрузка хоста, то активированный механизм высокой доступности может решить, что произошел сбой сервера. Для корректного завершения работы сервера, находящегося в пуле с включенной высокой доступностью:

1. Деактивируйте сервер:

```
xe host-disable host=<host-name>
```

2. Извлеките сервер:

```
xe host-evacuate uuid=<host-uuid>
```

3. Завершите его работу.

```
xe host-shutdown host=<host-name>
```

© 2025 Нума Технологии, ООО

6.10. Возможные ошибки

6.10.1. Ошибки при работе с Multipathing и агрегированными сетевыми интерфейсами

Механизм HA спроектирован для работы с многоканальным подключением хранилищ и агрегированными сетевыми интерфейсами, и они должны быть сконфигурированы ПЕРЕД активацией HA. Если этого не было сделано, то вследствие нестабильности сетевого оборудования может возникнуть непредвиденное поведение хоста при перезагрузке (так называемое самоизолирование, selffensing).

6.10.2. Сбой мастера пула

При возникновении сбоя мастер-сервера:

1. Замените вышедшего из строя мастера пула работающим рядовым сервером. Для этого в консоли рядового сервера выполните:

```
xe pool-emergency-transition-to-master
```

2. Подключите остальные серверы к новому мастеру пула:

```
xe pool-recover-slaves
```

3. Перезапустите ВМ, которые находились на вышедшем из строя сервере:

```
xe vm-reset-powerstate vm=<vm_uuid> --force
```

6.10.3. Ошибка "The uuid you supplied was invalid"

В случае получения сообщения 'The uuid you supplied was invalid' последовательно выполните следующие команды:

```
xe host-emergency-ha-disable --force
```

```
xe-toolstack-restart
```

```
xe pool-ha-disable
```

6.10.4. Изменение IP-адреса сервера при включенном механизме HA

Если IP-адрес сервера изменяется, когда включена высокая доступность, механизм высокой доступности предположит, что сеть хоста вышла из строя. Изменение IP-адреса может заблокировать хост и оставить его в не загружаемом состоянии. Чтобы исправить эту ситуацию:

1. Отключите механизм высокой доступности:

```
xe host-emergency-ha-disable
```

2. Сбросьте мастера пула:

© 2025 Нума Технологии, ООО

```
xe pool-emergency-reset-master
```

3. Затем снова включите высокую доступность:

```
xe pool-ha-enable heartbeat-sr-uuids=<sr_uuid>
```

6.10.5. Выключение ВМ с приоритетом protected

ВМ с приоритетом `protected` не может завершить работу при активированной высокой доступности в пуле. Для корректного завершения работы ВМ:

1. Деактивируйте высокую доступность в пуле

```
xe pool-ha-disable
```

2. Выключите ВМ

```
xe vm-shutdown uuid=<vm-uuid>
```

> **Примечание**
>
> Если завершить работу ВМ из гостевой системы, то ВМ автоматически перезапустится. Для завершения работы следует сначала деактивировать высокую доступность в параметрах ВМ.

© 2025 Нума Технологии, ООО

7. Команды управления Numa vServer

Администрирование Numa vServer осуществляется с помощью командной строки (CLI) командами xe.

7.1. Общая информация

Получение справки по отдельным командам xe CLI.

```
xe help <команда>
```

Получение справки по формату ввода команд и списка основных команд xe.

```
xe help
```

Список всех команд xe.

```
xe help --all
```

Основной синтаксис всех команд xe.

```
xe <команда> <параметр>=<значение> <параметр>=<значение>
```

Каждая команда содержит свой собственный набор параметров, которые имеют формат `<параметр>=<значение>`. Некоторые команды имеют обязательные параметры, а большинство имеют набор необязательных параметров. Обычно команда предполагает значения по умолчанию для некоторых необязательных параметров при вызове без них.

Если значение параметра не содержит пробелов, не используйте кавычки. Не включайте пробелы между именем параметра, знаком равенства (`=`) и значением. Любой параметр, не соответствующий этому формату, игнорируется.

Значения, содержащие пробелы, пишите в следующем формате: `<параметр>="значение с пробелами"`

Команды имеют функцию автодополнения табуляцией, похожую на функцию в стандартной оболочке Linux bash. Например, если вы введете `xe vm-l` и затем нажмете клавишу `Tab ↹`, остальная часть команды будет автоматически дополнена. Если с `vm-l` начинаются две и более команды, нажмите дважды `Tab ↹` для вывода списка всех возможных команд. Эта функция полезна при указании UUID объектов в командах.

> **Примечание**
>
> Автодополнение клавишей `Tab ↹` обычно не работает при запуске команд на удаленном сервере Numa vServer.

7.2. Удаленный запуск команд

Если команда xe запускается удаленно, для подключения и аутентификации используются дополнительные параметры:

- `username` или `-u` – имя пользователя, инициирующее действие
- `password` или `-pw` – пароль пользователя, инициирующего действие
- `server` или `-s` – IP-адрес или имя сервера, над которым производится действие

© 2025 Нума Технологии, ООО

Пример:

На локальном сервере

```
xe vm-list
```

На удаленном сервере

```
xe vm-list username=<имя-пользователя> password=<пароль-пользователя> server=<IP-адрес|имя-сервера>
```

или

```
xe vm-list -u <имя-пользователя> -pw <пароль-пользователя> -s <IP-адрес|имя-сервера>
```

> **Обратите внимание**
>
> Удаленный запуск команд можно сделать только к мастеру пула.

7.3. Типы команд

Команды xe можно разделить на две группы: низкоуровневые и высокоуровневые. Низкоуровневые команды связаны с листингом и манипуляцией параметрами объектов API. Высокоуровневые команды используются для взаимодействия с виртуальными машинами или хостами на более абстрактном уровне.

Формат низкоуровневых команд:

- `<class>-list`
- `<class>-param-get`
- `<class>-param-set`
- `<class>-param-list`
- `<class>-param-add`
- `<class>-param-remove`
- `<class>-param-clear`

Где `class` может принимать следующие значения: `bond`, `host`, `network`, `pbd`, `pif`, `pool`, `snapshot`, `sr`, `subject`, `task`, `template`, `vbd`, `vdi`, `vif`, `vlan`, `vm`.

> **Примечание**
>
> Не каждый класс может иметь формат `<class>-param-<действие>`.

7.4. Типы параметров

Большинство параметров могут принимать только одно значение. Например, параметр `name-label` ВМ содержит одно строковое значение.

В выводах команд для просмотра списка параметров, таких как `xe vm-param-list uuid=<vm_uuid>` значения параметров могут быть типа чтение-запись (RW) или только чтение (RO). Например:

© 2025 Нума Технологии, ООО

```
user-version ( RW): 1
is-control-domain ( RO): false
```

Параметр `user-version` может быть изменен, а `is-control-domain` доступен только для чтения.

Также есть еще многозначные параметры типа MRW и SRO. Например:

```
platform (MRW): acpi: true; apic: true; pae: true; nx: false
allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
hard_shutdown; hard_reboot; suspend
```

Параметр `platform` имеет множество пар ключ-значение, отделяемых двоеточием (`:`), например, `acpi: true`. Буква M перед RW указывает, что этот параметр состоит из пар ключ-значение и доступен для чтения и записи. Пары ключ-значение отделяются точкой с запятой (`;`). например, `acpi: true; apic: true;`.

Для изменения параметра с парой ключ-значение используйте двоеточие (:). Например, для изменения значения ключа `foo` для параметра `other-config`:

```
xe vm-param-set uuid=VM uuid other-config:foo=baa
```

Параметр `allowed-operations` имеет набор значений. Буква S перед RO указывает, что параметр доступен для чтения, но не для записи.

7.5. Справочник команд

В этом разделе приведены часто используемые команды.

7.5.1. Команды управления bond-интерфейсами

Команды для работы с физическими сетевыми интерфейсами, объединенными в одну виртуальную интерфейсную группу (bond) с целью увеличения производительности, отказоустойчивости или нагрузки между несколькими физическими интерфейсами.

Действие	Команда	Примечание
Создание bond-интерфейса из существующих PIF	`xe bond-create network-uuid=<network_uuid> pif-uuids=<pif_uuid_1>,<pif_uuid_2>,...`	Команда не выполняется в любом из следующих случаев: • Если PIF уже входят в другие bond-интерфейсы • Если у какого-либо участника bond-интерфейса установлен тег VLAN • Если указанные PIF находятся на разных серверах Numa vServer • Если указано менее двух PIF
Удаление bond-интерфейса с сервера	`xe bond-destroy uuid=<bond_uuid>`	
Изменение типа связи bond-интерфейса	`xe bond-set-mode uuid=<bond_uuid> mode=<bond_mode>`	Параметр `mode` может принимать следующие значения: • `balance-slb` – используется для объединения пропускной способности нескольких физических интерфейсов и балансировки нагрузки на них • `active-backup` – используется для резервирования подключения. В этом режиме работает один из физических интерфейсов, включенных в агрегацию, а остальные будут задействованы в случае отказа активного

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
		• `lacp` – протокол агрегирования каналов, используется для повышения пропускной способности и отказоустойчивости

7.5.2. Команды управления серверами

Серверы Numa vServer — это физические серверы, на которых установлено и запущено программное обеспечение Numa vServer. На них работают виртуальные машины под управлением специальной привилегированной виртуальной машины, известной как домен управления или dom0.

Действие	Команда	Примечание
Вывод списка серверов в пуле	`xe host-list`	
Формирование файла резервной копии домена управления указанного сервера	`xe host-backup file-name=<backup_filename> host=<host_name>`	Внимание! Запускайте команду только с удаленного сервера
Вычисление объема свободной памяти на сервере	`xe host-compute-free-memory host=<host_name>`	
Вывод информации о физических процессорах сервера	`xe host-cpu-info [uuid=host_uuid]`	
Отключение сервера для предотвращения запуска на нем виртуальных машин. Это действие подготавливает серверы к выключению или перезагрузке	`xe host-disable host=<host-name>`	
Включение сервера для запуска на нем виртуальных машин	`xe host-enable host=<host-name>`	
Перенос (живая миграция) всех работающих ВМ на другой подходящий сервер	`xe host-evacuate host=<host-name>`	Порядок эвакуации сервера: 1. Сначала отключите эвакуируемый сервер с помощью команды `xe host-disable host=<host-name>` 2. Если эвакуируемый сервер является мастером пула, то необходимо выбрать другой сервер в качестве мастера пула: • При отключенном механизме HA используйте команду `xe pool-designate-new-master host-uuid=<uuid_of_new_master>` • При включенном механизме HA единственным вариантом является выключение сервера (команда `xe host-shutdown host=<host-name>`) для того, чтобы механизм HA выбрал мастера пула случайным образом. 3. Далее выполните команду по эвакуации сервера, который перенесет все работающие ВМ на другой сервер: `xe host-evacuate host=<host-name>`
Перезагрузка сервера	`xe host-reboot host=<host-name>`	Серверы должны быть сначала отключены с помощью команды `xe host-disable host=<host-name>`, иначе отобразится ошибка `HOST_IN_USE`. Если указанные серверы входят в пул ресурсов, то сначала при выключении серверов произойдет потеря связи с пулом, затем при включении серверов пул восстановит работу. Другие серверы и мастер пула продолжают функционировать. Если вы отключите мастера пула, пул перестанет работать до тех пор, пока не произойдет одно из следующих действий: 1. Вы назначите одного из серверов мастером пула.

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
		2. Исходный мастер пула перезагружается и снова подключается к сети. Когда мастер пула снова подключается к сети, участники повторно подключаются и синхронизируются с мастером пула.
Выключение сервера	`xe host-shutdown host=<host-name>`	Серверы должны быть сначала отключены с помощью команды `xe host-disable host=<host-name>`, иначе отобразится ошибка `HOST_IN_USE`. Если указанные серверы входят в пул ресурсов, то сначала при выключении серверов произойдет потеря связи с пулом, затем при включении серверов пул восстановит работу. Другие серверы и мастер пула продолжают функционировать. Если вы отключите мастера пула, пул перестанет работать до тех пор, пока не произойдет одно из следующих действий: 1. Вы назначите одного из серверов мастером пула. 2. Исходный мастер пула перезагружается и снова подключается к сети. Когда мастер пула снова подключается к сети, участники повторно подключаются и синхронизируются с мастером пула.

7.5.3. Команды управления сетями

Действие	Команда	Примечание
Список объектов	`xe network-list`	
Создание сети	`xe network-create name-label=<network-name> [name-description=<descriptive_text>]`	Команда выведет UUID созданной сети
Уничтожение сети	`xe network-destroy uuid=<network_uuid>`	

7.5.4. Команды управления PBD

Команды работы с физическими блочными устройствами (PBD). PBD – это программные объекты, через которые сервер обращается к хранилищам.

Действие	Команда	Примечание
Список объектов PBD	`xe pbd-list`	
Создание PBD	`xe pbd-create host-uuid=<host-uuid> sr-uuid=<sr-uuid> [device-config:key=<corresponding_value>]`	Команда выведет UUID созданного PBD
Уничтожение PBD	`xe pbd-destroy uuid=<pbd-uuid>`	
Подключение PBD к серверу	`xe pbd-plug uuid=<pbd-uuid>`	Если команда выполнена успешно, хранилище (и содержащиеся в нем VDI) станет видимым для сервера
Отключение PBD от сервера	`xe pbd-unplug uuid=<pbd-uuid>`	

© 2025 Нума Технологии, ООО

7.5.5. Команды управления PIF

Команды для работы с PIF (объектами, представляющими физические сетевые интерфейсы).

Действие	Команда	Примечание
Список объектов PIF	`xe pif-list`	
Уничтожение указанного PIF на определенном сервере	`xe pif-forget uuid=<pif-uuid>`	
Создание объекта PIF на сервере	`xe pif-introduce host-uuid=<host_uuid> mac=<mac_address_for_pif> device=<interface_name>`	
Запуск физического интерфейса	`xe pif-plug uuid=<pif-uuid>`	
Вывести из строя физический интерфейс	`xe pif-unplug uuid=<pif-uuid>`	
Сканирование на наличие новых физических интерфейсов на сервере	`xe pif-scan host-uuid=<host-uuid>`	
Изменение IPv6-адреса на PIF	`xe pif-reconfigure-ipv6 uuid=<uuid_of_pif> [mode=dhcp|mode=static] [gateway=<network_gateway_address>] [IPv6=<static_ip_for_this_pif>] [DNS=<dns_address>]`	
Изменение IPv4-адреса на PIF	`xe pif-reconfigure-ip uuid=<uuid_of_pif> [mode=dhcp|mode=static] gateway=<network_gateway_address> IP=<static_ip_for_this_pif> netmask=<netmask_for_this_pif> [DNS=dns_address]`	Для статической конфигурации IP установите для параметра `mode` значение `static`, и заполните параметры `gateway`, `IP` и `netmask`. Чтобы использовать DHCP, установите для параметра `mode` значение `dhcp` и оставьте статические параметры незаполненными. Пример настройки статического IP-адреса: `xe pif-reconfigure-ip uuid=<pif-uuid> mode=static IP=192.168.1.1 gateway=192.168.1.254 netmask=255.255.255.0 DNS=8.8.4.4` Пример настройки DHCP: `xe pif-reconfigure-ip uuid=<pif-uuid> mode=dhcp`

7.5.6. Команды управления пулом

Пул — это совокупность одного или нескольких серверов Numa vServer. Пул использует один или несколько общих хранилищ, чтобы виртуальные машины, работающие на одном сервере в пуле, можно было мигрировать практически в реальном времени на другой сервер в пуле. Эта миграция происходит, пока виртуальная машина все еще работает, без необходимости ее выключения и повторного запуска.

Каждый сервер на самом деле является пулом, состоящим из одного сервера по умолчанию. Он же будет являться и мастером пула. Когда к пулу присоединяется еще один сервер, он назначается подчиненным сервером.

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
Просмотр сведений о пуле	`xe pool-list`	
Назначение нового мастера пула	`xe pool-designate-new-master host-uuid=<uuid_of_new_master>`	Эта команда выполняет упорядоченную передачу роли мастера пула другому серверу в пуле. Эта команда работает только тогда, когда текущий мастер пула находится в сети. Она не заменяет команды аварийного режима, перечисленные ниже
Сброс IP-адреса мастера пула на новое значение через подчиненный сервер и попытка подключения к нему	`xe pool-emergency-reset-master master-address=<ip-address_of_pool_master>`	Внимание! Не запускайте данную команду на мастере пула.
Назначение сервера Numa vServer мастером пула при переходе текущего мастера пула в аварийный режим (с ним нельзя связаться после нескольких повторных попыток)	`xe pool-emergency-transition-to-master`	Если пароль сервера был изменен с момента присоединения к пулу, эта команда может привести к сбросу пароля сервера
Сброс IP-адреса подчиненных серверов в пуле, которые в данный момент работают в аварийном режиме	`xe pool-recover-slaves`	Эта команда обычно используется после назначения нового мастера пула с помощью команды `xe pool-emergency-transition-to-master`
Отключение внешней аутентификации на всех серверах в пуле	`xe pool-disable-external-auth [uuid=uuid] [config=config]`	
Включение внешней аутентификации на всех серверах в пуле	`xe pool-enable-external-auth auth-type=<auth_type> service-name=<service_name> config:user=<username> config:pass=<password>`	
Вывод указанного сервера из пула	`xe pool-eject host-uuid=<uuid_of_host_to_eject>`	
Присоединение сервера к пулу	`xe pool-join master-address=<ip-address> master-username=<username> master-password=<password>`	
Включение механизма обеспечения высокой доступности в пуле	`xe pool-ha-enable heartbeat-sr-uuids=<sr-uuid> ha-config:timeout=<время-в-секундах>`	Где `heartbeat-sr-uuids` – UUID общего хранилища
Отключение механизма обеспечения высокой доступности в пуле	`xe pool-ha-disable`	
Расчет максимально допустимого количества отказов сервера с использованием указанных ВМ и их приоритета запуска	`xe pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=vm_uuid] [restart-priority=restart_priority]`	Где `restart-priority` может принимать следующие значения: • restart: запуск ВМ до тех пор, пока она не включится • best-effort: 1 попытка запуска ВМ после запуска всех ВМ с приоритетом restart
Расчет максимально допустимого количества отказов сервера при текущей конфигурации пула	`xe pool-ha-compute-max-host-failures-to-tolerate`	

© 2025 Нума Технологии, ООО

7.5.7. Команды управления снимками состояния (снапшотами)

Действие	Команда	Примечание
Создание нового снимка путем клонирования существующего снимка состояния	`xe snapshot-clone new-name-label=<name_label> uuid=<snapshot-uuid> [new-name-description=<description>]`	Созданный снимок будет располагаться на том же хранилище
Создание нового снимка путем копирования существующего снимка состояния	`xe snapshot-copy new-name-label=name_label uuid=<snapshot-uuid> [new-name-description=<name_description>] [sr-uuid=<sr_uuid>]`	Образы дисков скопированной виртуальной машины гарантированно будут «полными образами», т.е. не будут частью цепочки CoW
Уничтожение снимка состояния	`xe snapshot-destroy [uuid=uuid] [snapshot-uuid=snapshot_uuid]`	Эта команда оставляет хранилище, связанное со снимком, нетронутым. Чтобы удалить хранилище, используйте `xe snapshot-uninstall`
Вывод списка дисков снимков состояния	`xe snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-params=vbd_params] [vdi-params=vdi_params]`	
Экспорт снимка состояния в шаблон ВМ	`xe snapshot-export-to-template filename=file_name snapshot-uuid=snapshot_uuid [preserve-power-state=true|false]`	
Возврат ВМ к предыдущему состоянию или снимку	`xe snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]`	
Удаление снимка состояния	`xe snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]`	Эта операция уничтожит те VDI, которые помечены как RW и подключены только к этому снимку. Чтобы просто удалить снимок ВМ, используйте `xe snapshot-destroy`

7.5.8. Команды управления хранилищами

Действие	Команда	Примечание
Вывод списка хранилищ	`xe sr-list`	
Создание хранилища	`xe sr-create name-label=<sr-name> physical-size=<size-in-bytes> type=<sr-type> content-type=<content_type> device-config:config_name=<value> [host-uuid=<host_uuid>] [shared=true|false]`	Данная команда создает хранилище на диске, вводит его в базу данных и создает PBD для подключения хранилища к серверу Numa vServer. При указании для параметра `shared` значения `true` PBD создается на каждом сервере в пуле. При указании для параметра `shared` значения `false` PBD создается только на сервере, UUID которого был указан в параметре `host-uuid`. Значение параметра `device_config` различается в зависимости от типа хранилища (`type`).
Уничтожение хранилища	`xe sr-destroy uuid=<sr_uuid>`	

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
Сканирование хранилища	`xe sr-probe type=<sr-type> [host-uuid=<host_uuid>] [device-config:config_name=<value>]`	
Принудительное сканирование хранилища	`xe sr-scan uuid=<sr_uuid>`	

7.5.9. Команды управления субъектами доступа

Действие	Команда	Примечание
Добавление пользователя в список субъектов доступа, которые могут получить доступ к пулу	`xe subject-add subject-name=<subject_name>`	
Удаление пользователя из списка субъектов доступа, которые имеют доступ к пулу	`xe subject-remove subject-uuid=<uuid>`	
Присвоение роли субъекту доступа	`xe subject-role-add uuid=<subject-uuid> [role-name=<role_name>] [role-uuid=<role_uuid>]`	
Удаление роли субъекта доступа	`xe subject-role-remove uuid=<subject-uuid> [role-name=<role_name>] [role-uuid=<role_uuid>]`	

7.5.10. Команды управления задачами

Команды для работы с длительными асинхронными задачами. Эти команды представляют собой такие задачи, как запуск, остановка и приостановка виртуальной машины. Задачи обычно состоят из набора других атомарных подзадач, которые вместе выполняют запрошенную операцию.

Действие	Команда	Примечание
Вывод списка задач	`xe task-list`	
Отмена выполнения задачи	`xe task-cancel uuid=<task-uuid>`	

7.5.11. Команды управления шаблонами ВМ

Шаблоны по сути являются ВМ, параметр `is-a-template` которой имеет значение `true`. Шаблон — это эталонный образ, содержащий все различные параметры конфигурации для создания экземпляра конкретной виртуальной машины.

Numa vServer содержит базовый набор шаблонов, которые являются сырыми ВМ, для развертывания которых необходимо загрузить установочный образ ОС. Также есть возможность создать ВМ, настроить их для ваших конкретных нужд и сохранить их копии в качестве шаблонов для будущего использования при развертывании ВМ.

> **Примечание**
>
> Шаблон нельзя напрямую преобразовать в ВМ, установив параметр `is-a-template` в значение `false`. Установка для параметра `is-a-template` значения `false` не поддерживается и приводит к невозможности запуска ВМ.

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
Вывод списка шаблонов в Numa vServer	`xe template-list`	
Преобразование ВМ в шаблон	`xe vm-param-set uuid=<vm-uuid> is-a-template=true`	
Экспорт копии указанного шаблона в файл	`xe template-export template-uuid=<uuid_of_existing_template> filename=<filename_for_new_template>`	
Удаление пользовательского шаблона	`xe template-uninstall template-uuid=<template_uuid> [--force]`	Эта команда уничтожит те VDI, которые помечены как «принадлежащие» этому шаблону

7.5.12. Команды управления VBD

Команды для работы с виртуальными блочными устройствами.

VBD — это программный объект, который соединяет ВМ с VDI, представляющим содержимое виртуального диска. VBD имеет атрибуты, которые связывают VDI с ВМ (загрузочный ли он, его метрики чтения/записи и т. д.). VDI имеет информацию о физических атрибутах виртуального диска (какой тип хранилища, является ли диск общим, является ли носитель доступным для чтения/записи или только для чтения и т. д.).

Действие	Команда	Примечание
Вывод списка VBD и их параметров	`xe vbd-list`	
Создание VBD на виртуальной машине	`xe vbd-create vm-uuid=<uuid_of_the_vm> device=<device_value> vdi-uuid=<uuid_of_vdi_to_connect_to> [bootable=true] [type=Disk|CD] [mode=RW|RO]`	Допустимые значения для `device` — целые числа от 0 до 15. Указанное число должно быть уникальным для каждой виртуальной машины. Текущие допустимые значения можно увидеть в параметре `allowed-VBD-devices` на указанной виртуальной машине. Это рассматривается как `userdevice` в параметре `vbd`. Если `type` является `Disk`, потребуется `vdi-uuid`. Для диска параметр `mode` может быть в значении `RO` или `RW`. Если `type` является `CD`, указывать `vdi-uuid` необязательно. Если UUID VDI не указан, для CD создается пустой VBD. Для компакт-диска (CD) параметр `mode` должен быть в значении `RO`
Уничтожение VBD	`xe vbd-destroy uuid=<uuid_of_vbd>`	Если VBD имеет параметр `other-config:owner` в значении `true`, соответствующий VDI также уничтожается.
Извлечение носителя из привода	`xe vbd-eject uuid=<uuid_of_vbd>`	Эта команда работает только в том случае, если носитель является съемным (физический CD или ISO). В противном случае появится сообщение об ошибке `VBD_NOT_REMOVABLE_MEDIA`
Подключение нового носителя в привод	`xe vbd-insert uuid=<uuid_of_vbd> vdi-uuid=<uuid_of_vdi_containing_media>`	Эта команда работает только в том случае, если носитель является съемным (физический CD или ISO). В противном случае появится сообщение об ошибке `VBD_NOT_REMOVABLE_MEDIA`
Попытка подключения VBD при включенном ВМ	`xe vbd-plug uuid=<uuid_of_vbd>`	
Попытка отсоединения VBD от	`xe vbd-unplug uuid=<uuid_of_vbd>`	

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
ВМ, находящегося во включенном состоянии		

7.5.13. Команды управления VDI

Команды для работы с образами виртуальных дисков.

VDI — это программный объект, представляющий содержимое виртуального диска, видимого виртуальной машиной. VDI отличается от VBD, который является объектом, связывающим виртуальную машину с VDI. VDI содержит информацию о физических атрибутах виртуального диска (какой тип хранилища, является ли диск общим, является ли носитель доступным для чтения/записи или только для чтения и т. д.). VBD содержит атрибуты, связывающие VDI с виртуальной машиной (загрузочный ли он, его метрики чтения/записи и т. д.).

Действие	Команда	Примечание
Вывод списка VDI и их параметров	`xe vdi-list`	
Создание новой, записываемой копии VDI, которую можно использовать напрямую	`xe vdi-clone uuid=<vdi-uuid>`	Это вариант `vdi-copy`, который может предоставить высокоскоростные возможности клонирования образа там, где они существуют
Копирование VDI в указанное хранилище	`xe vdi-copy uuid=<vdi-uuid> sr-uuid=<uuid_of_the_destination_sr>`	
Создание VDI	`xe vdi-create sr-uuid=<uuid_of_sr_to_create_vdi_on> name-label=<name_for_the_vdi> type=system|user|suspend|crashdump virtual-size=<size_of_virtual_disk> sm-config-\*=storage_specific_configuration_data`	Параметр `virtual-size` может быть указан в байтах или с использованием стандартных суффиксов KiB, MiB, GiB и TiB. Примечание. Типы хранилищ, которые поддерживают тонкое выделение дисков (например, Local VHD и NFS), не обеспечивают виртуальное распределение дисков. Будьте очень осторожны при избыточном выделении виртуального дискового пространства на хранилище. Если избыточно выделенное хранилище заполняется, дисковое пространство должно быть доступно либо на целевом хранилище, либо путем удаления неиспользуемых VDI в хранилище. Некоторые типы хранилищ могут округлить значение параметра `virtual-size`, чтобы сделать его делимым на настроенный размер блока
Уничтожение VDI	`xe vdi-destroy uuid=<vdi-uuid>`	Если вы используете отслеживание измененных блоков для создания инкрементных резервных копий VDI, убедитесь, что вы используете команду `vdi-data-destroy` для удаления снимков, но сохранения метаданных. Не используйте `vdi-destroy` на снимках VDI, в которых включено отслеживание измененных блоков. Для типов Local VHD и NFS SR дисковое пространство не освобождается немедленно `vdi-destroy`, но периодически во время операции сканирования хранилища. Если вам необходимо принудительно сделать удаленное дисковое пространство доступным, вызовите `sr-scan` вручную.

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
Экспорт VDI	`xe vdi-export uuid=<vdi-uuid> filename=<filename_to_export_to> [format=format] [base=uuid_of_base_vdi] [--progress]`	Вы можете экспортировать VDI в одном из следующих форматов: • raw • vhd Формат VHD может быть разреженным. Если в VDI есть нераспределенные блоки, эти блоки могут быть исключены из файла VHD, что сделает файл VHD меньше. Вы можете экспортировать в формат VHD из всех поддерживаемых типов хранилищ на основе VHD (EXT3/EXT4, NFS). Если вы укажете параметр `base`, эта команда экспортирует только те блоки, которые изменились между экспортированным VDI и базовым VDI.
Удаление записи VDI из базы данных, не удаляя его из хранилища	`xe vdi-forget uuid=<vdi-uuid>`	Для полноценного удаления используйте команду `vdi-destroy`.
Импорт VDI	`xe vdi-import uuid=<vdi-uuid> filename=<filename_to_import_from> [format=format] [--progress]`	Вы можете экспортировать VDI в одном из следующих форматов: • raw • vhd
Изменение размера VDI	`xe vdi-resize uuid=<vdi-uuid> disk-size=<new_size_for_disk>`	Параметр `disk-size` может быть указан в байтах или с использованием стандартных суффиксов KiB, MiB, GiB и TiB
Создание версии VDI для чтения и записи, которую можно использовать для создания шаблона	`xe vdi-snapshot uuid=<vdi-uuid> [driver-params=params]`	Шаблон можно создать с использованием любых VDI

7.5.14. Команды управления VLAN

Команды для работы с VLAN (виртуальными сетями). Чтобы вывести список и изменить виртуальные интерфейсы, обратитесь к командам PIF, которые имеют параметр `VLAN`, указывающий на то, что у них есть связанная виртуальная сеть.

Действие	Команда	Примечание
Вывод списка VLAN	`xe vlan-list`	
Создание VLAN на сервере	`xe vlan-create pif-uuid=<pif-uuid> vlan=<vlan-number> network-uuid=<network-uuid>`	
Создание VLAN на всех серверах пула	`xe pool-vlan-create pif-uuid=<pif-uuid> vlan=<vlan-number> network-uuid=<network-uuid>`	Создание VLAN на всех серверах пула с определением интерфейса (например, eth0), на котором будет находиться сеть (на каждом сервере), а затем создав и подключив новый объект PIF к каждому серверу соответственно
Удаление VLAN	`xe vlan-destroy uuid=<uuid_of_pif_mapped_to_vlan>`	Требуется указать UUID PIF, который представляеет VLAN

© 2025 Нума Технологии, ООО

7.5.15. Команды управления VIF

Команды для работы с VIF (виртуальными сетевыми интерфейсами).

Действие	Команда	Примечание
Просмотр списка VIF	`xe vif-list`	
Создание VIF на ВМ	`xe vif-create vm-uuid=<uuid_of_the_vm> device=<device-value> network-uuid=<uuid_of_network_to_connect_to> [mac=<mac_address>]`	Допустимые значения для `device` — целые числа
Уничтожение VIF	`xe vif-destroy uuid=<vif-uuid>`	
Перенос VIF на другую сеть	`xe vif-move uuid=<vif-uuid> network-uuid=<network-uuid>`	
Подключение VIF к работающей ВМ	`xe vif-plug uuid=<vif-uuid>`	
Отключение VIF от работающей ВМ.	`xe vif-unplug uuid=<vif-uuid>`	
Настройка конфигурации IPv4 для VIF. Настройка static VIF	`xe vif-configure-ipv4 uuid=<vif-uuid> mode=static address=<CIDR_address> gateway=<gateway_address>`	
Настройка конфигурации IPv4 для VIF. Очистка конфигурации IPv4	`xe vif-configure-ipv4 uuid=<vif-uuid> mode=none`	
Настройка конфигурации IPv6 для VIF. Настройка static VIF	`xe vif-configure-ipv6 uuid=<vif-uuid> mode=static address=<IP_address> gateway=<gateway_address>`	
Настройка конфигурации IPv6 для VIF. Очистка конфигурации IPv6	`xe vif-configure-ipv6 uuid=<vif-uuid> mode=none`	

7.5.16. Команды управления ВМ

В данном разделе описаны базовые команды для управления виртуальными машинами (ВМ).

Действие	Команда	Примечание
Действия с ВМ		
Создание ВМ (импорт)	`xe vm-import filename=<filename.xva>`	Создание ВМ путем импорта файла-образа ВМ с расширением ova или xva. Данная команда создает ВМ на локальном хранилище сервера. Для выбора другого хранилища используйте параметр sr-uuid с указанием uuid необходимого хранилища
Создание ВМ (из установочного образа)	`xe vm-install new-name-label=<vm-name> template=<template-name>`	Создание ВМ из установочного образа. Процесс создания ВМ из установочного образа описан в разделе Установка виртуальной машины
Удаление ВМ (destroy)	`xe vm-destroy uuid=<vm-uuid>`	Удаление ВМ. VDI ВМ не будет удален
Удаление ВМ (uninstall)	`xe vm-uninstall vm=<vm-name>`	Полное удаление ВМ, включая ее VDI. Необходимо подтверждение удаления ВМ и VDI
Копирование ВМ	`xe vm-copy vm=<vm-name> new-name-label=<vm-copy-name>`	Создание полной копии ВМ с возможностью выбора целевого хранилища.

© 2025 Нума Технологии, ООО

Действие	Команда	Примечание
		Для выбора целевого хранилища используйте параметр sr-uuid с указанием uuid необходимого хранилища
Клонирование ВМ	`xe vm-clone vm=<vm-name> new-name-label=<vm-clone-name>`	Создание клона ВМ на том же хранилище, на котором расположена исходная ВМ
Миграция ВМ	`xe vm-migrate vm=<vm-name> host=<host-name>`	Выполнение миграции ВМ на другой физический сервер. Миграция предназначена для переноса ВМ между серверами с сохранением всех настроек и параметров
Создание снимка состояния (снапшота) ВМ	`xe vm-snapshot vm=<vm-name> new-name-label=<snapshot-name>`	Снимок будет создан на том же хранилище, на котором расположена исходная ВМ
Управление состоянием ВМ		
Запуск ВМ	`xe vm-start vm=<vm-name>`	
Выключение ВМ	`xe vm-shutdown vm=<vm-name>`	
Перезагрузка ВМ	`xe vm-reboot vm=<vm-name>`	
Приостановка ВМ (suspend)	`xe vm-suspend vm=<vm-name>`	Приостановка ВМ с сохранением текущей памяти, состояния процессора, запущенных приложений и с освобождением используемых ресурсов. Возобновление работы ВМ требует некоторое время
Возобновление работы ВМ (из состояния suspend)	`xe vm-resume vm=<vm-name>`	
Приостановка ВМ (pause)	`xe vm-pause vm=<vm-name>`	Приостановка ВМ без сохранения ее состояния на диск, ресурсы не освобождаются. Работа ВМ может быть быстро возобновлена.
Возобновление работы ВМ (из состояния pause)	`xe vm-unpause vm=<vm-name>`	
Управление параметрами ВМ		
Просмотр всех параметров ВМ	`xe vm-param-list uuid=<vm-uuid>`	Вывод списка текущих параметров указанной ВМ
Задание параметра	`xe vm-param-set uuid=<vm-uuid> <param-name>=<value>`	Задание нового значения параметра ВМ
Очистка параметра	`xe vm-param-clear param-name=<param-name> uuid=<vm-uuid>`	Удаление значения параметра ВМ
Удаление параметра	`xe vm-param-remove param-name=<param-name> uuid=<vm-uuid> param-key=<key>`	Удаление существующего параметра ВМ и его значения. У каждой ВМ свой набор параметров и ключей. Чтобы посмотреть для конкретной ВМ все `param-key` нужно либо вывести все параметры вм командой `xe vm-param-list`, либо конкретный параметр `xe vm-param-get param-name=<param-name>` и посмотреть в выводе ключи для этого параметра.

© 2025 Нума Технологии, ООО

8. Проброс USB-устройств в ВМ

Для настройки сквозного подключения USB-флеш-накопителя в ВМ с помощью Numa vServer выполните следующие действия:

1. Подключите USB-флеш-накопитель к серверу, на котором установлен Numa vServer.
2. Авторизуйтесь в CLI Numa vServer как локальный суперпользователь root.
3. Выполните команду для просмотра подключённых USB-флеш-накопителей:

Команда

```
xe pusb-list
```

Пример вывода

```
[root@localhost:~]# xe pusb-list
uuid ( RO)            : 77b8f209-4171-522d-92a8-3270f171dba5
             path ( RO): 1-10
       vendor-id ( RO): 0781
     vendor-desc ( RO): SanDisk Corp.
       product-id ( RO): 5571
     product-desc ( RO): Cruzer Fit
           serial ( RO): 00017428010822104644
          version ( RO): 2.00
     description ( RO): SanDisk Corp._Cruzer Fit_00017428010822104644

uuid ( RO)            : 50c69bd0-79d3-dd55-e4e6-85dde8501ee9
             path ( RO): 1-6
       vendor-id ( RO): 058f
     vendor-desc ( RO): Alcor Micro Corp.
       product-id ( RO): 3828
     product-desc ( RO):
           serial ( RO):
          version ( RO): 2.00
     description ( RO): Alcor Micro Corp.

uuid ( RO)            : 730d6957-8ba9-6ba8-ff1d-5b3485fcad10
             path ( RO): 1-7
       vendor-id ( RO): 13fe
     vendor-desc ( RO): Kingston Technology Company Inc.
       product-id ( RO): 4300
     product-desc ( RO):
           serial ( RO): 0708236999B4BE80
          version ( RO): 2.00
     description ( RO): Kingston Technology Company Inc._0708236999B4BE80
```

© 2025 Нума Технологии, ООО

4. Выполните команду для включения сквозной передачи для определенного USB-флеш-накопителя:

Команда

```
xe pusb-param-set uuid=<pusb-uuid> passthrough-enabled=true
```

Пример ввода

```
[root@localhost:~]# xe pusb-param-set uuid=77b8f209-4171-522d-92a8-3270f171dba5 passthrough-
enabled=true
```

где `<pusb-uuid>` – UUID USB-флеш-накопителя из пункта 2.

5. Выключите ВМ, для которой необходимо настроить сквозное подключение USB-флеш-накопителя.

> **Внимание!**
>
> Убедитесь, что целевая ВМ выведена из механизма высокой доступности.

6. Узнайте UUID USB-группы, в которую входит подключаемый USB-флеш-накопитель:

Команда

```
xe usb-group-list PUSB-uuids=<pusb-uuid>
```

Пример ввода

```
[root@localhost:~]# xe usb-group-list PUSB-uuids=77b8f209-4171-522d-92a8-3270f171dba5
uuid ( RO)                  : 24b42d83-f89e-476b-d5d6-a92877f9fae7
          name-label ( RW): Group of 0781 5571 USBs
    name-description ( RW):
```

7. Подключите USB-флеш-накопитель к ВМ:

Команда

```
xe vusb-create usb-group-uuid=<usb-group-uuid> vm-uuid=<vm-uuid>
```

Пример вывода

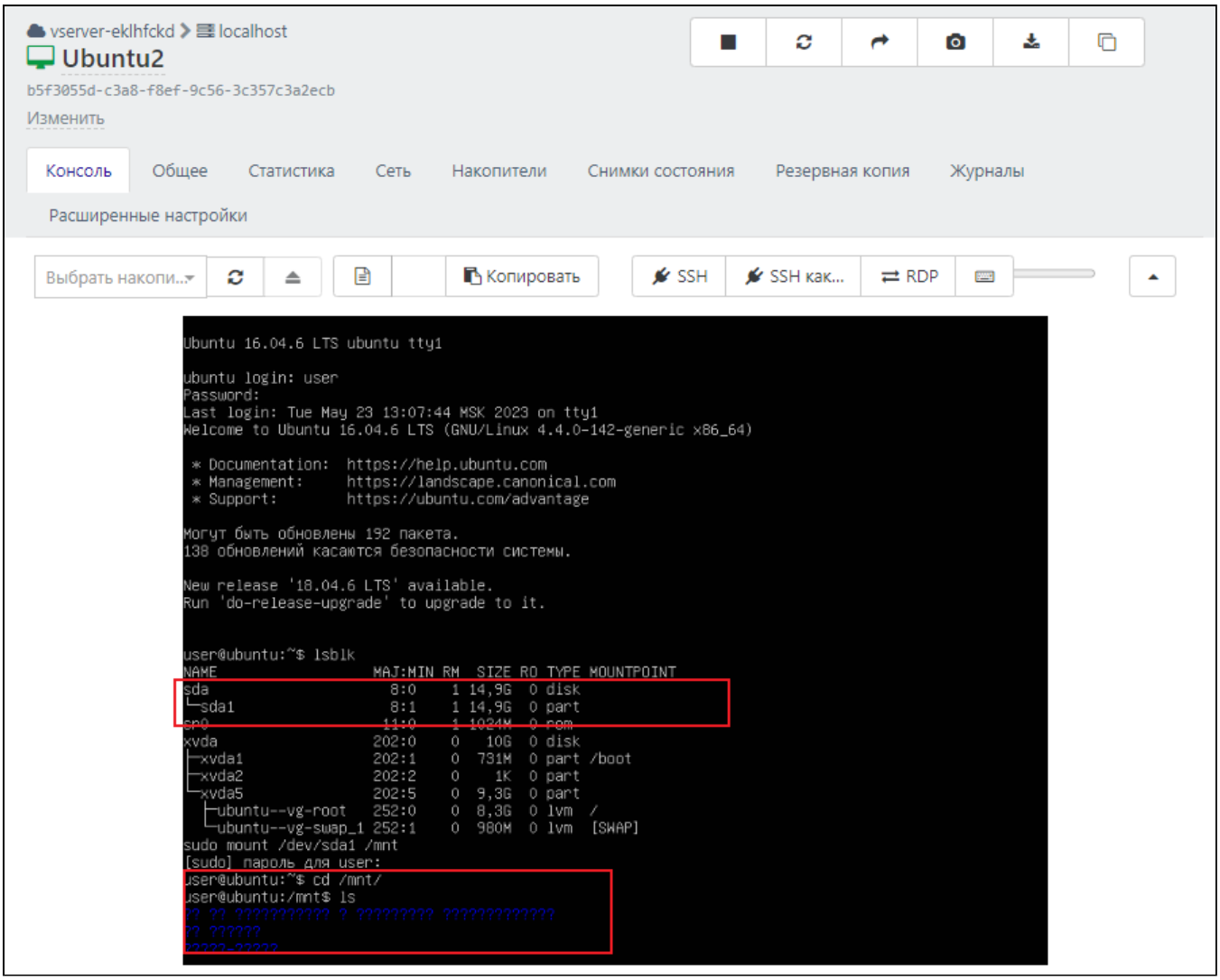
```
[root@localhost:~]# xe vusb-create usb-group-uuid=24b42d83-f89e-476b-d5d6-a92877f9fae7 vm-
uuid=b5f3055d-c3a8-f8ef-9c56-3c357c3a2ecb
d885b152-eb32-cbc7-0c14-ef51b9ae4b9c
```

где:

- `<vm-uuid>` – UUID ВМ, для которой необходимо настроить сквозное подключение USB;
- `<usb-group-uuid>` – UUID USB-группы из пункта 5.

8. Включите ВМ, в консоли выполните команду `lsblk` и убедитесь, что USB-флеш-накопитель подключился:

© 2025 Нума Технологии, ООО



Подтверждение подключения USB в ВМ

> **Примечание**
>
> После выполнения проброса USB-флеш-накопителя для ВМ можно активировать механизм высокой доступности с выбором приоритета best-effort.

> **Внимание!**
>
> Для дальнейшей корректной работы ВМ отключите USB-флеш-накопитель от целевой ВМ. Иначе часть функций, таких как копирование ВМ, снимки состояния и т.п., работать не будут.

9. Для отключения USB-флеш-накопителя от ВМ выполните команду:

```
xe vusb-unplug uuid=<vusb-uuid>
```

где `<vusb-uuid>` – значение, выведенное в пункте 6.

10. Для удаления USB-флеш-накопителя выполните команду:

© 2025 Нума Технологии, ООО

```
xe vusb-destroy uuid=<vusb-uuid>
```

где `<vusb-uuid>` – значение, выведенное в пункте 6.

© 2025 Нума Технологии, ООО

9. Прямой доступ к PCI-устройствам в ВМ

> **Предупреждение**
>
> Для PCI Passthrough подходят видеокарты NVIDIA серии 600 и выше с минимальной версией драйвера R465. При несоблюдении данного условия в Windows будет получена «Ошибка 43».

Для организации прямого доступа к PCI-устройствам в ВМ (Passthrough) выполните следующие действия:

1. Авторизуйтесь в CLI Numa vServer как локальный суперпользователь root.
2. Выведите список PCI-устройств, доступных в сервере.

```
lspci
```

3. Убедитесь, что ВМ, для которой необходимо настроить сквозное подключение PCI-устройства, находится в выключенном состоянии.

Команда

```
xe vm-param-get param-name=power-state uuid=<vm-uuid>
```

Пример вывода

```
[root@vserver:~]# xe vm-param-get param-name=power-state uuid=65270801-93e9-842b-1d4c-
be23a938dc3c
halted
```

4. В конфигурации ВМ укажите адрес устройства, к которому будет осуществлен прямой доступ.

Команда

```
xe vm-param-set other-config:pci=0/000:<pci-id> uuid=<vm-uuid>
```

Пример ввода

```
xe vm-param-set other-config:pci=0/000:00:1f.3 uuid=4533cebc-b07f-3c74-df77-a78373fbcbc5
```

В данном примере `pci-id` = `00:1f.3`, `vm-uuid` = `4533cebc-b07f-3c74-df77-a78373fbcbc5`

5. Включите виртуальную машину.

```
xe vm-start uuid=<vm-uuid>
```

6. Проверьте список устройств, назначенных для прямого доступа из ВМ.

```
xl pci-assignable-list
```

© 2025 Нума Технологии, ООО

7. Проверьте наличие устройства в виртуальной машине:

   • для Linux:

```
lspci
```

   • для Windows: перейдите в «Диспетчер устройств»

> **Примечание**
>
> Для удаления PCI-устройств из виртуальной машины выполните команду:
>
> ```
> xe vm-param-remove param-name=other-config param-key=pci uuid=<vm-uuid>
> ```

© 2025 Нума Технологии, ООО

10. Преобразование и установка образов ВМ

Для преобразования и установки образа ВМ в Numa vServer выполните следующие действия:

1. Подключитесь к Numa vServer и скопируйте необходимый для дальнейшей работы образ ВМ.

2. Преобразуйте образ ВМ в формат VHD:

Команда

```
qemu-img convert -f <image_format_input> -O vpc <input_file.image_format_input> <outputfile.vhd>
```

Пример ввода

```
[root@vserver:~]# qemu-img convert -f vmdk -O vpc ubuntu-18.10-server-cloudimg-amd64.vmdk
ubuntuKs.vhd
```

где

- `<image_format_input>` – формат входного файла согласно таблице:

Тип формата	<image_format_input>
raw	raw
qcow2	qcow2
VDI	vdi
VMDK	vmdk
VHD	vpc
VHDX	vhdx

- `<input_file.image_format_input>` – наименование входного файла (с расширением);
- `<outputfile.vhd>` – наименование итогового файла (с расширением).

© 2025 Нума Технологии, ООО

3. Посмотрите информацию о созданном файле:

Команда

```
qemu-img info <outputfile.vhd>
```

Пример вывода

```
[root@vserver:~]# qemu-img info ubuntuKs.vhd
image: ubuntuKs.vhd
file format: vps
virtual size: 10 GiB (10737893376 bytes)
disk size: 1.12 GiB
cluster_size: 2097152
Child node '/file':
    filename: ubuntuKs.vhd
    protocol type: file
    file length: 1.16 GiB (1250230784 bytes)
    disk size: 1.12 GiB
```

4. Создайте ВМ по шаблону импортируемой ВМ:

```
xe template-list
```

```
xe vm-install template=<template-name> new-name-label=<name_VM>
```

```
xe vif-create vm-uuid=<vm-uuid> network-uuid=<network-uuid> mac=random device=0
```

где

- `<template-name>` указан в параметре `name-label` для команды `xe template-list`;
- `<network-uuid>` можно узнать командой `xe network-list`;
- `<vm-uuid>` можно узнать командой `xe vm-list`.

5. Создайте неразмеченный виртуальный диск:

Команда

```
xe vdi-create name-label=<name_VDI> virtual-size=<vitrual_size_GiB> sr-uuid=<uuid_sr>
```

Пример вывода

```
[root@vserver:~]# xe vdi-create name-label=ubuntuKs virtual-size=12GiB sr-uuid=5df7ebd8-cb45-34ee-
fef7-5bafbf8fe717
df1feba5-6984-4623-8e56-8e4e5c8d9bb4
```

где

- `<name_VDI>` – имя виртуального диска;
- `<vitrual_size_GiB>` – объем создаваемого диска. Указываемый объем должен быть на 15-20% больше, чем планируемый объем импортируемого диска. Указываются также единицы изменения: KiB, MiB, GiB;

© 2025 Нума Технологии, ООО

- `<uuid_sr>` – UUID хранилища, в которое требуется поместить виртуальный диск.

В качестве вывода Numa vServer присвоит созданному VDI UUID.

6. Создайте новый VBD для отображения виртуального диска в ВМ:

Команда

```
xe vbd-create vm-uuid=<uuid_VM> device=1 vdi-uuid=<uuid_VDI> bootable=true type=Disk mode=RW
```

Пример вывода

```
[root@vserver:~]# xe vbd-create vm-uuid=7681fc64-7c32-f046-eac8-1eae3310cfc5 device=1 vdi-
uuid=df1feba5-6984-4623-8e56-8e4e5c8d9bb4 bootable=true type=Disk mode=RW
f94bd2f9-9e43-bb4e-9e57-74c008df772c
```

где

- `<uuid_VM>` – UUID виртуальной машины;
- `<uuid_VDI>` – UUID VDI полученный на предыдущей этапе.

В качестве вывода Numa vServer присвоит созданному VBD UUID.

7. Импортируйте сконвертированный на 1 этапе VDI:

Команда

```
xe vdi-import filename=<outputfile.vhd> format=vhd uuid=<uuid_VDI>
```

Пример ввода

```
[root@vserver:~]# xe vdi-import filename=ubuntuKs.vhd format=vhd
uuid=df1feba5-6984-4623-8e56-8e4e5c8d9bb4
```

где

- `<outputfile.vhd>` – итоговый файл, полученный на этапе 1;
- `<uuid_VDI>` – UUID VDI, полученный на этапе 5.

После чего ВМ будет доступна к запуску и дальнейшей работе.

© 2025 Нума Технологии, ООО

Внимание!

Для корректного запуска ОС семейства Red Hat выполните следующие команды в shell ОС до импорта или в shell ОС в rescue-режиме:

```
yum install dracut-config-generic dracut-network
```

```
dracut --add-drivers xen-blkfront -f /boot/initramfs-$(uname -r).img $(uname -r)
```

В случае дальнейшего использование Legacy:

```
dracut --regenerate-all -f && grub2-mkconfig -o /boot/grub2/grub.cfg
```

При использовании UEFI:

```
dracut --regenerate-all -f && grub2-mkconfig -o /boot/efi/EFI/<your distribution>/grub.cfg
```

© 2025 Нума Технологии, ООО

11. Настройка SNMP в Numa vServer

Перед использованием протокола SNMP в составе Numa vServer выполните следующие действия:

1. Создайте резервную копию snmpd.conf:

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.backup
```

2. В snmpd.conf укажите режим доступа, пароль, перечень IP, у которых будет доступ к данному серверу. Пример:

```
rocommunity public 192.168.1.0/24
rwcommunity private 192.168.1.1
```

3. Откройте порты 161/udp и 162/udp. Для этого пропишите в `/etc/iptables/iptables` следующие строки:

```
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m udp -p udp --dport 161 -j ACCEPT -A
vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m udp -p udp --dport 162 -j ACCEPT
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:vServer-Firewall-0-INPUT - [0:0]
-A INPUT -j vServer-Firewall-0-INPUT
-A FORWARD -j vServer-Firewall-0-INPUT
-A vServer-Firewall-0-INPUT -i lo -j ACCEPT
-A vServer-Firewall-0-INPUT -p icmp --icmp-type any -j ACCEPT
# DHCP for host internal networks (CA-6996)
-A vServer-Firewall-0-INPUT -p udp -m udp --dport 67 --in-interface xenapi -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
# Linux HA hearbeat
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m udp -p udp --dport 694 -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m udp -p udp --dport 161 -j ACCEPT
-A vServer-Firewall-0-INPUT -m conntrack --ctstate NEW -m udp -p udp --dport 162 -j ACCEPT

-A vServer-Firewall-0-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Пример конфигурационного файла

4. Перезапустите сервис iptables:

```
systemctl restart iptables
```

5. Перезапустите сервис snmpd:

© 2025 Нума Технологии, ООО

```
systemctl restart snmpd
```

11.0.1. Подключение сервера с Numa vServer к Zabbix

Для добавления vServer в Zabbix выполните следующие действия:

1. Пройдите авторизацию в веб-оболочке Zabbix-server.
2. В панели навигации нажмите «Monitoring» → «Hosts».
3. На открывшейся странице нажмите «Create host».
4. В открывшейся форме в поле для ввода «Host name» введите имя добавляемого сервера.
5. В поле для ввода «Templates» введите «Linux by SNMP» и кликните на совпадение в выпадающем меню.
6. В поле для ввода «Host groups» введите «Hypervisors» и кликните на совпадение в выпадающем меню.
7. В разделе «Interfaces» кликните на ссылку «Add», во всплывшем меню выберите «SNMP».
8. В поле для ввода «IP address» введите IP-адрес сервера Numa vServer.
9. В поле для ввода «SNMP community» введите пароль, указанный во время настройки SNMP в Numa vServer.
10. Нажмите «Add».

Сервер Numa vServer успешно добавлен.

© 2025 Нума Технологии, ООО

12. Управление журналом событий

12.1. Перечень журналируемых событий

Для просмотра журнала событий безопасности используется утилита journalctl.

Тип события	Расшифровка события
AUDIT_VIRT_CONTROL: pause	Постановка ВМ на паузу
AUDIT_VIRT_CONTROL: unpause	Снятие ВМ с паузы
AUDIT_VIRT_CONTROL: start	Запуск ВМ
AUDIT_VIRT_CONTROL: hard_shutdown	Принудительное выключение ВМ
AUDIT_VIRT_CONTROL: hard_reboot	Принудительная перезагрузка ВМ
AUDIT_VIRT_CONTROL: clean_reboot	Перезагрузка ВМ
AUDIT_VIRT_CONTROL: clean_shutdown	Выключение ВМ
AUDIT_VIRT_CONTROL: suspend	Приостановка ВМ
AUDIT_VIRT_CONTROL: resume	Возобновление работы ВМ после приостановки
AUDIT_VIRT_INTEGRITY_CHECK	Проверка целостности
AUDIT_VIRT_CREATE	Создание ВМ
AUDIT_VIRT_DESTROY	Уничтожение ВМ
AUDIT_VIRT_MIGRATE_IN	Миграция ВМ в хост
AUDIT_VIRT_MIGRATE_OUT	Миграция ВМ из хоста
SERVICE_START	Запуск сервисов
SERVICE_STOP	Остановка сервисов
USER_ROLE_CHANGE	Смена роли пользователя
USER_START	Аутентификация пользователя
USER_LOGIN	Идентификация пользователя

12.2. Просмотр событий безопасности

Просмотр журнала событий производится с помощью утилиты journalctl. Для просмотра определенных событий безопасности используются специальные параметры и ключи.

Ключ	Описание
`-b <номер журнала>`	Вывод журнала из определенной сессии
`-f`	Просмотр событий в режиме реального времени
`--since`	Просмотр событий с определенной даты/времени. Допустимые форматы: `yyyy-mm-dd hh:mm:ss`, `yyyy-mm-dd`, `hh:mm`, `yesterday`, `today`
`--until`	

© 2025 Нума Технологии, ООО

Ключ	Описание
	Просмотр событий до определенной даты/времени. Допустимые форматы: `yyyy-mm-dd hh:mm:ss`, `yyyy-mm-dd`, `hh:mm`, `yesterday`, `today`, `<N> hour ago` и т.д.
`-p <уровень критичности>`	Просмотр событий с определенным уровнем критичности, где `<уровень критичности>` принимает значения от 0 до 7
`-n <количество>`	Вывод последних событий, где `<количество>` - количество выводимых событий

Уровни критичности:

- 0: emergency (неработоспособность системы)
- 1: alerts (предупреждения, требующие немедленного вмешательства)
- 2: critical (критическое состояние)
- 3: errors (ошибки)
- 4: warning (предупреждения)
- 5: notice (уведомления)
- 6: info (информационные сообщения)
- 7: debug (отладочные сообщения)

Просмотр всех событий из определенной сессии

```
journalctl -b <номер журнала>
```

где `<номер журнала>` определяется при выполнении команды `journalctl --list-boots`.

Просмотр списка журналов сессий

Команда

```
journalctl --list-boots
```

Пример вывода

```
[root@vserver:~]# journalctl --list-boots
-3 0701fbd4aebb42a78a73526f2a86a4a8 Thu 2024-03-21 15:23:14 MSK—Fri 2024-03-22 19:01:21 MSK
-2 d39a3f4520da4c82932f72d6f413b9d9 Mon 2024-03-25 13:31:07 MSK—Fri 2024-04-05 19:20:35 MSK
-1 f965e7161502442eb2f59240e51b0801 Mon 2024-04-08 10:27:17 MSK—Fri 2024-04-12 19:13:42 MSK
0 02fd52b6ac92479e8784f0a6cbad32a5 Wed 2024-04-17 18:44:30 MSK—Fri 2024-04-19 10:36:03 MSK
```

где первый номер показывает номер журнала, а второй номер - boot ID - уникальный идентификатор журнала, который также можно использовать для вывода журнала.

12.3. Фильтрация событий безопасности

Для фильтрации событий безопасности используется параметр grep:

Запуск сервиса

```
journalctl | grep SERVICE_START
```

Остановка сервиса

© 2025 Нума Технологии, ООО

```
journalctl | grep SERVICE_STOP
```

Запуск ВМ

```
journalctl | grep "VIRT_CONTROL.*start"
```

Неуспешный запуск

```
journalctl | grep "VIRT_CONTROL.*start.*failed"
```

Запуск определенной ВМ

```
journalctl | grep "VIRT_CONTROL.*start.*<vm-uuid>"
```

где `<vm-uuid>` – это uuid ВМ, который можно узнать командой `xe vm-list`

Завершение работы ВМ

```
journalctl | grep "VIRT_CONTROL.*shutdown"
```

Успешные попытки:

```
journalctl | grep "VIRT_CONTROL.*clean_shutdown.*success"
```

Определенная ВМ:

```
journalctl | grep "VIRT_CONTROL.*clean_shutdown.*<vm-uuid>"
```

где `<vm-uuid>` – это uuid ВМ, который можно узнать командой `xe vm-list`

"Чистое" завершение работы

Вариант 1

```
journalctl | grep "VIRT_CONTROL.*clean_shutdown"
```

Вариант 2

```
journalctl | grep "VM.clean_shutdown.*audit"
```

Принудительное завершение работы

Вариант 1

```
journalctl | grep "VIRT_CONTROL.*hard_shutdown"
```

Вариант 2

```
journalctl | grep "VM.hard_shutdown.*audit"
```

© 2025 Нума Технологии, ООО

Поставнока ВМ на паузу

```
journalctl | grep "VM.pause.*audit"
```

Снятие ВМ с паузы

```
journalctl | grep "VM.unpause.*audit"
```

Приостановка ВМ

```
journalctl | grep "VM.suspend.*audit"
```

Возобновление работы ВМ после приостановки

```
journalctl | grep "VM.resume.*audit"
```

Перезагрузка ВМ

Вариант 1

```
journalctl | grep "VIRT_CONTROL.*VM.clean_reboot"
```

Вариант 2

```
journalctl | grep "VM.clean_reboot.*audit"
```

Принудительная перезагрузка

Вариант 1

```
journalctl | grep "VIRT_CONTROL.*VM.hard_reboot"
```

Вариант 2

```
journalctl | grep "VM.hard_reboot.*audit"
```

Импорт ВМ

Импорт ВМ фиксируется как событие создания ВМ.

Экспорт ВМ

```
journalctl | grep VM.*export
```

Клонирование ВМ

```
journalctl | grep "VIRT_CREATE.*VM.clone"
```

Создание субъекта доступа

© 2025 Нума Технологии, ООО

```
journalctl | grep subject.create
```

Удаление субъекта доступа

```
journalctl | grep subject.destroy
```

Доступ субъектов доступа к УВМ

```
journalctl -b 0 | grep USER_LOGIN
```

```
journalctl | grep USER_AUTH
```

Успешный доступ

```
journalctl | grep "USER_LOGIN.*success"
```

```
journalctl | grep "USER_AUTH.*success"
```

Неуспешный доступ

```
journalctl | grep "USER_LOGIN.*failed"
```

```
journalctl | grep "USER_AUTH.*failed"
```

Доступ определенного субъекта доступа к УВМ

```
journalctl | grep "USER_LOGIN.*user"
```

Доступ по ssh

```
journalctl | grep "USER_LOGIN.*ssh"
```

Неуспешная попытка доступа по ssh (неправильный логин)

```
journalctl | grep "sshd.*invalid"
```

Создание ВМ

```
journalctl | grep "VIRT_CREATE.*VM.create"
```

Удаление ВМ

```
journalctl | grep VIRT_DESTROY
```

Копирование ВМ

```
journalctl | grep "VIRT_CREATE.*VM.copy"
```

© 2025 Нума Технологии, ООО

Управление ролями пользователей (присвоение/удаление/изменение)

```
journalctl | grep 'role.*add' && journalctl -b | grep 'role.\*remove'
```

Контроль целостности объектов контроля (VDI ВМ)

```
journalctl | grep VIRT_INTEGRITY_CHECK
```

Успешный контроль целостности

```
journalctl | grep "VIRT_INTEGRITY_CHECK.*success"
```

Неуспешный контроль целостности

```
journalctl | grep "VIRT_INTEGRITY_CHECK.*failed"
```

Обновление КС VDI ВМ

```
journalctl | grep VDI.update_checksum
```

Создание снапшота

```
journalctl | grep VM.snapshot
```

Миграция ВМ на другой сервер

```
journalctl | grep VIRT_MIGRATE_OUT
```

Миграция ВМ с другого сервера

```
journalctl | grep VIRT_MIGRATE_IN
```

Создание хранилища

```
journalctl | grep sr.create
```

12.4. Удаление журнала событий

Удалить журналы, оставив только последние 100 Мб:

```
journalctl --vacuum-size=100M
```

Удалить журналы, оставив журналы только за последние 7 дней:

```
journalctl --vacuum-time=7d
```

© 2025 Нума Технологии, ООО

12.5. Экспорт журнала событий

1. Выполните команду по выгрузке журнала в файл. Пример выгрузки:

```
journalctl [ключи|параметры] > journal.log
```

2. Подключите и смонтируйте USB-Flash-накопитель к устройству, на которое установлен Numa vServer.
3. Скопируйте полученный файл на USB-Flash-накопитель.

12.6. Контроль целостности журнала событий

Для обеспечения проверки целостности журнала аудита:

1. Сгенерируйте пару ключей для подписи журнала аудита.

```
journalctl --setup-key
```

   Команда выведет значение секретного ключа.

2. Проверьте целостность журнала.

```
journalctl --verify --verify-key '<значение секретного ключа>'
```

© 2025 Нума Технологии, ООО