Лаборатория 50
http://лаб50.рф

КЛАСТЕР ВЫСОКОЙ ГОТОВНОСТИ

Кластер высокой готовности предназначен для обеспечения непрерывной доступности прикладных приложений и сервисов. При отказе любого сервиса или узла целиком кластер высокой готовности автоматически перезапустит сервис на работающем узле с минимальным прерыванием для клиентов кластера.

Кластер высокой готовности гарантирует целостность данных при переносе пользовательских сервисов с одного узла кластера на другой. В случае необходимости, для предотвращения порчи данных, отказавшие узлы будут автоматически исключены из кластера.

Максимальный размер одного кластера — 16 узлов. Узлы могут быть либо виртуальными машинами, либо работать на физическом оборудовании.

Поддерживаемые приложения, сервисы и ресурсы:

- Стандартные службы LSB
- Веб-сервер Apache
- Реплицируемые тома DRBD
- Интерфейсы Ethernet
- IP-адреса
- Тома iSCSI
- СУБД PostgreSQL, MySQL
- Серверы и тома NFS
- Почтовые сервер Postfix
- Сервер приложений Tomcat
- ...

Защищённые системы

Кластер высокой готовности предназначен для построения защищённых отказоустойчивых программно-аппаратных комплексов, соответствующих требованиям ФСТЭК для автоматизированных систем, обрабатывающих конфиденциальную информацию и данные до уровня «совершенно секретно». Кластер совместно с сертифицированной операционной системой образует комплекс, удовлетворяющий следующим требованиям ФСТЭК и Минобороны России:

1) контроль отсутствия НДВ до уровня 2;

2) класс защищённости от НСД к информации до 1Б.

Область применения

- Обеспечение постоянной доступности критически важным приложениям, работающим на физических или виртуальных узлах, независимо от каких-либо программных или аппаратных сбоев.
- Требуется постоянная доступность услуг и прерывание услуг не допустимо.
- Необходимо защитить общее хранилище от повреждения данных при сбоях.
- Система функционирует автономно, нет возможности быстрого вмешательства для устранения неполадок.

Основные возможности

- Возможность работы с общим хранилищем данных и без него.
- Управление кластером из веб-панели или командной строки.
- Поддержка практически любых типов приложений и сервисов.
- Широкой диапазон схем конфигурации избыточности ресурсов.
- Фенсинг (процесс защиты разделяемых ресурсов).
- Поддержка кворума (решающего большинства).
- Задание различных вариантов зависимостей между ресурсами.
- Автоматизированная установка и настройка.
- Обнаружение и восстановление после сбоев аппаратных средств и программного обеспечения.

КОМПОНЕНТЫ

Основу кластера высокой готовности составляет система управления кластером, панель управления для администратора, набор агентов для поддержки приложений и сервисов и система управления конфигурацией.

Система управления кластером определяет отказы программных или аппаратных средств и немедленно осуществляет перезапуск приложения или систем без вмешательства оператора. Такой процесс называется преодолением отказа. В процессе преодоления отказа кластер может производить подготовку узла для запуска на нем приложения. Например, подключать общее хранилище, настраивать сетевые интерфейсы, запускать требуемые вспомогательные службы.

Требования

Процессор Intel x86-64 Xeon

Оперативная память 16 Гб

4 сетевых порта 1 и 10 Гбит/с

До 60 дисков SAS или SATA

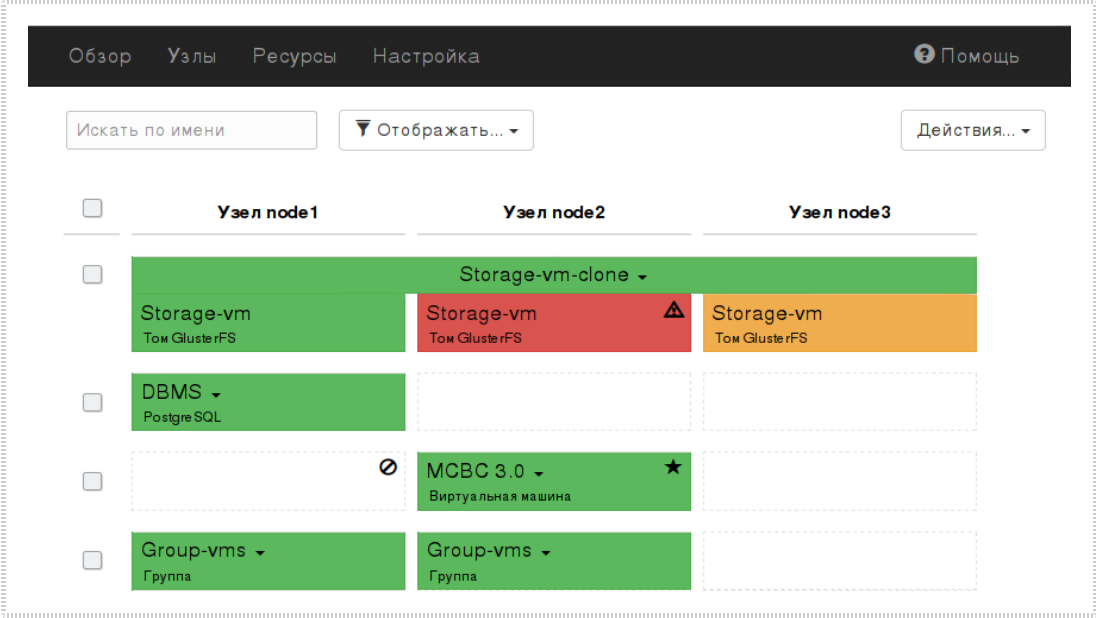
RAID контроллер с поддержкой RAID-6 и RAID-1+0

Важнейшей особенностью кластера высокой готовности является способность обрабатывать состояние расщепления (split-brain), которое возникает при потере связи между частями кластера. Если это произойдет, любой узел в кластере может ошибочно решить, что произошел отказ другого узла и попытается запустить сервисы, которые по-прежнему работают. В этом случае система управления кластером определит проблемные узлы и попытается устранить отказы.

Как и любая вычислительная система, кластер высокой готовности должен включать оборудование питания, вычислительные узлы, сетевое оборудование. Для достижения высокой готовности программно-аппаратного комплекса требуется специальная конфигурация аппаратных средств, обеспечивающая отказоустойчивость каждой из подсистем кластера.

В основе системы управления кластером лежит программное обеспечение Pacemaker и Corosync.

Веб-панель управления предоставляет администраторам все основные функции по управлению кластером: контроль состояния и управление узлами, виртуальными машинами, кластерной файловой системой и другими ресурсами кластера высокой готовности. Архитектура панели спроектирована без единой точки отказа и не зависит от внешних СУБД или разделяемых хранилищ. Панель управления доступна при наличии хотя бы одного исправного узла в кластере. Помимо веб-панели предоставляется традиционный интерфейс командной строки для управления кластером.



Возможности

Объектный доступ позволяет получить доступ хранилищу посредством API

Георепликация между площадками позволяет повысить надежность хранения

Избыточное кодирование для восстановления или исправления поврежденных данных

Многоярусное хранение — автоматический перенос данных между быстрыми и медленными носителями

Кластерная файловая система

Необходима для создания общих хранилищ данных, в том числе конфиденциальных или содержащих гостайну.

В основе кластерной файловой системы лежит GlusterFS, доработанная для поддержки мандатного разграничения доступа.

GlusterFS — это распределённая параллельная линейно-масштабируемая файловая система с возможностью защиты от сбоев. С помощью InfiniBand RDMA или TCP/IP GlusterFS может объединить хранилища данных, находящиеся на разных серверах, в одну параллельную сетевую файловую систему.

Основные характеристики:

- **Эластичность.** Тома хранения не привязаны к аппаратным средствам и управляются независимо. Размеры могут изменяться путем добавления или удаления систем из пула хранения. Даже при изменении объемов данные остаются доступными для клиентов.
- **Петабайтная масштабируемость**. Хранилище на базе GlusterFS позволяет начинать с небольших объемов и расти по мере необходимости вплоть до петабайтных значений.
- **Надежность и высокая доступность**. Автоматическая репликация и отсутствие централизованного сервера метаданных обеспечивает отказоустойчивость и высокий уровень защиты данных. Кластерная файловая система предоставляет различные схемы конфигурации избыточности (RAID 0, 1, 6, 10 и др.) для получения необходимого баланса надежности и производительности.
- **Простота и совместимость**. Кластерная файловая система обеспечивает встроенную совместимость с файловой системой POSIX, включая ACL и поддержку мандатной защиты Astra Linux Special Edition и Альт Линукс СПТ, а также поддерживает общие протоколы, включая CIFS, NFS и OpenStack® Swift. Ваше существующее программное обеспечение не потребует модификации при использовании кластерной файловой системы.
- **Совместимость с защищённой виртуализацией**. Помимо отказоустойчивого файлового хранилища кластерная файловая система предоставляет возможность «бесшовной» миграции виртуальных машин между узлами кластера.

Защищённая виртуализация

Защищённая виртуализация реализована на основе гипервизора KVM, входящего в состав операционной системы Линукс. В состав программного комплекса виртуализации входит эмулятор оборудования (QEMU), обеспечивающий возможность запуска различных гостевых операционных систем.

Технологии

NUMA для минимизации потерь при доступе к памяти

SR-IOV позволяет виртуальным машинам прямой доступ к части аппаратных средств

VFIO — проброс PCI устройств в гостевую ОС

KSM — использование общих страниц для экономии памяти

Каждая гостевая операционная система представляет собой отдельный процесс базовой операционной системы. Процесс KVM имеет изолированное от других гостевых процессов адресное пространство. Гипервизор использует аппаратные возможности для виртуализации процессора (Intel VT и AMD-V) и памяти (AMD NPT и Intel EPT).

Мандатное разграничение доступа осуществляется путем установки соответствующей метки на все объекты (сокеты, файлы и т.п.), через которые осуществляется взаимодействие виртуальной машины с пользователем и внешними системами. Помимо этого, производится дискреционное разграничение доступа с помощью стандартных механизмов Линукс. При подключении к удаленному рабочему столу по протоколам SPICE и VNC аутентификация пользователей происходит с помощью механизма SASL с использованием метода Kerberos.

Для виртуальных машины доступны следующие важные возможности:

- «горячая» миграции – перенос с одного узла кластера на другой без останова гостевой операционной системы;
- создание мгновенных снимков состояния;
- проброс устройств USB в гостевую ОС;
- работа со специальными томами iSCSI, GlusterFS и образами QCOW2.

Защищённая виртуализация доступна как самостоятельный продукт и используется как одна из основ для **защищённой облачной платформы «Глобус»**

Подробности смотрите на нашем сайте http://лаборатория50.рф

Защищённая виртуализация позволяет запускать широкую номенклатуру гостевых операционных систем:

- Linux (Альт, Astra Linux, Red Hat, семейство МСВС);
- Windows XP (x86) – Windows 10 (x86, x86_64);
- Windows Server 2003/2008/2012 (x86, x86_64);
- QNX 6, КПДА.

Для большинства гостевых операционных систем доступны драйверы паравиртуальных устройств ввода-вывода, повышающие производительность. При использовании SPICE доступны специальные графические драйверы QXL, предоставляющие расширенные графические возможности.

ПРЕИМУЩЕСТВА

Кластер высокой готовности «Лаборатории 50» базируется на знаниях и опыте работы наших специалистов с отечественными операционными системами и программным обеспечением. Наши программные продукты учитывают многие проблемные места отечественных дистрибутивов, работают со средствами защиты информации и могут применяться для обработки информации до уровня «совершенно секретно».

Важным преимуществом служит основа кластера высокой готовности — открытое программное обеспечение. При необходимости вы сможете интегрировать наши решения с другими программами или перейти на другое ПО.

ПОДДЕРЖКА

Для продукта предоставляется бесплатная дистанционная техническая поддержка. Платная поддержка приобретается отдельно и включает в себя дополнительное часы разработчиков (например, для модификации интерфейса управления под требования заказчика).

Телефон: 8 (812) 981-68-09
Эл. почта: team@lab50.net