Стратегии обеспечения безопасности облачных вычислений

Strategies to ensure the security of cloud computing

Ключевые слова: облачные вычисления – cloud computing; безопасность – security; виртуализация – virtualization.

В статье рассматриваются вопросы обеспечения безопасного функционирования и предоставления доступа к облачным сервисам. Представлены стратегии обеспечения безопасности облачных вычислений. Даются рекомендации по вопросам безопасности облачных вычислений.

The article considers the tasks of providing safe operation and granting access to cloud services. Cloud services security provision strategies are presented. Recommendations on cloud computing security issues are given.

ГАРБАР / GARBAR P.
Павел Юрьевич
(pgarbar@gmail.com)
технический специалист
кафедры Программных систем,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (НИУ ИТМО),
г. Санкт-Петербург

ХОРУЖНИКОВ / KHORUZHNIKOV S.
Сергей Эдуардович
(xse@vuztc.ru)
кандидат физико-математических наук, доцент,
декан факультета инфокоммуникационных технологий,
директор ЦАО ИТ,
НИУ ИТМО,
г. Санкт-Петербург

ЗУДИЛОВА / ZUDILOVA T.
Татьяна Викторовна
(zudilova@ifmo.spb.ru)
кандидат технических наук, доцент,
заведующая кафедрой Программных систем,
заместитель Директора ЦАО ИТ,
НИУ ИТМО,
г. Санкт-Петербург

ПРЫГУН / PRYGUN V.
Виктор Викторович
(victor@ifmo.spb.ru)
заведующий лабораторией,
НИУ ИТМО,
г. Санкт-Петербург

Облачные вычисления опираются на несколько стратегий безопасного функционирования и предоставления сервисов для клиентов. В зависимости от того, о поставщике или потребителе облачных услуг будет идти речь, различные аспекты безопасности будут в большей или меньшей степени относиться к субъекту [1–4].

Стратегии безопасности включают в себя:
– надежность серверов;
– отказоустойчивость;
– резервное копирование;
– масштабируемость;
– доступность;
– защита консоли сервера;
– шифрование;
– гарантированное уничтожение информации;
– подписывание пакетов;
– система отслеживания транзакций (TTS);
– бесперебойное электропитание (ИБП);
– защита от вирусов;
– исправления и пакеты поддержки.

При этом необходимо следить за потенциальными рисками и проводить аудит. Кроме того, необходимо обеспечить безопасность клиентских устройств, с которых осуществляется доступ к облачным сервисам.

НАДЕЖНОСТЬ СЕРВЕРОВ

Надежность характеризуется большим временем наработки на отказ – система может непрерывно работать продолжительное время, без сбоев, не требуя плановых остановов.

Надежные компоненты позволяют работать длительное время без сбоев.

При построении центра обработки данных для облачных вычислений рекомендуется применять компьютеры и другое оборудование серверного класса, прошедшее сертификацию программных и аппаратных производителей.

В облачной среде лучше использовать однотипное оборудование, так как это позволит иметь унифицированные запасные части, стандартизованные процедуры по замене и ремонту вышедшего из строя оборудования и упростить перенос рабочей нагрузки между серверами. Для прикладных программных продуктов также предусмотрена сертификация. Все это позволяет серверам обеспечивать продолжительное время беспрерывной работы. В облачной модели надежность серверов будет практически полностью входить в сферу ответственности поставщиков.

ОТКАЗОУСТОЙЧИВОСТЬ

Облачное решение должно предоставлять надежный и отказоустойчивый доступ к данным для пользователей и приложений. Один из способов повысить надежность доступа – это обеспечить их отказоустойчивость, а это достигается путем избыточности компонентов для устранения единой точки отказа сети.

Отказоустойчивость предоставляет возможность пережить сбой или обеспечить малое время восстановления.

Отказоустойчивость в облачной среде обеспечивается несколькими путями:

– Кластеризация виртуальных серверов.
– Кластеризация физических серверов.
– Геокластер.

КЛАСТЕРИЗАЦИЯ

В облачной среде рабочая нагрузка обычно представляется в виде виртуальных машин, на которых работают сетевые операционные системы (ОС). В сетевых ОС применяются схемы повышения отказоустойчивости на уровне всей системы. Кластеризация виртуальных машин применима в сервисных моделях «Программа как сервис – SaaS» и «Платформа как сервис – PaaS». В модели «Инфраструктура как сервис – IaaS» в кластер объединяются физические компьютеры.

В итоге кластеры позволяют:

– предоставлять непрерывный доступ к данным и ресурсам;
– пасштабироваться в соответствии с растущими требованиями в объемах хранения;
– снижать стоимость управления хранения данных.

ГЕОКЛАСТЕРЫ

При катаклизмах и катастрофических разрушениях центра обработки данных, в котором размещаются облачные вычислительные ресурсы, сервисы для клиентов должны продолжать оставаться доступными в соответствии с соглашениями об уровне обслуживания. Это возможно организовать при наличии дополнительных центров обработки данных. Такие центры стоит обустраивать на значительных расстояниях друг от друга (порядка 100 км) или даже в других странах и на других континентах. Такой подход позволит нивелировать последствия масштабных катастроф и природных катаклизмов. Кроме того, это позволит переносить рабочую нагрузку в центры обработки данных физически более близкие к клиентам, а также учитывать перемещение рабочего времени по часовым поясам в течение суток. Высвободившиеся мощности в разгруженных центрах обработки данных можно будет переводить в режим обслуживания, не нарушая при этом соглашения об уровне обслуживания клиентов.

УПРАВЛЕНИЕ ЦЕЛОСТНОСТЬЮ ДАННЫХ НА СЕРВЕРАХ

Сетевые ОС имеют несколько свойств томов, которые помогают обеспечивать целостность данных:

– немедленная запись данных на диск при закрытии файла (Flush Files Immediately);
– применение системы слежения за транзакциями приложений для отката незавершенных изменений (Transaction Tracking System);
– применение мгновенных снимков томов для резервного копирования открытых файлов (File-Level Snapshot).

Кроме средств ОС целостность данных может обеспечиваться и на аппаратном уровне. Так, для дисковых контроллеров предусмотрено батарейное питание кэшей, на современных дисках кэш может размещаться в энергонезависимой флэш-памяти, в дисковых массивах. Существуют аппаратные средства создания и управления мгновенными снимками дисковых томов. Аппаратные средства переноса данных в дисковых массивах позволяют существенно ускорять перемещение виртуальных машин с одного физического компьютера на другой практически без остановки ее работы и потери данных (live migration).

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

Резервное копирование – одна из важнейших задач поставщика облачных сервисов. Данные обрабатываются, хранятся и архивируются в самом центре обработки данных, что упрощает их резервное копирование и длительное хранение. При необходимости восстановления данных из резервных копий операторы центра сделают это профессионально и быстро по запросу клиента.

Данные или виртуальные машины могут быть восстановлены в исходное место или на новой виртуальной машине (другом экземпляре).

ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

При хранении данных и резервных копий в облаке заказчики хотят быть уверенными, что данные будут гарантированно уничтожены и ни при каких обстоятельствах не будут доступны посторонним лицам после завершения срока их хранения или при удалении из системы. Это касается всех резервных копий, мгновенных снимков и кэшированных данных. Также может иметь большое значение, в каком физическом месте располагаются данные, так, например, конфиденциальные и секретные данные не должны сохраняться в других странах или на определенных территориях. Эти условия должны специально оговариваться в условиях по обслуживанию в договоре между поставщиком облачных услуг и клиентом.

Гарантированное уничтожение данных скрывает удаленные файлы, перезаписывая их случайными образцами шестнадцатеричных символов. Это препятствует тому, чтобы неавторизованные пользователи использовали дисковый редактор, чтобы получить доступ к удаленным файлам.

Гарантированное уничтожение данных требует существенной дисковой пропускной способности, что может привести к потере производительности, так как гарантированное уничтожение данных подразумевает многократное выполнение процедуры записи.

МАСШТАБИРУЕМОСТЬ

Масштабируемость показывает способность к увеличению емкости, производительности, мощности, скорости и т.п.

Вертикальная масштабируемость (увеличевает возможность одного сервера) достигается добавлением большего или лучшего оборудования в сервер.

Горизонтальная масштабируемость (увеличивает емкость приложения) достигается добавлением серверов для выполнения вычислений.

Масштабируемость – одно из основных свойств вычислительного облака. Для заказчиков вертикальная масштабируемость может заключаться в перемещении виртуальной машины на более мощный физический сервер, а горизонтальная – в запуске нужного количества дополнительных виртуальных машин с нужным программным обеспечением.

ДОСТУПНОСТЬ

Доступность – это уровень сервиса, который предоставляет приложение, служба или система, выражается обычно в процентном соотношении времени, когда услуга предоставляется и не предоставляется с указанным качеством.

В частности, свойство доступности информации (ресурсов автоматизированной системы) является одним из основных критериев информационной безопасности объекта.

Высокодоступные системы или сервисы доступны 99% времени или выше.

Высокая доступность:

– требования отличаются в зависимости от того, как измерять доступность;

– обычно не учитывается время плановых простоев при расчете доступности.

В сетевых ОС высокая доступность обеспечивается не только надежными компонентами и средствами повышения отказоустойчивости, но и разнообразием способов доступа к информации.

Отказоустойчивость – способность пережить сбой или быстро восстановиться после сбоя.

Высокая доступность – возможность получить доступ к сервисам или ресурсам тем или иным оговоренным способом. Это может быть несколько независимых каналов связи, поддержка различных протоколов (IPX/SPX, TCP/IP, HTTP/HTTPS, NCP, FTP, WebDAV, CIFS, NFS, AFP(AppleShare)), кластер и геокластер, добавление или замена устройств на ходу.

ЗАЩИТА СЕРВЕРНОЙ КОМНАТЫ. ЗАЩИТА КОНСОЛИ СЕРВЕРА

Безопасность серверной должна включать меры безопасности на физическом, процедурном уровне и для персонала. По крайней мере, все серверные должны оснащаться замками на дверях, чтобы ограничить доступ только для уполномоченного персонала. Также могут быть необходимы дополнительные средства физической защиты в зависимости от эксплуатационных потребностей. Примеры дополнительной физической безопасности включают возможные комбинации из нижеследующего:

– охрана, наблюдающая за входами и выходами;

– сотрудник службы безопасности, сопровождающий персонал при работе в серверной;

– служебный пропуск или маркер с аутентификацией и схемой аудита;

– кодовый замок на двери;

– камеры видеонаблюдения для фиксации действий возможного нарушителя;

– датчики и аварийные сигналы для обнаружения и предупреждения о несанкционированном доступе.

ЗАЩИТА КОНСОЛИ

Первый принцип консольной безопасности сервера – физическая безопасность. Если не обеспечена

физическая безопасность, все остальное не будет иметь существенного значения.

Системный блок должен быть размещен в таком месте, где никто не сможет унести его или выключить/перезагрузить. Некоторые администраторы сети убирают клавиатуру, монитор и управляют сервером при помощи средств удаленного управления.

Блокировка консоли должна быть активирована и для физической консоли и для утилит удаленного доступа. Блокировка консоли не заменяет безопасность консоли, а только дополняет ее.

ШИФРОВАНИЕ

В современных серверных операционных системах может применяться шифрование, как на уровне отдельных файлов, так и для разделов или логических томов целиком.

В облачной среде шифрование необходимо при хранении данных на чужой территории, при пересылке между центрами обработки данных, а также между облаком и клиентом.

ПОДПИСЫВАНИЕ ПАКЕТОВ

Подпись пакета – это усовершенствованная возможность защиты серверов и рабочих станций посредством использования технологии открытых/закрытых ключей, предотвращающая подлог и повтор пакетов.

Использование подписи пакета настоятельно рекомендуется при взаимодействии облака и клиента, так как это общение обычно происходит по открытым каналам Интернета. Подпись пакета предотвращает подлог, требуя, чтобы сервер и станция-клиент "подписывали" каждый пакет, используя один из алгоритмов шифрования с использованием личного и открытого ключей. Подписи различны для каждого пакета.

Пакеты с неправильными подписями отклоняются без разрыва соединения рабочей станции-клиента с сервером. Однако предупреждающее сообщение с записью об источнике неправильного пакета заносится в журнал ошибок. Если подпись пакета установлена на сервере и на всех рабочих станциях-клиентах сети, то практически невозможно подделать пакет так, чтобы это осталось незамеченным. На сегодняшний день подобный принцип защиты пакетов применяется в IPsec.

IPSEC

IPsec — это платформа открытых стандартов для защиты обмена данными по IP сетям посредством криптографических служб безопасности. IPsec поддерживает:

– одноранговую проверку подлинности на уровне сети;

– проверку подлинности источника данных;

– обеспечение целостности данных;

– обеспечение конфиденциальности данных;

– защиту от повторной передачи перехваченных данных.

IPsec обычно используется для обеспечения конфиденциальности, целостности данных и проверки их подлинности при передаче по небезопасным каналам. Первоначально эта платформа предназначалась для защиты трафика в публичных сетях, однако ее реализации часто используются для повышения уровня безопасности частных сетей, поскольку организации не всегда уверены в отсутствии уязвимостей их частных сетей, которыми могут воспользоваться злоумышленники.

IPsec обладает следующими преимуществами:

– предложение взаимной проверки подлинности перед началом обмена данными и в ходе обмена;

– принудительная взаимная идентификация сторон в процессе обмена данными;

– обеспечение конфиденциальности данных посредством шифрования IP-трафика и проверки подлинности цифровых пакетов.

IPsec работает в двух режимах.

– Транспортный режим. Это режим IPsec по умолчанию. В транспортном режиме IPsec шифрует только полезные IP-данные, IP-заголовки не шифруются. Транспортный режим следует выбирать для сквозного обмена данными, например между клиентом и сервером.

– Туннельный режим. В туннельном режиме IPsec шифрует как полезные данные, так и заголовки IP-пакетов. Туннельный режим, прежде всего, предназначен для обмена данными между двумя сетями, когда данные передаются через ненадежную сеть, такую как Интернет.

СИСТЕМА ОТСЛЕЖИВАНИЯ ТРАНЗАКЦИЙ (TTS)

Некоторые ОС, файловые системы и прикладные программы для обеспечения целостности обрабатываемых и сохраняемых данных используют систему, следящую за транзакциями, названную системой отслеживания транзакций (TTS). Если файл помечен как транзакционный, TTS может предотвратить повреждение записей в файле, отменяя незавершенные транзакций и ведя учет подтвержденных данных.

ПРИМЕЧАНИЕ: файл, отмеченный как транзакционный, не может быть удален или переименован.

TTS может также отменить сокращение или увеличение файла и многократные изменения в той же области данных во время единственной транзакции. TTS может даже отменить прерванные

отмены, если сервер перестал работать в процессе отката транзакций.

Также TTS может защитить от таких типов ошибок приложения любого типа, которые используют работу, блокировкой отдельных записей, включая традиционные базы данных, некоторые приложения электронной почты, и некоторых коллективных планировщиков.

Файлы, которые не организованы в виде дискретных записей (такие как файлы обработки текста), не могут быть защищены TTS.

Транзакции в сети могут быть прерваны в любой из следующих ситуаций:

– электропитание рабочей станции или сервера было нарушено во время транзакции;

– аппаратура сервера или рабочей станции дала сбой (например, ошибка четности);

– сервер или рабочая станция зависла в ходе транзакции (программный сбой);

– сетевое оборудование (такое как концентратор, коммутатор или маршрутизатор) дало сбой в процессе транзакции.

БЕСПЕРЕБОЙНОЕ ЭЛЕКТРОПИТАНИЕ (ИБП)

Источник бесперебойного питания (ИБП – UPS) – модуль резервного питания, который предоставляет бесперебойное питание, если происходит отключение электроэнергии. ИБП – необходимая часть сети. Он не только помогает предотвращать повреждение компьютеров от скачков напряжения и снижений напряжения, но и предотвращает потерю данных во время отключений электроэнергии. Современные центры обработки данных оснащаются мощными ИБП и системами аварийного автономного питания на случай, если перерыв в централизованном электроснабжении превышает несколько часов.

Клиентские рабочие места стоит оснащать устройствами бесперебойного электропитания. Мобильные клиентские устройства, такие как ноутбуки, планшеты, смартфоны, имеют независимое батарейное электропитание и поэтому меньше подвержены проблемам, связанным с электропитанием.

ЗАЩИТА ОТ ВИРУСОВ

Вирус — это фрагмент вредоносного кода, который копирует себя и распространяется в определенном виде или форме. Такой код обычно распространяется с помощью нежелательной почты или путем получения доступа к другим компьютерам и попытки их заражения. Слово «вирус» стало универсальным термином для обозначения традиционных вирусов, распространение которых не имело другой цели, кроме использования соответствующего кода. Однако сейчас этим термином называют вредоносные программы, программы для показа рекламы, шпионское ПО и все программы, которые заражают компьютеры. Многие вирусы выполняют вредоносные действия на зараженных компьютерах, такие как кража данных или отключение важных приложений.

Поставщики облачных услуг могут предоставлять защиту от вирусов в сервисных моделях «Программа как сервис – SaaS» и «Платформа как сервис – PaaS».

На клиентских устройствах об этом должны позаботиться владельцы этих устройств.

ИСПРАВЛЕНИЯ И ПАКЕТЫ ПОДДЕРЖКИ

Повсеместно вычисления выполняются в постоянно меняющейся среде. Ежедневно появляются новые технологии, в то время как новые способы использовать эти технологии, кажется, появляются ежечасно. По мере развития технологий и появления потребности в обеспечении безопасности необходимо подготовить серверную инфраструктуру к эффективной работе и одновременно защитить ее.

Поставщики облачных услуг могут обеспечивать обновление операционных систем и ряда приложений в сервисных моделях «Программа как сервис – SaaS» и «Платформа как сервис – PaaS».

При использовании модели «Инфраструктура как сервис – IaaS» задачи по обновлению и установке заплаток остаются в ведении заказчика.

Литература

1. The Microsoft white paper, Risk Model for Operations Eric Cole, Network Security Bible, 2 edition – Wiley, 2005. 936 с.

2. *Vic (J.R.) Winkler*, Securing the Cloud. – Syngress Elsevier, 2011 – 315 с.

3. *Tim Mather, Subra Kumaraswamy, and Shahed Latif*, Cloud Security and Privacy, – O'REILLY, 2009. 316 с.

4. *T. Dierks and E. Rescorla*, "The Transport Layer Security (TLS) Protocol Version 1.2", 2008, [Электронный ресурс]. – Режим доступа: http://www.ietf.org/rfc/rfc5246.txt. свободный. Яз.анг. (дата обращения 25.10.2013).