Нагрузочное тестирование как элемент формирования безопасных систем

Котов С.Л.

Надежность информационной системы как элемент обеспечения безопасности

Одним из важных составных аспектов безопасности информации в крупных информационных системах является надежность системы, в частности - отказоустойчивость в критических режимах. Угроза безопасности информации может возникать не только в результате преднамеренных атак на информационную систему или неправильных действий пользователя, но и из-за превышения критической нагрузки на систему.

Для надежного и предсказуемого функционирования информационной системы необходимо иметь данные о предельной нагрузке (выраженной, например, в количестве одновременно поступающих в систему пользовательских запросов), о характере поведения системы в условиях перегрузки и возможных последствиях в случае отказа системы из-за превышения допустимой нагрузки. К сожалению, расчетные значения таких характеристик, определенные теоретическими методами, не всегда совпадают с фактическими и не адекватно отражают поведение системы в реальной критической ситуации.

Кроме того, информационная система сама по себе неоднородна с позиции предельной производительности: всегда имеются критичные элементы программно-аппаратной платформы, накладывающие ограничение на производительность системы и снижающие ее надежность. Выявление таких элементов не всегда является тривиальной задачей, и экспериментальные данные дают порой весьма неожиданные результаты.

С позиции поведения информационной системы в условиях критической нагрузки их можно условно разделить на три группы:

1. системы, у которых при повышении нагрузки производительность достигает максимального значения и затем остается практически постоянной при дальнейшем росте нагрузки («идеальные» системы);
2. системы, у которых наблюдается медленный плавный спад производительности при превышении максимального уровня нагрузки;
3. системы, у которых производительность резко падает при незначительном превышении максимальной нагрузки.

Системы третьего типа наиболее критичны с позиции надежности и безопасности информации и требуют соблюдения постоянного наличия резерва по производительности.

Метод нагрузочного тестирования для проверки надежности и безопасности систем

Оценка показателей функционирования информационной системы является сложным процессом, требующим организации работы и четкого взаимодействия большого числа пользователей для создания различных уровней нагрузки на систему. При этом возможно возникновение ситуаций, создающих реальную угрозу безопасности информации, особенно в режимах с пиковой нагрузкой. Поэтому решение задачи измерения показателей функционирования должно базироваться на применении специальных методов тестирования и, соответственно, специальных инструментальных программных средств, позволяющих значительно снизить стоимость испытаний и обеспечить необходимый уровень безопасности информации.

Для получения данных о производительности используется тестирование под нагрузкой с последующим анализом временных характеристик выполнения тестовых заданий. Тестирование под нагрузкой является методом, при котором тестовые задания имитируют нагрузку на информационную систему, подобную той, которая создается реальными пользователями системы.

Инструментальные средства для измерения производительности

Необходимой основой для проведения нагрузочного тестирования являются инструментальные средства, позволяющие в лабораторных условиях эмулировать сложное окружение реального мира телекоммуникационных, клиент-серверных и Internet-взаимодействий и выполнить всестороннее тестирование распределенной системы.

Задача таких инструментальных средств — организация лабораторного испытательного стенда, который будет эмулировать от десятков до тысяч пользователей, посылающих и получающих информацию, воспроизводя тем самым сложное взаимодействие между клиентским и серверным приложением, базами данных, Internet-серверами и другими системами. Большинство развитых инструментальных средств нагрузочного тестирования позволяет организовать испытательный стенд с распределенным выполнением тестов и централизованным управлением. Как правило, структура такого стенда включает:

1. сам объект испытаний;
2. центральную управляющую станцию, где располагаются сервисы управления процессом тестирования, сервисы обработки статистики, репозиторий результатов тестирования и управляющая графическая консоль пользователя;

3. несколько рабочих станций моделирования нагрузки, на которых расположены компоненты для имитации деятельности пользователей. На каждой такой станции может быть смоделирована работа до нескольких сотен виртуальных пользователей (VU);
4. дополнительные станции мониторинга и генерации тестовых данных, на которых запускаются генераторы тестовых данных для обеспечения бесперебойного снабжения тестовыми данными рабочих станций моделирования нагрузки. Также на отдельных станциях запускаются измерительные мониторы, осуществляющие наблюдение за процессами обработки на тестируемой системе и передающие измеренную статистику на центральную станцию.

Обобщенно, структура испытательного стенда представлена на рис.1.

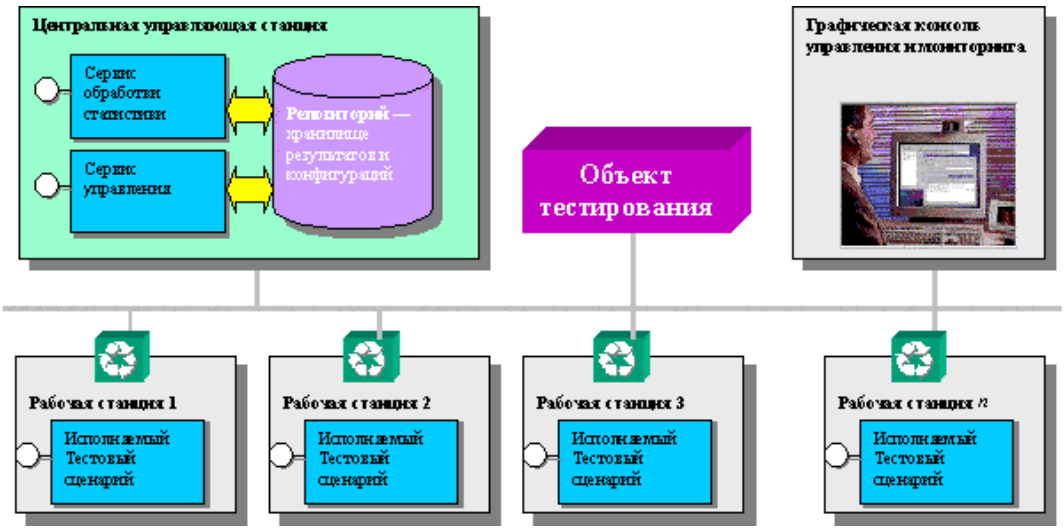

Рис. 1

Моделирование нагрузки осуществляется путем выполнения тестовых транзакций, каждая из которых включает определенный набор тестов, выполняемых в последовательном или произвольном порядке.

При тестировании сложных систем большое значение имеет адекватность моделирования взаимосвязанных процессов обработки информации. Выполнение следующего этапа технологического цикла обработки запроса зависит от результатов предыдущего, т. е. практически образуется цепочка работ, каждая из которых принимает на входе результаты предыдущего этапа обработки и на выходе передает собственные результаты следующему этапу. Группы пользователей или клиентские приложения, взаимодействующие с автоматизированной системой, являются частью общего технологического цикла и их действия являются взаимосвязанными между собой. Для обеспечения достоверного

моделирования сложных технологических циклов, инструментальные средства тестирования должны учитывать взаимосвязи работ, преобразуя их в соответствующие этапы выполнения тестовых заданий. Адекватное моделирование работы пользователей в таких системах возможно только при поддержке тестовым инструментарием определенной схемы выполнения тестов — конвейерной модели выполнения тестов с асинхронной передачей результатов между этапами выполнения.

Накопленный опыт работы с инструментальными средствами нагрузочного тестирования позволяет сформулировать ряд требований к их характеристикам:

1. **Масштабируемость нагрузки.** Поддержка возможности параллельного запуска систем выполнения тестовых транзакций на большом числе станций испытательного стенда. Каждая станция должна обладать возможностью имитации до 100 виртуальных пользователей.
2. **Централизованный сбор статистики.** Инструмент должен обладать централизованным компонентом сбора статистики в реальном режиме времени. Средства статистической обработки должны давать возможность строить временные ряды для изучения динамики измерения показателей в течение сеанса тестирования;
3. **Централизованное управление.** Подготовка к выполнению сеансов, планирование, запуск и остановка сеансов, просмотр результатов – все эти процессы должны выполняться из единой точки. Процедуры конфигурирования и управления состоянием исполняющих систем, измерительных мониторов и агентов должны осуществляться в автоматическом режиме.
4. **Гибкость моделирования.** Инструментальное средство тестирования должно обладать способностью построения реалистичных по составу потоков тестовых запросов. Необходимо иметь возможность независимого исполнения нескольких тестовых транзакций с различными тестовыми смесями, для каждой транзакции должен задаваться свой план выполнения и число имитируемых пользователей. Для моделирования сложных систем, особенно связанных с документооборотом, требуется поддержка конвейерной модели выполнения тестов с асинхронной передачей результатов между этапами выполнения.
5. **Развитые средства хранения конфигурации сеансов и результатов тестирования.** Конфигурация сеансов тестирования представляет достаточно сложную систему взаимосвязанных параметров, поэтому инструментальное средство должно предоставлять возможности по структурированному хранению конфигурации сеансов. Необходимо иметь возможность многократного запуска каждого сеанса тестирования с сохранением статистических результатов по всем реализациям с

целью последующего проведения сравнительного анализа. Наилучшим решением является использование реляционной СУБД для хранения конфигураций и связанных с ними наборов результатов.

6. **Наличие средств мониторинга показателей системной статистики.** Весьма желательным является наличие инструментов для измерения и записи показателей статистики ядра операционной системы параллельно с измерением и записью показателей производительности. Анализ показателей системной и прикладной статистики, привязанных к единой временной шкале, позволяет более точно определить причину возникновения «узких мест» и несбалансированности в системе.
7. **Наличие средств регистрации событий (журнализация).** Эти средства требуются для выполнения автоматизированной фиксации нештатных ситуаций и записи сообщений об обнаруженных в ходе тестирования отклонений в поведении испытываемый системы.

Практическое применение инструментов для нагрузочного тестирования телекоммуникационных информационных систем

Существующая практика применения инструментов нагрузочного тестирования для телекоммуникационных информационных систем предусматривает, как правило, реализацию сеансов тестирования с имитацией параллельной работы необходимого числа пользователей, выполняющих определенные запросы к испытуемой системе в сетевой среде. Общая цель таких сеансов — оказать в течение заданного времени определенное воздействие на тестируемую систему в диапазоне от расчетной нагрузки до пиковой, моделируя при этом как допустимые (штатные), так и дестабилизирующие действия пользователей.

Особенный практический интерес представляет моделирование с уровнем нагрузки, максимально приближенным к предельному, что позволяет выявить возможные проблемы надежности систем до того, как они станут реальной угрозой информационной безопасности. Практически любые действия пользователей в пиковых режимах нагрузки оказывают значительное дестабилизирующее воздействие, поэтому устойчивость системы в этих условиях является чрезвычайно важным компонентом общей надежности.

Существует три основных практических сценария применения инструментов для нагрузочного тестирования, ориентированные именно на анализ надежности и безопасности систем:

- моделирование DOS (Denial-Of-Service) атак на различном уровне работы информационных систем — моделирование преднамеренных дестабилизирующих воздействий;

- моделирование нормальной деятельности пользователей пиковых режимах нагрузки;
- определение предельно допустимого уровня нагрузки на систему в конкретном окружении.

Моделирование DOS-атак ставит своей целью проверку устойчивости системы к преднамеренным дестабилизирующим воздействиям. Распределенные инструментальные средства нагрузочного тестирования как нельзя лучше подходят для организации моделирования таких атак. DOS-атака может быть организована на любом уровне системы, от уровня протокола TCP до прикладного уровня сервисов. Благодаря гибкости инструментальных средств тестирования возможна реализация алгоритмов любых атак и проведение комплексных испытаний с одновременным воздействием по всем уязвимым местам системы.

Целью DOS-атак является исчерпание ресурсов серверного приложения или системы в целом, что вызовет потерю работоспособности. Устойчивое приложение должно теми или иными способами блокировать нежелательные запросы и не допускать опасного уровня исчерпания ресурсов. Достаточно уязвимыми для таких атак являются приложения распределенных вычислений, которые ассоциируют с каждым открывающимся соединением определенные ресурсы системы, такие как области памяти, потоки, порты и т.д. Кроме того, выполнение даже относительно небольшого количества ресурсоемких запросов может существенно дестабилизировать работу системы.

Благодаря свойству масштабируемости инструментальных средств достаточно легко организовать массированную тестовую атаку с одновременным участием тысяч пользователей, используя всего 10–15 станций моделирования нагрузки. Целесообразно выполнять проведение атаки параллельно с моделированием нормальной работы пользователей, чтобы оценить степень влияния дестабилизирующих воздействий на нормальный ход процесса обработки.

Моделирование нормальной деятельности пользователей в режимах пиковой нагрузки предусматривает высокоинтенсивное выполнение реальных транзакций от имени имитируемых пользователей. Тестирование преследует две основные цели — определение нагрузочной способности системы и обнаружение ошибок.

Режим работы системы, при котором загружено более 80% системных ресурсов принципиальным образом отличается от обычного режима работы. В этих условиях вероятность обнаружения ошибок, которые в обычных условиях не проявляют себя, существенно повышается. К ошибкам, наиболее часто проявляющимся в условиях высокоинтенсивной нагрузки, относятся:

- взаимные блокировки (deadlocks) на таблицах баз данных;
- ошибки синхронизации и управления состоянием;
- ошибки управления ресурсами (утечки памяти, утечки ресурсов);
- переполнение выделенных областей памяти, переполнение буферов и очередей;
- ошибки обработки тайм-аутов, отказы в выделении ресурсов (памяти, сетевых соединений, портов);
- несбалансированность процессов обработки между собой (перегрузки одних процессов на фоне недогруженности других);
- потеря управляемости (невозможность выполнения управляющих команд);
- прогрессирующая деградация производительности вследствие неэффективности алгоритмов диспетчеризации, а также сегментации памяти или иных необратимых процессов.

Каждая из этих ошибок способна привести к внезапной остановке системы, сопровождающейся потерей обрабатываемых данных. Для обнаружения признаков возможных ошибок наряду с моделированием нагрузки используется расширенный мониторинг системы, включая наблюдение за характеристиками функционирования ядра операционной системы, сетевыми протоколами, параметрами СУБД, этапами прикладных процессов обработки.

Применение инструментов нагрузочного тестирования, обладающих способностью одновременного запуска различных по составу последовательных тестов, позволяют гибко моделировать характерные ситуации, выделяя проблемные «узкие места».

Определение предельно допустимого уровня нагрузки на систему в конкретном окружении - достаточно распространенная практика получения объективных сведений о характеристиках системы. С помощью тестового инструментария выполняется серия реализации одного и того же сеанса тестирования с определенным шагом увеличения интенсивности нагрузки от реализации к реализации. Увеличение интенсивности обычно заключается в добавлении на каждом шаге определенного числа новых пользователей. При фиксированных значениях показателей времени отклика становится возможным определить предельно допустимое число пользователей, которые при заданной частоте обращений могут получить гарантированный уровень качества обслуживания.

В заключение, в качестве примеров практической иллюстрации применения нагрузочного тестирования, рассмотрим типичные графики динамики изменения времени отклика, полученные во время испытаний систем оперативной обработки запросов.

Первый график (рис.2) характерен для режима работы системы, приближенного к пиковому: время отклика увеличивается почти в 9 раз в течение первых 20 минут, однако в

дальнейшем имеется тенденция к стабилизации. Если предельно допустимое время отклика принять за 5 секунд, то данный режим работы уже является перегрузкой системы. Несмотря на это прикладная система демонстрирует наличие стабилизирующих механизмов: процент загрузки процессоров во время тестирования не превышал 85%—90%, стабильным являлось также использование и других системных ресурсов.

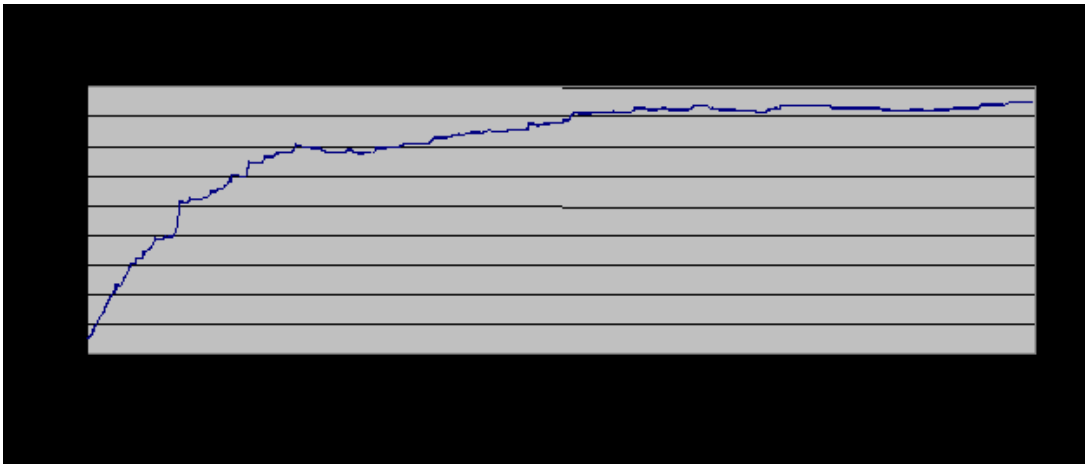

Рис. 2

На втором графике (рис.3) вероятно, имеет место перегрузка системы — рост времени отклика развивается в динамике благодаря исчерпанию свободных ресурсов. Требуется более длительное тестирование для уточнения общей картины.

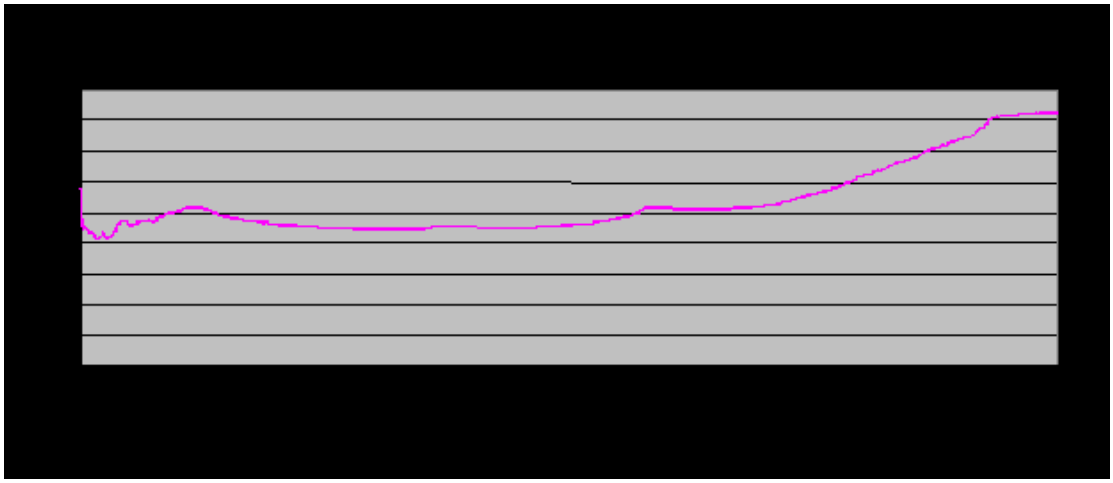

Рис. 3

На третьем графике (рис.4) представлен случай потери устойчивости системы к нагрузке. При неизменном уровне нагрузки наблюдается прогрессирующий рост времени отклика. Характерной особенностью системы является наличие внутренних очередей обработки, поэтому уже по первым минутам тестирования с большой уверенностью можно

прогнозировать переполнение очередей и крах системы (что и произошло через 3 часа после начала тестирования).

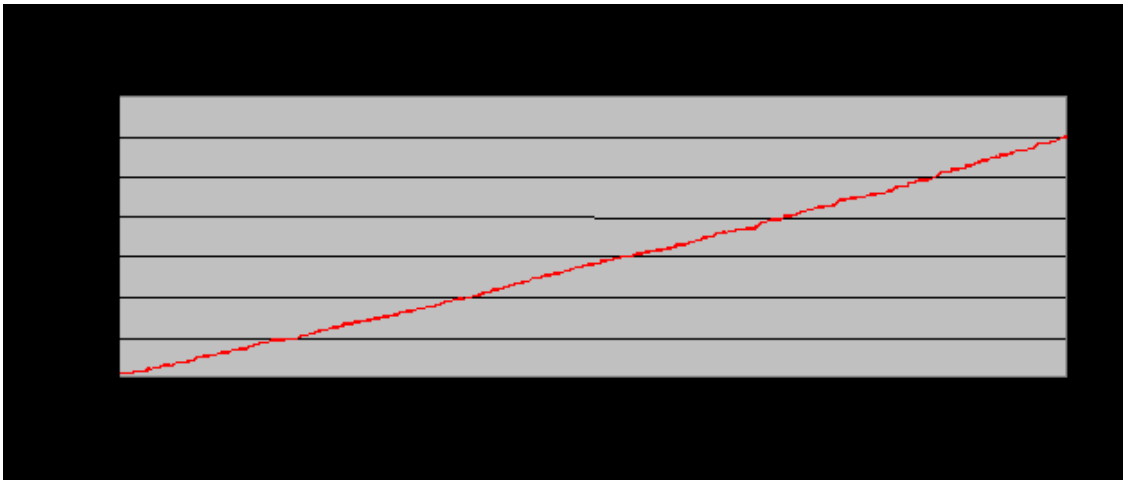

Рис. 4

На четвертом графике (рис.5) имеет место стационарная работа системы в нормальных условиях: разброс времени отклика не превышает заданных значений, выраженной динамики (изменений) процесса не наблюдается.

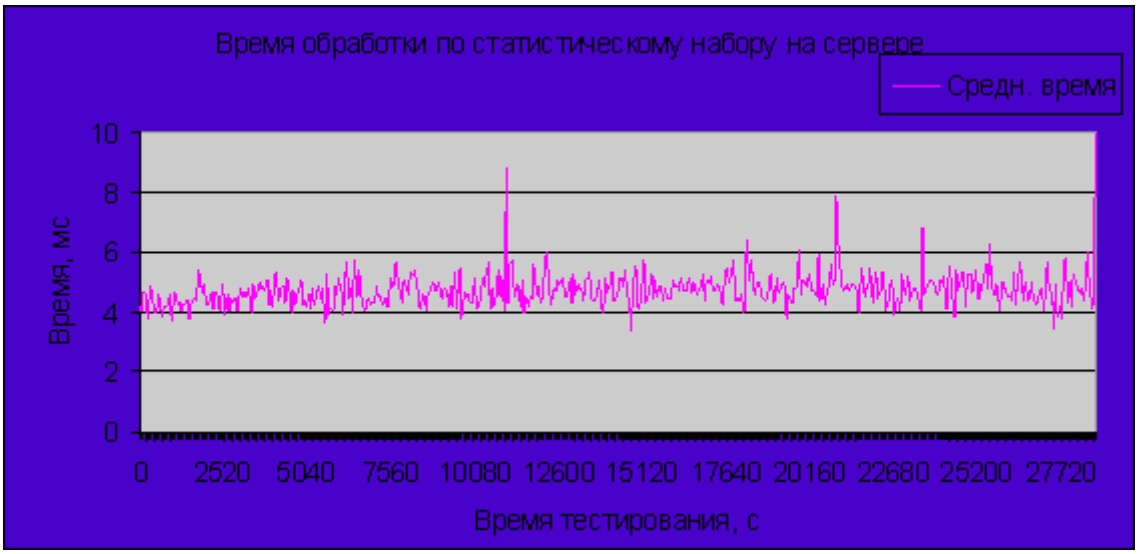

Рис. 5