УДК 681. 324: 681. 518

АУДИТ-КОНТРОЛЬ В ЛОКАЛЬНЫХ СЕТЯХ

МАКРУШАН И.А.

Обсуждаются актуальные проблемы контроля функционирования сети и защиты от несанкционированного доступа анонимных клиентов.

1. Актуальность

Изменение организационной структуры предприятия в сторону уменьшения ее иерархичности потребовало иных форм организации иерархии компьютерных систем. Необходимость осуществления связи между разнородными компьютерными системами, охватывающими одно или несколько предприятий, привела к тому, что корпоративные сети стали основной архитектурой компьютерных сетей. К этому добавилось широкое расспространение Extranet и Intranet технологий, открывших сети для несанкционированного доступа анонимных клиентов. Одним из путей уменьшения проблем несанкционированного повреждения данных в сетях является использование развернутых процедур администрирования и аудит-контроля.

2. Описание проблемы

В соответствии с [1] администрирование характеризуется набором задач управления системой при отклонении параметров функционирования системы от заданных значений.

Состояние системы описывается множествами состояний **X** и показателей эффективности функционирования **W**. Задача управления сводится к переустановке прав и бюджетов в соответствии с формируемыми внешними требованиями (заявками) или в соответствии с текущей ситуацией в сети **X[i]**.

Задача управления безопасностью предполагает использование определенных механизмов защиты ресурсов и ресурсосодержащих элементов от потери функциональных способностей или несанкционированного доступа. Решение задачи сводится к автоматической установке различных блокировок.

Наиболее распространенными операционными системами, которые могут быть использованы как для небольших организаций, так и для корпораций, имеющих расположенные в разных географических точках филиалы, являются NetWare и WinNT.

По мере того, как сети становятся больше, возрастает потребность в более совершенных системах аудита, так как с увеличением

размеров сети возрастает опасность нарушения нормальной работы по причине большого количества возникающих ошибок, которые умышленно или неумышленно совершает пользователь. Операционные системы NetWare и WinNT имеют встроенные системы аудита, целью которых является контроль за всеми важными процессами в сети и сохранение информации о них в специальном массиве данных для последующего анализа. Система аудита NetWare 4.x позволяет уполномоченому на то пользователю сети генерировать и администрировать массивы данных для аудита. Этому пользователю не нужно обладать правами администратора [2].

Аудитор уполномочен контролировать события, происходящие в NDS (NetWare Directory Service), связанным со всеми имеющимися ресурсами. Существует также возможность предоставлять этому же или другому аудитору право контролировать события внутри файловой системы. При этом допуск к контролю осуществляется всегда на уровне томов.

Аудитор имеет возможность протоколировать и анализировать события в сети, не имея при этом права доступа к контролируемым объектам (контейнерам и файлам). Единственными файлами, которые разрешено анализировать аудитору, являются сгенерированные им самим файлы данных (Audit Data) и протоколы (Audit History). Как и прежде, аудитор имеет доступ лишь к тем файлам, каталогам и NDS-объектам, права на которые были переданы ему администратором сети. Однако, чтобы администратор сети не мог анализировать данные контроля, аудитор вправе изменить пароль на том или контейнер.

Одной из проблем управления ресурсами сети является оценка состояний всех ее элементов. Существует несколько путей получения этих оценок: использование специальных программ контроля и обмена информацией на уровне SNMP; использование программ дополнительного тестирования и обмена информацией на уровне IPX, SPX (без SNMP), использующих механизмы сокетов или MAPI (Win 95, NT); использование встроенных средств аудит-контроля для конкретных сетевых OS. В работе рассматривается третий вариант.

Таким образом, задача сводится к оценке состояния **X[i]** компьютерной сети, получаемой на основании информации стандартного аудит-контроля, расчету показателей эффективности и формированию рекомендаций по перестройке отдельных элементов сети или их связей. При этом оценка производится мгновенная и статистическая. Статистическая оценка рассчитывается на некотором временном интервале отчетности ΔT.

3. Классификация объектов, событий и критериев аудит-контроля

Встроенные системы аудита осуществляют контроль за всеми важными видами деятельности в сети и сохраняют информацию о

них в специальном массиве данных для последующего анализа. Аудитор выполняет контроль группы объектов по произошедшим событиям в сети с учетом критериальных условий и делает вывод о влиянии события на качественную оценку состояния системы. Исходя из этого, принимается решение об оптимизации каких-либо показателей эффективности функционирования системы.

Предлагается классифицировать контролируемые объекты, события и критериальные условия по группам.

Контролю подлежат следующие объекты сети: сервер, очередь, контейнер, том, каталог, файл, Bindery-объекты, объекты NDS и Security Equivalences, бюджет пользователя и права на ресурсы. Для файловой системы контроль осуществляется на уровне томов, а для NDS – на уровне контейнеров.

Предлагается выделить четыре группы событий W1, W2, W3, W4, для которых должны протоколироваться данные аудита, причем каждая группа обслуживается определенной встроенной функцией системы аудит-контроля.

В первую группу входят события W1 ={W11,W12,...W1n}, подлежащие контролю на уровне каталогов и файлов: создание каталога, файла; удаление каталога, файла; открытие файла; закрытие файла; чтение файла; переименование и перемещение файла; запись файла; модифицирование каталога, файла.

Вторая группа объединяет события для очередей W21 ={W21,W22,...W2n}: создание и удаление очереди; начало и окончание работы очереди; подсоединение и отключение сервера; установка приоритета; изменение прав.

В третьей группе перечислим события на сервере W31 ={W31,W32,...W3n}: изменение даты и времени на сервере; остановы сервера; установка или удаление тома.

В четвертой группе можно задать режим протоколирования следующих событий, происходящих на уровне пользователя W41 ={W41,W42,...W4n}: отключение ведения счета; наделение правами опекуна; регистрация и прекращение работы в сети; изъятие прав опекуна; разрыв связи; ограничение объема памяти на жестком диске, предоставляемого пользователю.

Состояние системы можно оценить значениями критериев, представляющими собой расчетные величины. Критериальные условия **Yj** по оптимизации каких-либо показателей эффективности **Wj** при администрировании не учитываются для формирования управляющих воздействий, а обеспечивают качественную оценку администрирования за какой-либо период **DT**, т.е. **Yj= Yj(W[i]| i =i1,...i2; [i1,i2]** – период отчетности). Предлагается система критериев **Yj**:

– оптимальность структуры хранения данных (по времени доступа к каталогам и файлам, начиная от времени регистрации до

открытия первого файла). Простая и наглядная структура обеспечивает быстрый доступ и обработку данных, слишком сложные структуры приводят к увеличению эксплуатационных затрат, так как в этом случае сложно ориентироваться в данных;

– оптимальность защиты данных от несанкционированного доступа (по времени доступа к данным, количеству попыток несанкционированного доступа), т.е. процесс представления прав доступа не должен приводить к большим издержкам;

– скорость передачи пакета данных по линии сети;

– пропускная способность сети (исходя из вероятности появления ошибок при приеме данных);

– производительность сети. Все пакеты данных, поступающие в очередь, необходимо упорядочить так, чтобы канал использовался оптимально.

Сравнение альтернативных состояний сводится к сравнению соответствующих им значений критериев. При этом выбор сводится к отысканию альтернативы с наибольшим значением критерия. На практике оценивание любого варианта единственным числом обычно оказывается неприемлемым упрощением. Более полное представление о состоянии системы дает оценка не по одному, а по нескольким критериям, качественно различающимся между собой. Поэтому следует ввести глобальный критерий, выполняющий роль упорядочивающей функции. Глобальный критерий упорядочивает альтернативы по значению критерия, выделив тем самым наилучшую Yo**(W)**= Yo**(** Y1 **(W),** Y 2**(W),...** Yp **(W))**.

Задача оптимизации сводится к выбору такого состояния системы, при котором глобальный критерий достигает максимума **P= max**(Yo).

4. Процедура оценки состояния сети

Предлагается процедура оценки состояния сети.

Этап 1. Оценка параметров функционирования системы **W[i]= W (W[i])]**.

Этап 2. Выбор критериев оптимизации **Yj= Yj(W[i])** , формирование глобального критерия Yo**(W)**= Yo**(** Y1 **(W),** Y 2**(W),...** Yp **(W))**.

Этап 3. Оценка оптимальности системы **P= max**(Yo) и прогноз состояния **P= Yj(W[i] | i =i1,...i2; [i1,i2]** – период отчетности) .

Этап 4. Принятие решения о переводе системы из состояния **A** в состояние **B** , т.е. формирование набора команд **U[i]**.

Рассмотрим процедуру оценки состояния сети на следующем примере: начальное состояние системы характеризуется множествами состояний **X[i]** и показателей эффективности функционирования **W[j].**

Предположим, что в сети происходит событие **W[i]**, например, чтение файла. Система аудит-контроля фиксирует время доступа к файлу и все предшествующие действия пользователя в специальных файлах данных и протоколах. Процедура оценки состояния включает в себя следующие этапы:

Этап 1. Оценка параметров сети **W[i]= W (W[i])**. Оценке подлежат следующие параметры: время регистрации в сети; количество попыток несанкционированного доступа; наличие или отсутствие прав на определенный каталог или файл; время доступа к данным.

Этап 2. Выбор критериев и формирование глобального критерия **Yj= Yj(W[i])**. В качестве глобального критерия выбираем оптимальность защиты данных от несанкционированного доступа.

Этап 3. Оценка оптимальности работы сети **P= max(Yo)** в состоянии **X[i+1]=X(W[i])**. На этом этапе можно выполнить прогноз состояния сети **P= Yj= Yj(W[i] | i =i1,...i2; [i1,i2]** – период отчетности).

Этап 4. Принятие решения по оптимизации каких-либо показателей эффективности **Wj**, т.е. формировании исполнительных команд **U[i]** в целях достижения нормального функционирования системы. В данном случае принимается решение об использовании определенных механизмов защиты данных от несанкционированного доступа (переустановка прав на ресурсы, ограничение бюджета, изменение пароля и т.п.). Выявленные нарушения в работе системы и предложения по их устранению сообщаются администратору сети.

Особенности реализации процедуры оценки состоят в том, что дополнительно к стандартным средствам сетевой операционной системы создаются специальные обработчики событий, в своем роде менеджеры аудита, позволяющие формировать специальную справочную базу, накапливать информацию об объекте и проводить анализ данных за рассматриваемый период. Предлагается оценку таких процедур проводить комбинированно, т.е. формируется оценка мгновенных состояний системы и вычисляется ее критериальная величина; формируются оценки по статистическим выборкам за заданный период. Результаты образуют новые выборки, представляющие собой одну из реализаций случайного процесса, заданного во времени. Сравнение этих функций между собой позволяет в полной мере дать оценку об истинном поведении системы. Таким образом, комбинированный статистический анализ представляется наилучшим решением по формированию оценки состояния системы.

5. Выводы

Встроенные системы аудита сетевых операционных систем NetWare и WinNT, целью которых является контроль за всеми важными видами деятельности в сети и сохранение информации о

них, позволяют решать задачи распределения ресурсов, администрирования и безопасности. В статье дана классификация объектов, событий и критериев аудит-контроля, а также предложена процедура оценки состояния системы с возможностью прогноза на определенный период времени.

Комментарий. Работа выполнена под руководством доц. Саенко В.И.

Литература. 1. *Саенко В.И.* Администрирование, управление и мониторинг в компьютерных сетях // АСУ и приборы автоматики. 1998. №.108. С. 251-258. 2. *Ценк А.* Novell Netware 4.x. К.: BHV,1996. 784 с.

Поступила в редколлегию 12.05.98

УДК 681.324

АДМИНИСТРИРОВАНИЕ, УПРАВЛЕНИЕ И МОНИТОРИНГ В КОМПЬЮТЕРНЫХ СЕТЯХ

САЕНКО В.И.

Рассматривается формальный анализ базовых задач, их взаимосвязанность и особенности реализации в реальном масштабе времени. К ним относятся задачи: управления сетевыми объектами, администрирования, мониторинга.

1. Актуальность

Важным моментом развития информационных технологий является переход от концепции сосредоточенных локальных систем к системам распределенным, предполагающим распределенность не только ресурсов транспортной системы, но и ресурсов самой информационной системы, например распределенность баз данных и обрабатывающих модулей. Эти аспекты, прежде всего, затрагивают вопросы организации управления проектируемой и существующих систем. Для распредленнной системы характерно наличие множества задач, разобщенных топологически, но близких по функциям. Представляется актуальным формализация основных задач, обеспечивающих эффективность функционирования распределенных информационных систем.

2. Описание проблемы

Распределенную информационную систему рассматриваем как совокупность функционально однородных, связанных виртуальных сетей, функционирующих на фиксированной транспортной струк-