Конвергентная биллинговая система

WideCoup Billing 3.0

Мониторинг событий и контроль доступа

СОДЕРЖАНИЕ

Общие сведения **3**
Аудит событий безопасности **3**
Общие сведения об аудите **3**
Общие сведения о журнале событий **4**
Журнал приложений 4
Журнал безопасности 4
Журнал системы 4
Журнал Mediation 4
Просмотр журнала безопасности 4
Определение и изменение политики аудита для категории событий 5
Настройка протоколирования **6**
Анализ событий **6**
Заголовок события 6
Типы событий 7
Общее представление о параметрах ведения журнала событий **8**
Форматы файлов с архивами журналов **9**
Устранение неполадок **10**

Общие сведения

Все компоненты биллинговой системы WideCoup Billing 3.x реализованы в виде системных компонентов операционной системы Windows Server, а именно – системных служб WideCoup Mediation и WideCoup SyncService, а также Вер-приложений StorageControl и MyBills. Мониторинг работы сервисов и Веб-приложений, в том числе контроль доступа к ним пользователями домена, осуществляется с помощью системной оснастки «Просмотр событий». Данная оснастка используется для установки и просмотра параметров журналов событий с целью получения сведений о неполадках компонентов системы.

Аудит событий безопасности

Политику аудита можно настроить таким образом, чтобы создавались записи для пользователя или активности системы в указанной категории событий. Можно вести наблюдение за активностью, связанной с безопасностью, например за тем, кто получает доступ к объекту при входе и выходе пользователя из системы, или за изменением параметров политики аудита.

Общие сведения об аудите

Установка политики аудита является важным аспектом безопасности. Наблюдение за созданием и изменением объектов позволяет отслеживать возможные угрозы безопасности, проверять подлинность пользователя, а также получать уведомления в случае сбоя системы безопасности.

Наиболее общими типами событий для аудита являются:

- доступ к таким объектам, как файлы форм отчетов и папки групп отчетов MS Reporting Services;
- управление учетными записями пользователей и групп;
- вход и выход пользователей из Веб-приложений системы.

Для реализации политики аудита необходимо выполнить следующие шаги:

- Укажите категории событий, для которых следует провести аудит. Примерами категорий событий являются вход пользователя в систему, выход из нее и управление учетными записями. Выбранные категории событий составляют политику аудита.
- Установите размер и параметры журнала безопасности. Просмотреть журнал безопасности можно в окне программы Просмотр событий.
- Для проведения аудита доступа к объектам определите объекты, за доступом к которым нужно вести наблюдение, и желаемый тип наблюдения. Например, для аудита всех попыток пользователей открыть отдельный файл формы отчета MS Reporting Services можно настроить параметры политики аудита в категории событий доступа к объектам таким образом, чтобы создавались записи как для успешных, так и для неудачных попыток чтения файла формы отчета.

Рекомендуется включение параметров аудита событий безопасности для важных с точки зрения безопасности объектов и действий и периодический просмотр журналов безопасности на сервере биллинга.

Кроме того, включение политики аудита и просмотра журналов безопасности позволяет обнаружить несанкционированные действия злоумышленников или попытки взлома системы биллинга.

Общие сведения о журнале событий

Сервер биллинга с установленной операционной системой Windows Server 2003 по умолчанию записывает события в три вида журналов:

Журнал приложений

В журнале приложений содержатся данные, относящиеся к работе системных приложений и программ, а именно СУБД MS SQL Server, надстройки MS Reporting Services и службы Веб-публикаций Internet Information Services. События, вносимые в журнал этих приложений, определяются разработчиками корпорации Microsoft и не могут быть изменены со стороны поставщика биллинговой системы WideCoup Billing. Например, СУБД MS SQL Server может заносить в журнал сведения об ошибках, связанных с файлами, содержащими данные о звонках и начислениях за услуги связи.

Журнал безопасности

Журнал безопасности содержит записи о таких событиях, как успешные и безуспешные попытки доступа в систему, а также о событиях, относящихся к использованию ресурсов, например о создании, открытии и удалении файлов и других объектов. Например, после разрешения аудита входа в систему сведения обо всех попытках входа заносятся в журнал безопасности.

Журнал системы

Журнал системы содержит записи о событиях, внесенные компонентами системы Windows. Например, в журнале системы регистрируются сбои при загрузке драйвера или других системных компонентов при запуске системы. Типы событий, заносимых в журнал системы, предварительно определены сервером.

Журнал Mediation

Журнал системы WideCoup Mediation содержит записи о событиях, внесенные компонентами системы предобработки данных о звонках. Например, в этом журнале регистрируются сбои при загрузке модулей сбора и обработки файлов CDR или других компонентов DataProcessorTask при запуске системы WideCoup Mediation. Типы событий, заносимых в журнал системы, предварительно определены системы WideCoup Mediation на этапе инсталляции.

Служба журналов событий запускается автоматически при запуске Windows. Пользователь, входящий в группу Администраторы на сервере биллинга, может назначать разрешения доступа к журналам событий при помощи групповой политики.

Просмотр журнала безопасности

1. Запустите программу Просмотр событий.
2. В дереве консоли щелкните узел **Безопасность**. В области сведений будет отображен список отдельных событий безопасности.
3. Для получения дополнительных сведений о конкретном событии дважды щелкните значок события в области сведений.

Примечания

- Для выполнения этой процедуры необходимо входить в группу Администраторы на сервере биллинга или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду *Запуск от имени*.
- Чтобы открыть окно «Просмотр событий», нажмите кнопку **Пуск**, выберите команду **Панель управления**, дважды щелкните значок **Администрирование**, а затем дважды щелкните значок **Просмотр событий**.
- Дополнительные сведения о событиях безопасности см. в разделе «События безопасности» на веб-узле ресурсов Microsoft Windows (http://www.microsoft.com/).

Определение и изменение политики аудита для категории событий

Если сервер биллинга не является контроллером домена, то определить и изменить параметры политики аудита можно следующим образом:

1. Откройте оснастку Локальные параметры безопасности.
2. В дереве консоли щелкните папку **Политика аудита**.
    - Параметры безопасности
    - Локальные политики
    - Политика аудита
3. В области сведений дважды щелкните категорию событий, для которой требуется изменить параметры политики аудита.
4. Выполните одно или оба следующих действия и нажмите кнопку **OK**.
    - Чтобы производить аудит успешных попыток, установите флажок **Успех**.
    - Чтобы производить аудит неуспешных попыток, установите флажок **Отказ**.

Примечания

- Для выполнения этой процедуры необходимо входить в группу Администраторы на сервере биллинга или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы открыть оснастку «Локальные параметры безопасности», нажмите кнопку **Пуск**, выберите команду **Панель управления**, дважды щелкните значок **Администрирование**, а затем дважды щелкните значок **Локальная политика безопасности**.

Если сервер биллинга является контроллером домена, то определить и изменить параметры политики аудита можно следующим образом:

1. Откройте оснастку «Политика безопасности контроллера домена».
2. В дереве консоли щелкните папку **Политика аудита**.
    - Конфигурация компьютера
    - Конфигурация Windows
    - Параметры безопасности
    - Локальные политики
    - Политика аудита

3. В области сведений дважды щелкните категорию событий, для которой требуется изменить параметры политики аудита.
4. При первом определении данного параметра политики аудита для данной категории событий установите флажок **Определить следующие параметры политики**.
5. Выполните одно или оба следующих действия и нажмите кнопку **OK**.
    - Чтобы производить аудит успешных попыток, установите флажок **Успех**.
    - Чтобы производить аудит неуспешных попыток, установите флажок **Отказ**.

Примечания

- Для выполнения этой процедуры необходимо входить в группу Администраторы домена или Администраторы предприятия в Active Directory или получить соответствующие полномочия путем делегирования. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы открыть оснастку «Политика безопасности контроллера домена», нажмите кнопку **Пуск**, выберите команду **Панель управления**, дважды щелкните значок **Администрирование**, затем дважды щелкните значок **Политика безопасности контроллера домена**.

Настройка протоколирования

Существует возможность настройки следующих параметров:

- Максимальный размер журнала приложений
- Максимальный размер журнала безопасности
- Максимальный размер системного журнала
- Запретить доступ локальной группы гостей к журналу приложений
- Запретить доступ локальной группы гостей к журналу безопасности
- Запретить доступ локальной группы гостей к системному журналу
- Сохранение событий в журнале приложений, дней
- Сохранение событий в журнале безопасности, дней
- Сохранение событий в системном журнале, дней
- Сохранение событий в журнале приложений
- Сохранение событий в журнале безопасности
- Сохранение событий в системном журнале

Анализ событий

Анализ событий в системе биллинга осуществляется на уровне каждого отдельного события, при этом его структура содержит:

- Заголовок события
- Типы событий

Заголовок события

Заголовок события содержит следующие сведения.

Сведения	Описание
Дата	Дата, соответствующая событию. Дата и время события сохраняются в формате всемирного координированного времени (UTC), но всегда отображаются в

	соответствии с местоположением пользователя.
Время	Время, соответствующее событию. Дата и время события сохраняются в формате всемирного координированного времени (UTC), но всегда отображаются в соответствии с местоположением пользователя.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. Олицетворение происходит в тех случаях, когда на сервере один процесс присваивает атрибуты безопасности другого процесса.
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя сервера биллинга, если только просмотр событий не выполняется с другого компьютера.
Источник	Программа, занесшая событие. Это может быть как имя программы, например "SQL Server," так и название компонента системы или службы. Например, "Mediation" означает систему обработки данных о звонках. Источник всегда приводится на языке оригинала.
Событие	Число, определяющее конкретный тип события для данного источника. В первой строке описания обычно содержится название типа события. Например, 6005 — это идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Сведения об источнике и событии в совокупности могут использоваться представителями службы поддержки программного продукта для устранения неполадок.
Тип	Уровень важности событий: «Ошибка», «Уведомление» или «Предупреждение» в журналах системы и приложений; «Аудит успехов» или «Аудит отказов» в журнале безопасности. В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Эти сведения используются преимущественно в журнале безопасности. Например, для аудита событий безопасности категория соответствует одному из типов событий, для которых в групповой политике членом группы «Администраторы» может быть включен аудит успехов или отказов.

Типы событий

В окне «Просмотр событий» отображаются события пяти типов.

Тип события	**Описание**
Ошибка	Серьезные трудности, такие как потеря данных или функциональности. Например, если происходит сбой загрузки службы при запуске, в журнал заносится сообщение о событии типа «Ошибка».
Предупреждение	События, которые в момент записи в журнал не были существенными, но могут привести к сложностям в будущем. Например, если на диске осталось мало свободного места, в журнал заносится предупреждение.
Уведомление	Событие, описывающее удачное завершение действия приложением, драйвером или службой. Например, после успешной загрузки драйвера в журнал заносится событие уведомления.
Аудит успехов	Любое событие безопасности, соответствующее успешно завершенному действию. Например, в случае успешного входа пользователя в систему в

	журнал заносится событие типа «Аудит успехов»
Аудит отказов	Любое событие безопасности, соответствующее отказу в доступе. Например, в случае неудачной попытки доступа пользователя к сетевому диску в журнал заносится событие типа «Аудит отказов».

Общее представление о параметрах ведения журнала событий

Программа «Просмотр событий» позволяет назначить параметры ведения журнала для каждого вида журнала событий. Чтобы назначить параметры ведения журнала, в дереве консоли щелкните правой кнопкой мыши нужный журнал, а затем выберите команду **Свойства**. На вкладке **Общие** задайте максимальный размер журнала и выберите режим удаления старых событий.

По умолчанию политика ведения журнала предусматривает удаление самых старых событий для записи новых в случае, если журнал заполнен, и хранение событий не менее 7 дней. Можно назначить особую политику замены записей для журнала каждого типа. Возможны следующие варианты действий по достижении максимального размера журнала:

Применение	**Действие**
Затирать старые события по необходимости	Новые записи продолжают заноситься в журнал после его заполнения. Каждое новое событие заменяет в журнале наиболее старое. Этот выбор хорош в тех случаях, когда нет необходимости в жестком контроле за работой системы.
Затирать события старее [*x*] **дней**	Перезапись событий, хранящихся дольше указанного времени. По умолчанию события хранятся 7 дней. Этот выбор хорош для еженедельной архивации журнала. Такой подход минимизирует вероятность потери важных записей и позволяет выдерживать размер журнала в разумных пределах.
Не затирать события	Очистка и сохранение журнала только вручную. Этот режим следует выбирать в тех случаях, когда потеря записей абсолютно недопустима (например, для журнала безопасности, когда безопасность системы исключительно важна).

Для установки максимального размера журналов, параметров замены записей и разрешений доступа к журналам событий можно также использовать вкладку «Групповая политика». Ведение журналов приложений и системы начинается автоматически при запуске компьютера.

Примечания

- Для выполнения этих процедур необходимо входить в группу Администраторы на сервере биллинга или получить соответствующие полномочия путем делегирования. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.

Форматы файлов с архивами журналов

Журнал событий можно сохранить в файле одного из трех форматов.

- **Журнал событий** (*.evt). Позволяет просматривать сохраненный файл журнала в окне просмотра событий.
- **Текст (разделители — табуляция)** (*.txt). Позволяет использовать сведения журнала в таких программах, как текстовый процессор. Журнал, сохраненный в формате .txt, нельзя открыть в окне «Просмотр событий».
- **Текст CSV (разделители — запятые)** (*.csv). Позволяет использовать сведения журнала в таких программах, как средства работы с электронными таблицами и базами данных. Журнал, сохраненный в формате .csv, нельзя открыть в окне «Просмотр событий».

Описания событий сохраняются во всех форматах. Данные каждой отдельной записи события сохраняются в следующем порядке.

1. Дата
2. Время
3. Источник
4. Тип
5. Категория
6. Событие
7. Пользователь
8. Компьютер
9. Описание

Чтобы сохранить журнал в файле

1. Запустите программу Просмотр событий.
2. В дереве консоли щелкните правой кнопкой мыши журнал, который требуется сохранить в файле, и выберите команду **Сохранить файл журнала как**.
3. В поле **Имя файла** введите имя файла, в котором будет сохранен журнал.
4. В поле со списком **Тип файла** выберите формат файла и нажмите кнопку **Сохранить**.

Примечания

- Для выполнения этой процедуры необходимо входить в группу Администраторы или Операторы архива на сервере биллинга или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы открыть окно «Просмотр событий», нажмите кнопку **Пуск**, выберите команду **Панель управления**, дважды щелкните значок **Администрирование**, а затем дважды щелкните значок **Просмотр событий**.
- Журнал событий, сохраненный в основном формате файла журнала (.evt), может впоследствии быть изучен в окне просмотра событий. Журнал, сохраненный в текстовом формате или формате с разделением записей запятыми (*.txt и *.csv, соответственно), может быть открыт в других программах, например в текстовых редакторах или в программах обработки электронных таблиц, но не в окне просмотра событий.

- Журналы событий сохраняются в основном формате файла журнала только на компьютере, где возникают события; например, при использовании окна просмотра событий для просмотра журналов событий на удаленном компьютере.
- Для сохранения локального журнала событий в основном формате файла журнала на другом компьютере введите *\\имя_удаленного_компьютера\ресурс* в поле **Имя файла**, а затем введите путь к сохраняемому файлу и его имя.
- При сохранении файла журнала сохраняется весь журнал, вне зависимости от установленного фильтра. При сохранении журнала порядок сортировки будет утерян. Однако журнал, сохраненный в файле, можно опять фильтровать и сортировать, открывая его в окне «Просмотр событий».
- Сохранение журнала в файле не влияет на содержимое текущего журнала событий.
- Чтобы уничтожить файл журнала, следует удалить файл в окне проводника Windows.

Чтобы очистить журнал событий

1. Запустите программу Просмотр событий.
2. В дереве консоли выберите журнал, который нужно очистить.
3. В меню **Действие** выберите команду **Стереть все события**.
4. Чтобы сохранить журнал перед очисткой, нажмите кнопку **Да**.

Примечания

- Для выполнения этой процедуры необходимо входить в группу Администраторы на сервере биллинга или получить соответствующие полномочия путем делегирования. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы Администраторы домена. При этом по соображениям безопасности рекомендуется использовать команду Запуск от имени.
- Чтобы открыть окно «Просмотр событий», нажмите кнопку **Пуск**, выберите команду **Панель управления**, дважды щелкните значок **Администрирование**, а затем дважды щелкните значок **Просмотр событий**.
- Невозможно очистить журнал, сохраненный в файле. Вместо этого следует удалить файл журнала.

Устранение неполадок

Вид неполадки.

> При просмотре события в поле **Пользователь** области сведений виден глобальный уникальный идентификатор (GUID) или код безопасности (SID). В этом поле должно быть имя пользователя .

Причина: Учетная запись пользователя, на которую ссылается событие, была удалена.

Решение: Восстановить эти сведения через оснастку «Просмотр событий» нельзя.

> Вы можете просматривать все журналы, кроме журнала **Безопасность**.

Причина: Вы не являетесь членом группы «Администраторы» или вам не были делегированы

соответствующие права на сервере биллинга.

Решение: Станьте членом группы Администраторы или получите соответствующие права на сервере биллинга путем делегирования. При этом по соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду Запуск от имени.

Вы можете просматривать журнал **Безопасность**, но не можете просматривать другие журналы.

Причина: Ваша учетная запись была добавлена в группу Гости на данном компьютере, но она также включена в группу Администраторы.

Решение: Удалите вашу учетную запись из группы Гости данного компьютера.

1. Откройте окно **Управление компьютером**. Если сервер биллинга является удаленным, то в дереве консоли щелкните правой кнопкой компонент **Управление компьютером (локальным)** и выберите команду **Подключение к другому компьютеру**.
2. Под заголовком **Локальные пользователи и группы** нажмите компонент **Группы**.
3. В области сведений дважды щелкните компонент **Гости**.
4. Выберите нужную учетную запись и нажмите кнопку **Удалить**.
5. Нажмите кнопку **OK**.

Примечания

- Эта проблема обычно возникает, когда администраторы добавляют группу, содержащую широкие категории пользователей (такие как группы **Все**, **Интерактивные** или **Прошедшие проверку**) в группу **Гости**.
- По умолчанию членам группы **Гости** явно запрещается доступ к ресурсам, таким как журналы событий. Поэтому следует избегать включения пользователей, имеющих административные права, в группу **Гости**.
- Возможно вам придется выйти и повторно войти в систему, чтобы внесенные изменения вступили в силу.

Не удается получить доступ к расширению оснастки «Управление компьютером» на сервере биллинга.

Причина. На сервере биллинга не запущена служба «Удаленный реестр».

Решение. Убедитесь, что на сервере биллинга запущена служба «Удаленный реестр». Для запуска службы на удаленном компьютере необходимо иметь соответствующие разрешения.