Глава 14

Мониторинг и поддержка Active Directory

В этой главе:

- Мониторинг Active Directory
- Поддержка базы данных Active Directory

Повседневный мониторинг и поддержка обязательны для оптимизации производительности и надежности Active Directory. Active Directory Domain Services (AD DS) — это распределенная сетевая служба, которая бывает очень сложной в крупных организациях и может ежедневно подвергаться многим изменениям, в частности обусловленным созданием и удалением учетных записей пользователей, изменением атрибутов объекта, группового членства и разрешений. Чтобы такого рода изменения, наряду с постоянно меняющимся сетевым и серверным окружением, в котором размещена служба, не влияли на производительность Active Directory, необходимо принять соответствующие меры. В этой главе будут изучены две фундаментальные возможности инфраструктуры AD DS: мониторинг контроллеров домена и поддержка базы данных Active Directory.

Мониторинг Active Directory

Чтобы поддерживать надежную службу каталогов организации, нужно контролировать степень исправности AD DS. Пользователи полагаются на эффективную работу службы каталогов, используемой для регистрации в сети, доступа к совместным ресурсам, извлечения и отправки электронной почты. Какие действия могут быть определены как критические, полностью зависит от степени исправности и доступности Active Directory.

Мониторинг AD DS состоит из комплекса задач, преследующих общую цель — сравнить текущее состояние и производительность базовых компонентов (емкость диска, степень использования процессора, конфигурация и т. д.) с рекомендуемыми значениями (базовым уровнем). Каждый компонент содержит различные индикаторы, такие как счетчики производительности, события системы и журналы регистрации (данные трассировки), а также сведения о конфигурации. Имея столь большой объем собранной информации, важно реализовать решение мониторинга, которое объединило бы эти индикаторы, чтобы предоставить сведения для активного и эффективного содействия реализации службы. Windows Server 2008 предоставляет расширенный набор инструментов, объединенных в средстве, получившем название Windows Reliability And Performance Monitor (Монитор производительности и надежности Windows). Эту новую консоль мониторинга используют для исследования в реальном времени различных компонентов, связанных с производительностью сервера, а также для сбора и последующего анализа данных журнала регистрации.

ПРИМЕЧАНИЕ Многие доступные на рынке наборы инструментов совмещают опции мониторинга индикаторов в легком в управлении интерфейсе. Важное значение они имеют в первую очередь для крупных организаций, правда, являются дорогими, довольно сложными и требуют значительных ресурсов. В Windows Reliability And Performance Monitor предусмотрены возможности, способные почти полностью избавить небольшие компании от необходимости покупать замысловатые и сложные решения мониторинга у сторонних разработчиков.

Чтобы правильно понимать мониторинг, необходимо знать, зачем он проводится, как и что нужно контролировать в Active Directory. Для работы службы каталогов на высоком уровне производительности и надежности нужно исследовать полученные данные, которые помогут определить подходящий метод мониторинга и поддержки окружения AD DS.

Из первоисточника: мониторинг Active Directory, часть 1

Важно уяснить, что подразумевается под мониторингом Active Directory в контексте управления. Конечно, оценка производительности поиска LDAP может быть полезной, но в то же время неполной. Успешный поиск LDAP еще не означает, что будет применена ожидаемая политика GPO или обнаружен ближайший контроллер домена Active Directory для аутентификации! В работе Active Directory участвуют функциональные компоненты, распределенные по всей системе Windows и тесно связанные с содержимым Active Directory. К примеру, запрос аутентификации приводит в действие последующие процессы и использует в Active Directory такие свойства, как поиски DNS, запросы LDAP, запросы Kerberos, параметры GPO, совместный доступ к сети для ресурса SYSVOL, каталоги HOME и пр. Кроме того, мониторинг Active Directory должен быть целостным, а не сфокусированным на отдельных компонентах. Если состояние Active Directory контролируется в целом, значит, дает реальную картину доступности и надежности службы каталогов для поддержки всего вашего бизнеса!

Ален Лиссуар

Для чего производится мониторинг Active Directory

Цель мониторинга Active Directory — распознание потенциальных проблем до того, как они спровоцируют затяжные периоды простоя службы. Очень важным для бизнеса является разрешение мониторинга поддержки соглашения об уровне услуг (service-level agreement, SLA) для заказчика (пользователя сети). Контроль состояния системы Active Directory позволяет своевременно выявлять проблемы и таким образом предотвращать прерывание работы службы.

ПРИМЕЧАНИЕ Соглашение SLA — это договор между провайдером службы (вами) и коллективом пользователей, в котором определены обязанности каждой стороны и обязательства по предоставлению определенного уровня службы указанного качества и в нужном объеме. В соглашении между отделом информационных технологий (IT) и коллективом пользователей оговариваются максимально допустимый уровень простоя системы и другие показатели производительности, в частности время входа в систему и время ответа запросов поддержки. В ответ

на обязательства поставщика службы обеспечивать определенную производительность и действующие стандарты устанавливается определенный объем пользования, например наличие не менее 10 000 пользователей в Active Directory.

Еще одна цель мониторинга состояния системы Active Directory заключается в необходимости отслеживать изменения инфраструктуры: увеличился ли размер базы данных Active Directory по сравнению с прошлым годом; все ли серверы глобальных каталогов (GC) пребывают в режиме онлайн; сколько времени занимает, скажем, копирование изменений из контроллера домена, расположенного во Франции, в контроллер домена в Австралии. Такого рода информация может предотвратить ошибки уже сегодня, а также предоставить важные данные для планирования на будущее.

Выгоды от мониторинга Active Directory Domain Services

Перечислены основные выгоды от мониторинга Active Directory:

- возможность без простоев управлять SLA с работающими пользователями;
- более высокая производительность Active Directory за счет устранения нераспознанных узких мест;
- снижение затрат на администрирование путем упреждающего обслуживания системы;
- улучшенные возможности масштабирования и планирования будущих изменений в инфраструктуре путем глубокого изучения компонентов Active Directory, их возможностей и методов использования;
- рост доверия к IT-отделу благодаря положительным отзывам пользователей.

Расходы на мониторинг Active Directory

Мониторинг вашей инфраструктуры Active Directory требует определенных затрат. Далее перечислены некоторые расходы на реализацию эффективного решения по мониторингу:

- время, необходимое для разработки и установки решения мониторинга, а также для управления им;
- значительные финансовые средства могут понадобиться для приобретения оборудования, а также инструментов управления и обучения, которые понадобятся при реализации мониторинга служб;
- часть полосы пропускания сети будет использована для мониторинга состояния Active Directory во всех контроллерах домена на предприятии;
- память и ресурсы процессора используются для выполнения приложений агента на целевых серверах и на компьютере консоли центрального мониторинга.

Следует обратить внимание на то обстоятельство, что стоимость мониторинга быстро возрастает при перемещении на платформу мониторинга масштаба предприятия, например Microsoft System Center Operations Manager. При реализации подобного решения возникнут дополнительные расходы на программное обеспечение, на обучение оператора и может понадобиться больше системных ресурсов, чем для многих встроенных инструментов мониторинга

Windows Server 2008. Однако системы мониторинга предприятия проверены, интегрированы, а также поддерживаются продуктами, имеющими функции, с помощью которых можно получить долгосрочную экономию средств и повысить эффективность эксплуатации среды управления и мониторинга.

Выбирая уровень мониторинга, следует учитывать, насколько оправданными будут затраты на его осуществление. В любом случае общие затраты на проведение мониторинга должны быть оправданными, а экономия средств и получаемые преимущества очевидными. Поэтому в крупных организациях считается рентабельным инвестировать в решения мониторинга. Мелкие и средние предприятия зачастую применяют инструменты мониторинга, встроенные в Windows Server 2008.

ПРИМЕЧАНИЕ В состав System Center Operations Manager входят средства управления событиями, мониторинга служб и предупреждения, создания отчетов и анализа тенденций. Это выполняется посредством центральной консоли, в которой агенты, реализуемые в управляемых узлах (контролируемых серверах), отправляют данные для анализа, отслеживания и отображения в одной консоли управления. Такая централизация позволяет управлять большим количеством серверов из одного места с помощью мощных инструментов для удаленного администрирования сервера. Система Operations Manager использует пакеты управления для расширения базы знаний определенных сетевых служб. Пакеты управления доступны многим службам и приложениям, в том числе Active Directory, Domain Name System (DNS), Microsoft Internet Information Services (IIS) и Microsoft Exchange Server. Дополнительные сведения об Operations Manager вы найдете по адресу *http://www.microsoft.com/systemcenter/opsmgr/default.mspx*.

Мониторинг надежности и производительности сервера

В состав Windows Server 2008 входит Reliability And Performance Monitor (Монитор надежности и производительности), применяемый для анализа системной производительности и предоставляющий детальную информацию о надежности отдельных компонентов, связанных с Windows и различными приложениями. Монитор Reliability And Performance Monitor запускается из меню Administrative Tools (Инструменты администрирования) и включает три инструмента мониторинга, которые могут быть использованы для различных целей администрирования и устранения возникающих проблем: Resource Overview (Обзор ресурсов), Performance Monitor (Монитор производительности) и Reliability Monitor (Монитор надежности).

Resource Overview (Обзор ресурсов)

Домашняя страница Resource Overview (Обзор ресурсов) содержит краткое описание использования и производительности центрального процессора, дисков, сети и памяти для сервера. Данные отображаются в режиме реального времени в виде четырех графиков. Как показано на рис. 14-1, выбор корневого узла Root node в Reliability And Performance Monitoru (Мониторе производительности и надежности) отображает Resource Overview (Обзор ресурсов). Расширив раздел сведений, можно получить дополнительную информацию о каждом компоненте. Например, чтобы определить активные в данный момент процессы и показатель нагрузки центрального процессора при выполнении определенной операции, можно раскрыть раздел центрального процессора.

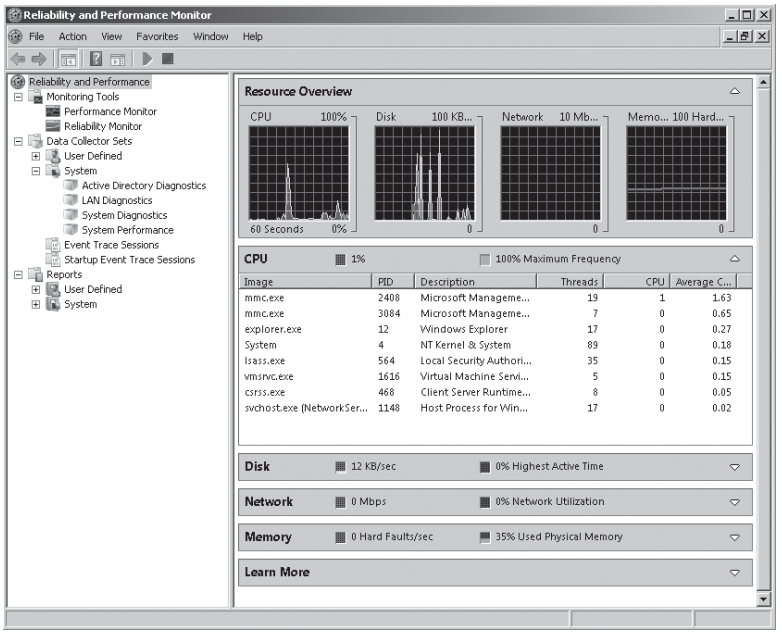

Рис. 14-1. Просмотр сведений Resource Overview

ПРИМЕЧАНИЕ Чтобы открыть автономную версию Resource Monitor (Монитора ресурсов), следует ввести в поле меню Пуск (Start) *perfmon /res*. Если Resource Overview не отображает реальное время, проверьте, запущен ли мониторинг, то есть щелкните зеленую кнопку пуска (только консоль Reliability And Performance (Производительность и надежность)) или выберите в меню Монитор (Monitor) пункт Запуски (Start) (только вид Resource Monitor (Монитор ресурсов)).

Performance Monitor (Монитор производительности)

Монитор производительности (ранее называвшийся Системный монитор) может быть использован для просмотра данных о производительности локального компьютера или нескольких удаленных компьютеров в режиме реального времени. Также с помощью Performance Monitor выполняется просмотр сохраненных журналов регистрации, которые значительно упрощают идентификацию тенденций производительности. Основные функциональные возможности Монитора производительности несущественно изменились по сравнению с предыдущими версиями Windows.

- Для оптимизации вида определенного счетчика щелкните счетчик внизу панели сведений и кнопку Highlight (Выделить) в панели инструментов (или нажмите Ctrl+H). Таким образом будет выделена выбранная строка графика счетчика, которую затем можно просмотреть.
- Переключайтесь между видами Line (Строка), Histogram (Гистограмма) и Report (Отчет), выбирая соответствующую кнопку в панели инструментов.
- График монитора производительности можно сохранять в виде HTML-страницы. Для этого нужно выполнить настройку графика с необходимыми счетчиками, щелкнуть график правой кнопкой мыши и выбрать Save Settings As (Сохранить параметры как). График будет сохранен в виде файла

HTML, который открывается в браузере. При открытии версии HTML графика отображение фиксируется. Чтобы перезапустить мониторинг, щелкните в браузере кнопку Unfreeze Display (Разморозить отображение), расположенную на панели инструментов Performance (Производительность).

- Сохраненный график можно импортировать обратно в Системный монитор, перетащив HTML-файл в окно Системного монитора; это удобный способ сохранения и перезагрузки часто используемых графиков производительности.
- Две новые группы безопасности в Windows Server 2008 — Performance Log Users (Пользователи журнала регистрации производительности) и Performance Monitor Users (Пользователи монитора производительности) — гарантируют получение доступа к важным данным производительности и возможность управления ими только надежными пользователями.

ПРИМЕЧАНИЕ Чтобы открыть автономную версию Монитора производительности, следует в поле меню Пуск (Start) ввести *perfmon /sys*.

По умолчанию счетчик % Processor Time (% Время процессора) предварительно загружается в Монитор производительности. Чтобы добавить дополнительные счетчики в консоль Монитора производительности, выполните следующие действия.

1. Щелкните правой кнопкой мыши панель сведений Монитора производительности и Add Counters (Добавить).
2. В диалоговом окне Add Counters (Добавить счетчики) щелкните <Local computer> (<Локальный компьютер>). Для мониторинга определенного компьютера, независимо от места, где запущена консоль, щелкните кнопку Browse (Обзор) и укажите имя компьютера.
3. Раскройте объект Performance Object (Объект производительности), затем щелкните счетчик, который нужно добавить.
4. Щелкните сначала кнопку Add (Добавить), а затем OK.

Хотя отличий в основных функциональных возможностях не наблюдается, однако в Мониторе производительности появились ожидаемые улучшения. На рис. 14-2 показаны некоторые из этих улучшений.

- **Улучшенные опции счетчиков** Теперь Монитор производительности предоставляет больше возможностей мониторинга просмотра счетчиков внутри панели сведений. Для типов графиков панелей Line (Строка) и Histogram (Гистограмма) имеется опция быстрого скрытия или показа выбранных счетчиков путем установки флажка, расположенного под столбцом Show (Показать). Кроме того, можно легко установить масштаб выбранных счетчиков, чтобы гарантировать видимость данных внутри графика. На рис. 14-2 представлен счетчик % Processor Time (% Время процессора) с установленным масштабом 10.
- **Всплывающие подсказки** В графике Line (Строка) можно использовать указатель мыши, чтобы определить точные данные счетчика производительности. На рис. 14-2 показано, как всплывающая подсказка содержит имя счетчика, значение и время точки на графике, где находится указатель мыши.

- **Инструмент «лупа»** Монитор производительности обеспечивает просмотр подробных сведений для регистрируемых данных с помощью увеличения в определенном промежутке времени. Обратите внимание, что нельзя использовать инструмент «лупа» при сборе данных в режиме реального времени.
- **Сравнение нескольких журналов регистрации** Автономная версия Монитора производительности имеет свойство, помогающее сравнить несколько журналов регистрации с базовым видом путем использования прозрачного наложения. При этом нужно открыть несколько автономных окон Монитора производительности, добавить журнал регистрации для сравнения в каждое окно и выбрать опции, которые находятся под меню Compare (Сравнить).

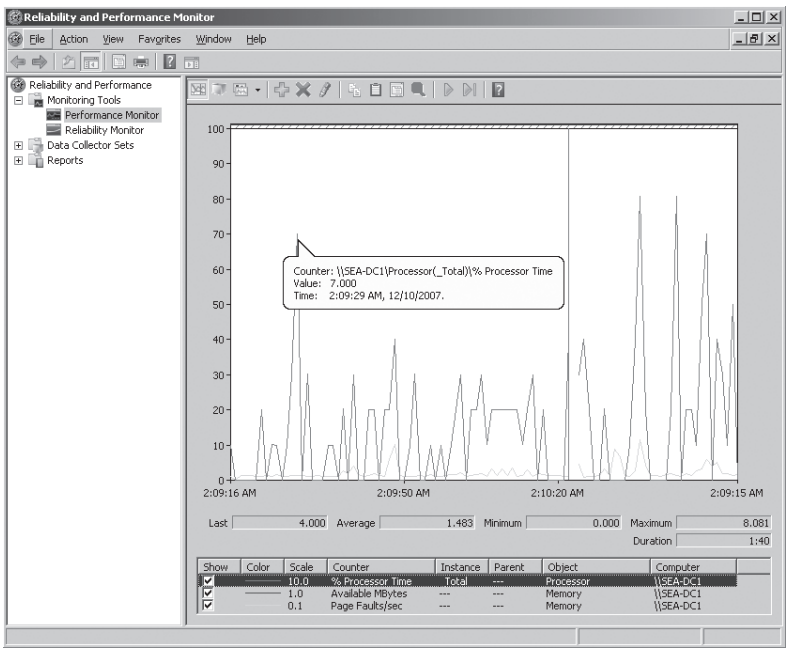

Рис. 14-2. Просмотр данных Монитора производительности

Reliability Monitor (Монитор надежности)

Монитор надежности предоставляет информацию об общей стабильности сервера. Индекс System Stability Index (Индекс стабильности системы) рассчитывается на основе данных, собранных как особые события, возникшие внутри сервера за определенный промежуток времени. Далее перечислены категории, составляющие события.

- **Software installs and uninstalls (Установка и удаление программного обеспечения)** Сюда входят приложения, установленные или удаленные

с помощью пакета установщика MSI, установки и удаления драйверов, установки и удаления обновлений программного обеспечения, и обновлений операционной системы, например пакетов обновлений или текущих исправлений.

- **Application failures (Сбой приложения)** Сообщает о событиях, связанных с зависаниями или аварийными отказами приложения.
- **Hardware failures (Сбой оборудования)** Уведомляет о событиях, связанных со сбоями в жестком диске и памяти.
- **Windows failures (Сбой Windows)** Сообщает о сбоях в загрузке, аварийных отказах операционной системы и сбоях в режиме ожидания.
- **Miscellaneous failures (Смешанный сбой)** Сообщает о неожиданном завершении работы системы.
- **System clock changes (Изменения в системных часах)** Уведомляет о любых изменениях в системных часах на сервере. Эта категория не появится в System Stability Report (Отчет стабильности системы), пока не будет выбран день, когда произошло определенное изменение в часах. Информационный значок появится в графике любого дня, когда возникло это изменение.

ПРИМЕЧАНИЕ Чтобы открыть автономную версию Монитора надежности, следует ввести в поле меню Пуск (Start) *perfmon /rel.*

Общая стабильность системы может быть определена путем просмотра графика System Stability Chart (График стабильности системы) либо разных видов сообщений отчетов System Stability Reports (Отчеты стабильности системы). System Stability Chart (График стабильности системы) отображает ежедневную оценку индекса стабильности от *1* до *10*. Оценка *10* указывает на то, что система работает стабильно; оценка *1* свидетельствует о крайне нестабильной работе системы. При выделении определенного дня в диаграмме можно просмотреть средний индекс и получить подробные сведения о сообщениях, расположенных внизу панели сведений.

Как показано на рис. 14-3, выделенная дата имеет индекс *8,81*, что соответствует менее стабильной работе системы по сравнению с предыдущими днями, зарегистрированными в System Stability Chart (График стабильности системы). Индикатор предупреждения отображается для категории Software (Un)Installs (Установка/удаление программного обеспечения), а индикаторы ошибок — для категорий Application Failures (Сбой приложения) и Miscellaneous Failures (Различные сбои). Раздел отчета System Stability Report (Отчет стабильности системы) содержит подробные сведения об ошибках, возникших в определенный день.

ПРИМЕЧАНИЕ Для Монитора надежности требуется сбор данных в течение 24 ч до вычисления индекса System Stability (Стабильность системы) или создания информации для System Stability Report (Отчет стабильности системы).

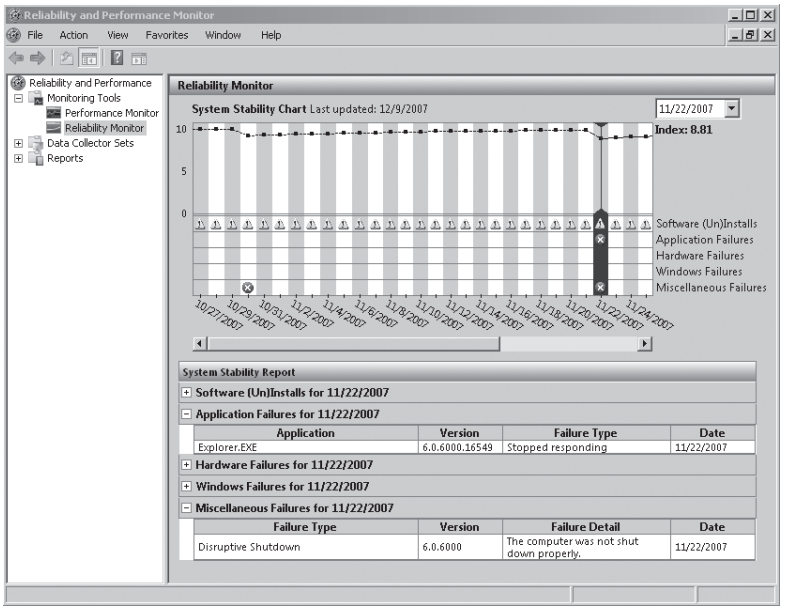

Рис. 14-3. Просмотр данных Монитора надежности

Обзор наборов и отчетов сбора данных

В Windows Server 2008 (как и в Windows Vista) представлена концепция Data Collector Set (наборов сбора данных). Набор Data Collector Set может содержать несколько мест сбора данных (*центров сбора данных*) для формирования одного конфигурируемого компонента. Этот компонент затем может быть сконфигурирован для предоставления таких опций, как диспетчеризация для целого набора сбора данных, безопасность для выполнения или просмотра набора сбора данных и выполнения определенных задач после окончания работы Data Collector Set по сбору данных.

Набор Data Collector Set содержит множество различных типов центров сбора данных.

- **Performance counters (счетчики производительности)** Используются для регистрации данных, связанных с производительностью системы. Можно добавить счетчики, которые используются для получения данных в режиме реального времени в мониторе Performance Monitor (Монитор производительности).
- **Event trace data (данные трассировки события)** Используется для регистрации информации на основе системных событий и событий приложений. Провайдеры трассировки события обычно устанавливаются с операционной системой либо предоставляются поставщиками приложений.
- **System configuration information (информация конфигурации системы)** Используется для регистрации информации, связанной с конфигурацией и изменениями в ключе Registry. Следует уяснить, какие конкретно ключи Registry нужно включить в набор Data Collector Set для мониторинга.

- **Performance counter alerts (предупреждения счетчика производительности)** Используется для конфигурации и предупреждения события, когда счетчик производительности достигает определенной пороговой величины или превышает ее. Например, можно сконфигурировать опцию на выполнение предупреждающего действия или задачи, когда показатель счетчика % Free Space (свободное место) на диске становится менее 20%. Предупреждающее действие бывает таким простым, как и регистрация записи в журнале регистрации событий приложения, или оно может задействовать последующий набор Data Collector Set для дополнительного мониторинга или возможностей трассировки. Можно также сконфигурировать Alert Task (задачу предупреждения) на выполнение определенного приложения, когда запускается предупреждение, например уведомление по электронной почте или административная утилита. Обратите внимание на то, что эта опция доступна при ручном создании набора Data Collector Set.

Узел Data Collector Set расположен в Reliability And Performance Monitor (Монитор производительности и надежности) и состоит из четырех контейнеров, используемых для хранения разных типов наборов Data Collector Set.

- **User Defined (Определяемый пользователем)** Позволяет создавать и хранить пользовательские наборы Data Collector Set либо вручную, либо из предварительно определенных шаблонов.
- **System (Система)** В зависимости от роли сервера этот контейнер по умолчанию хранит основанные на системе наборы Data Collector Set, используемые для предоставления диагностик Active Directory Diagnostics (Диагностика Active Directory), LAN Diagnostics (Диагностика сети), System Diagnostics (Диагностика системы) или System Performance (Производительности системы). Их нельзя непосредственно изменять, но можно использовать как шаблон для создания нового набора User Defined Data Collector Set (Определяемого пользователем набора сбора данных).
- **Event Trace Sessions (Сеансы трассировки события)** Используется для хранения наборов Data Collector Set на основе включенных провайдеров трассировки события.
- **Startup Event Trace Sessions (Сеансы трассировки события запуска)** Используется для хранения наборов Data Collector Set, содержащих провайдеры трассировки события, применяемые при мониторинге событий запуска.

На рис. 14-4 показан узел User Defined Data Collector Set (Определяемый пользователем набор сбора данных), который содержит два коллектора данных, используемых для сбора производительности для различных счетчиков и данных трассировки ядра NT.

Далее кратко изложен порядок создания набора Data Collector Set.

1. В Reliability And Performance Monitor (Монитор надежности и производительности) щелкните правой кнопкой мыши User Defined (Определяемый пользователем), выберите вариант New (Создать), а затем — Data Collector Set (Набор сбора данных).

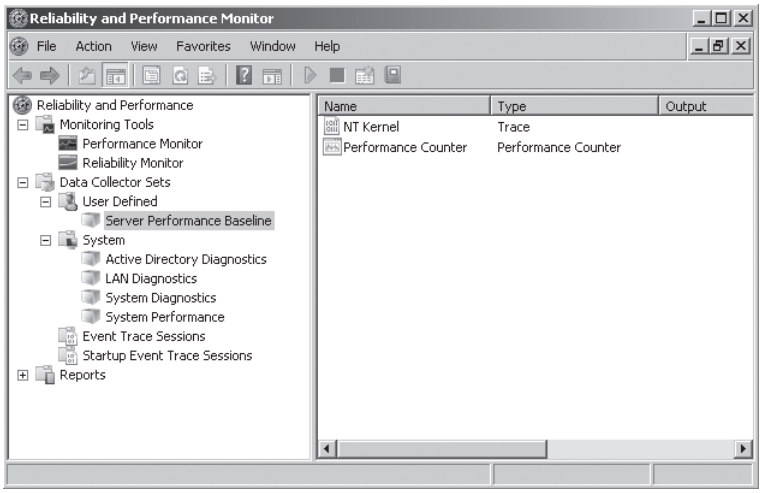

Рис. 14-4. Просмотр набора User Defined Data Collector Set (Определяемый пользователем набор сбора данных)

2. Укажите имя для набора Data Collector Set (Набор сбора данных) и уточните способ создания набора Data Collector Set — из шаблона или вручную.
3. Если вы будете использовать шаблон, то можно выбрать его на основе наборов System Data Collector Set (Системный набор сбора данных) или щелкнуть кнопку Browse (Обзор) и выбрать предварительно сконфигурированный шаблон на основе XML.
4. Чтобы создать новый набор Data Collector Set вручную, следует выбрать типы журналов регистрации данных и включить счетчик производительности, данные трассировки события или информацию о конфигурации системы. Можно также выбрать создание Performance Counter Alert (Предупреждение счетчика производительности). В зависимости от выбранных опций у вас будут особые страницы конфигурации для каждого типа журнала регистрации данных.
5. Выберите расположение, в котором вы хотели бы сохранить новый набор Data Collector Set. По умолчанию он сохранится в %systemdrive%\PerfLogs\Admin\.
6. Укажите учетную запись для использования набора Data Collector Set. По умолчанию наборы Data Collector Set выполняются как System user (Пользователя системы).
7. Щелкните Finish (Готово) для возвращения к консоли Reliability And Performance Monitor (Монитор производительности и надежности).
8. Щелкните правой кнопкой мыши набор Data Collector Set, а затем — Properties (Свойства) для изменения параметров целой коллекции. Например, возможно, понадобится указать расписание или условие остановки коллекции данных по прошествии определенного промежутка времени.
9. Для запуска набора Data Collector Set щелкните правой кнопкой мыши Data Collector Set (Набор сбора данных), а затем — Start (Запуск). Кол-

лекторы данных внутри набора начнут сбор информации в в соответствии с конфигурацией. После завершения сбора данных будет автоматически сгенерирован отчет и расположен под узлом Reports (Отчеты), как показано на рис. 14-5.

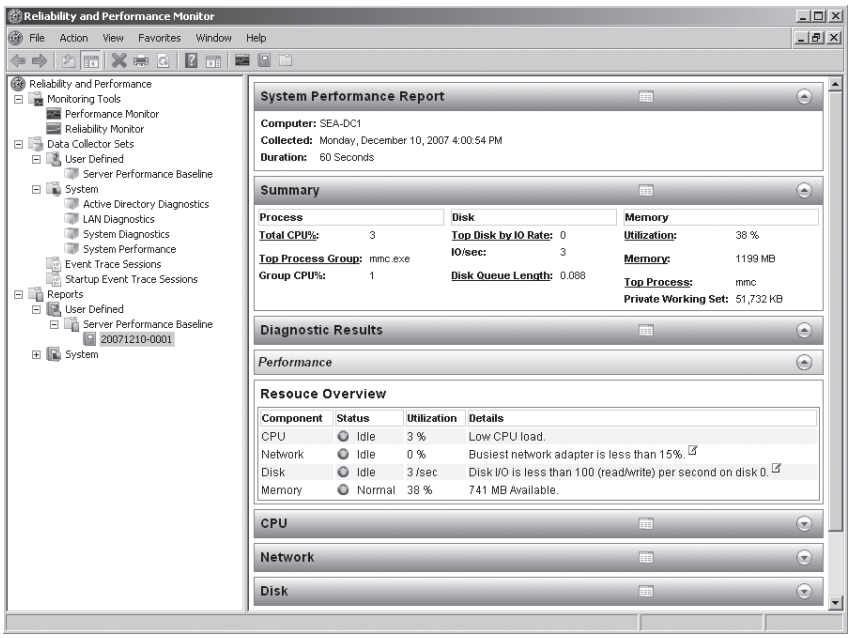

Рис. 14-5. Результаты отчета задачи сбора данных

Как осуществлять мониторинг Active Directory

Монитор Reliability And Performance Monitor (Монитор производительности и надежности) содержит различные счетчики Active Directory и события трассировки, которые можно использовать для достижения эффективного мониторинга системы. Процесс мониторинга Active Directory состоит из отслеживания этих ключевых индикаторов производительности и сравнения их с базовым условием, представляющим действие службы при нормальных параметрах. Различия между текущими результатами мониторинга по сравнению с исходными базовыми значениями помогут определить проблемы службы каталогов.

Как уже упоминалось ранее, набор Data Collector Set может содержать Performance Counter Alert (Предупреждения счетчика производительности). Если счетчик производительности превышает заданную пороговую величину производительности, то может быть сконфигурировано предупреждение, уведомляющее администратора сети (или оператора мониторинга в крупных организациях) о состоянии системы. Превышение пороговой величины производительности также может быть вызвано автоматическим действием, сконфигурированным внутри набора Data Collector Set для устранения проблемы или к минимизации дальнейшего ухудшения производительности либо состояния системы.

Далее описан порядок высокоуровневого процесса мониторинга Active Directory.

1. Определите, какие коллекторы данных нужны для мониторинга, а также необходимые в вашей организации исходные параметры. Сюда войдут счетчики производительности, информация трассировки и параметры системного реестра. Соглашение об уровне услуг (SLA) вашей организации является хорошим началом для предоставления информации об ожидаемых исходных параметрах и пороговых величинах для индикаторов производительности.
2. Создайте Data Collector Set (Набор сбора данных), включающий все необходимые коллекторы данных.
3. Запустите Data Collector Set (Набор сбора данных) для установки и документирования базового уровня производительности.
4. Определите пороговые величины для этих индикаторов производительности. (Другими словами, определите, на каком уровне необходимо предпринимать действия по предотвращению сбоя работы службы.)
5. Разработайте необходимую систему предупреждения для обработки достижения пороговой величины. Система предупреждения должна содержать:
   - уведомления оператора;
   - автоматические действия при наличии соответствующих действий;
   - действия, инициируемые оператором.
6. Разработайте систему отчетности для сбора ретроспективных данных о состоянии системы Active Directory. Можно использовать узел Reports (Отчеты) для содержания отчетов на основе даты, запущенной Data Collector Set (Набор сбора данных).
7. Реализуйте решение мониторинга для оценки производительности основных индикаторов в расписании, отображающем их разнообразие и влияние, которое оказывает каждый индикатор на состояние Active Directory.

Оставшаяся часть этого раздела посвящена изучению особенностей процесса мониторинга.

Установка базовых уровней и пороговых величин

После идентификации коллекторов данных и счетчиков производительности следует собрать данные их базовых уровней путем создания и запуска набора Data Collector Set, который представляет каждый тип коллектора данных в «нормальных пределах». «Нормальные пределы» должны включать значения высокого и низкого уровней для определенного счетчика производительности или события трассировки. Для получения более достоверных данных базового уровня следует собрать информацию о производительности за достаточный период времени, чтобы получить диапазон значений определенного параметра в период высокой и низкой активности. Например, при установке базового уровня для производительности запроса аутентификации убедитесь в мониторинге этого индикатора в течение периода, когда большинство пользователей входят в систему.

При определении значений базового уровня зафиксируйте эту информацию и поставьте дату создания версии документа. При установке пороговых величин эти значения пригодятся для идентификации тенденций производительности. Электронная таблица со столбцами для низких, средних и высоких значений для каждого счетчика, так же как для пороговых величин для предупреждений, хорошо подходит для этой цели.

ПРИМЕЧАНИЕ При изменении среды Active Directory (например, при увеличении количества пользователей или внесении изменений в контроллеры домена) восстановите базовые уровни. Базовый уровень всегда должен отображать самую актуальную краткую характеристику Active Directory, выполняемую при нормальных пределах производительности. Устаревший базовый уровень не эффективен для анализа текущих данных производительности.

Получив значения базового уровня, определите пороговую величину, которая должна генерировать задачу предупреждения или события. Помимо рекомендаций компании Microsoft, другой формулы для определения значений пороговой величины не существует. Поскольку каждая ситуация требует отдельного рассмотрения и подхода, существует необходимость определить на основе инфраструктуры сети, какой уровень производительности указывает, что счетчик производительности склоняется к прерыванию службы. При установке пороговых величин следует начинать с консервативных показателей. (Используйте значения, рекомендуемые Microsoft, или более низкие параметры.) В результате будет сгенерировано много предупреждений. По мере сбора данных о счетчике можно будет повысить пороговую величину, чтобы уменьшить количество предупреждений. Этот процесс может занять несколько месяцев, но в итоге будет корректно настроен для определенной реализации Active Directory.

Кроме того, необходимо иметь готовую стратегию ответа на предупреждение. При определении счетчиков, базового уровня и значений пороговой величины убедитесь в документировании действий по устранению неисправностей при возвращении индикатора в пределы нормы. Сюда входит устранение неисправности сбойной ситуации (например, возвращение контроллера домена в режим онлайн) или передача главной роли операций. Если система достигла максимального уровня вместимости, то, возможно, потребуется добавить пространство на диске или память для исправления ситуации. Другие предупреждения вызовут у вас желание выполнить поддержку Active Directory, такую как дефрагментацию файла базы данных Active Directory. Аналогичные ситуации будут описаны в разделе «Дефрагментация в автономном режиме базы данных Active Directory».

Счетчики производительности и пороговые величины

В представленных далее таблицах содержится список основных счетчиков производительности и пороговая величина, необходимые при мониторинге и регистрации производительности Active Directory. Важно запомнить, что сетевое окружение каждого предприятия будет иметь уникальные особенности, влияющие на применимость этих значений. Рассмотрите пороговые величины как отправной пункт и уточните эти значения, чтобы отобразить нужные вам данные.

Производительность Active Directory Счетчики производительности, перечисленные в табл. 14-1, выполняют мониторинг основных функций и служб Active Directory.

Табл. 14-1. Основные функции и службы Active Directory

Объект	Счетчик	Интервал	Почему важен счетчик
DirectoryServices/NTDS	DS Search sub-operations/sec (подоперации поиска DS/с)	Каждые 15 мин	Запросы поиска поддерева усложняют работу ресурсов системы. Любое существенное увеличение может вызвать проблемы производительности контроллера домена. Выполните проверку и убедитесь в корректности определения приложением цели применения данного контроллера домена
Process	% Processor Time (Instance=Isass) (% Время процессора (Instance = Isass))	Каждую минуту	Показывает соотношение времени центрального процессора, используемого службой Active Directory
DirectoryServices/NTDS	LDAP Searches/sec (Поиски LDAP/с)	Каждые 15 мин	Счетчик является хорошим индикатором общего использования контроллера домена. В идеале он должен быть равномерно распределен по контроллерам домена. Увеличение показателей в этом счетчике может свидетельствовать о том, что новое приложение работает с контроллером домена, или — о добавлении большего количества клиентов к сети
DirectoryServices/NTDS	LDAP Client Sessions (Сеансы клиента LDAP)	Каждые 5 мин	Определяет количество клиентов, подключенных в данный момент к контроллеру домена. Значительное увеличение данного показателя может свидетельствовать о сбое других машин вблизи этого контроллера домена. При анализе тенденций счетчика будет получена полезная информация о конкретном времени подключений пользователей и максимальном количестве клиентов, подключенных за один день

Табл. 14-1 (*окончание*)

Объект	Счетчик	Интервал	Почему важен счетчик
Process	Private Bytes (Instance=Isass) (Частные байты (Instance=Isass))	Каждые 15 мин	Полезен для анализа тенденций потребностей памяти контроллеров домена. Постоянно растущие показатели счетчика свидетельствуют о повышенном требовании рабочей станции, некорректном функционировании приложений (не закрывающиеся обработчики) или повышенном количестве рабочих станций, целью которых является этот контроллер домена. Если значения счетчика сильно отклоняются от нормальных величин других равноправных контроллеров домена, то следует определить источник запросов
Process	Handle Count (Instance=Isass) (Счет обработчика (Instance=Isass))	Каждые 15 мин	Эта статистика нужна для определения корректности работы приложения и наличия неправильно закрывающихся обработчиков. Счетчик увеличится линейно при добавлении рабочих станций клиента
Process	Virtual Bytes (Instance=Isass) (Виртуальные байты (Instance=Isass))	Каждые 15 мин	С помощью данного счетчика можно определить выполнение Active Directory при дефиците адресного пространства виртуальной памяти, что свидетельствует об утечке памяти. Убедитесь в обновлении новейшего пакета и составьте расписание перезагрузки в нерабочее время во избежание перебоев в системе. Счетчик можно также использовать для определения доступности менее 2 Гбайт виртуальной памяти

Пороговые величины определяются путем мониторинга базового уровня, если не задано другое. Эти счетчики можно добавить к Монитору производительности для предоставления данных в режиме реального времени или добавить коллектор данных Счетчика производительности либо предупреждение Счетчика производительности в набор Data Collector Set для регистрации производительности и возможностей предупреждений Active Directory.

Счетчики производительности репликации Счетчики производительности, рассмотренные в табл. 14-2, выполняют мониторинг количества повторных данных. Пороговые величины определяются базовыми уровнями, установленными ранее, если не указано иначе.

Табл. 14-2. Счетчики производительности репликации

Объект	Счетчик	Интервал	Почему важен счетчик
DirectoryServices/NTDS	DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec (Входные сжатые байты DRA (между сайтами, после сжатия) /с)	Каждые 15 мин (рекомендуемый)	Определяет количество данных репликации, поступающих на площадку. Существенное изменение в счетчике свидетельствует об изменении топологии репликации или о том, что значительная часть данных в Active Directory была добавлена или изменена
DirectoryServices/NTDS	DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec (Исходящие сжатые байты DRA (между сайтами, после сжатия)/с)	Каждые 15 мин (рекомендуемый)	Определяет количество данных репликации, исходящих из сайта. Значительное изменение в счетчике свидетельствует об изменении топологии репликации или о том, что большинство данных в Active Directory добавлено или изменено
DirectoryServices/NTDS	DRA Outbound Bytes Not Compressed (Исходящие не сжатые байты DRA)	Каждые 15 мин (рекомендуемый)	Определяет количество данных репликации, исходящих из контроллера домена, но направленных на цели внутри сайта
DirectoryServices/NTDS	DRA Outbound Bytes Total/sec (Сумма исходящих байтов DRA/с)	Каждые 15 мин (рекомендуемый)	Определяет количество данных репликации, исходящих из этого контроллера домена. Значительное изменение в счетчике свидетельствует об изменении топологии репликации или о том, что большинство данных в Active Directory добавлено либо изменено. Важно помнить, что за этим счетчиком производительности следует вести постоянное наблюдение

Производительность подсистемы безопасности Счетчики производительности, которые перечислены в табл. 14-3, выполняют мониторинг ключевых томов безопасности. Пороговые величины определяются путем мониторинга базового уровня, если не указано другое.

Табл. 14-3. Ключевые тома безопасности

Объект	Счетчик	Интервал	Почему важен счетчик
Security System-Wide Statistics (Статистика системной безопасности)	NTLM Authentications (Аутентификации NTLM)	Каждые 15 мин (рекомендуемый)	Определяет количество клиентов, выполняющих за секунду аутентификацию в контроллере домена, используя NTLM вместо технологии Kerberos (клиенты, использующие версии до Windows 2000)
Security System-Wide Statistics (Статистика системной безопасности)	KDC AS Requests (Запросы KDC AS)	Каждые 15 мин (рекомендуемый)	Определяет количество мандатов сеанса, выдаваемых за секунду Key Distribution Center (KDC) (Центр распределения ключей). Этот индикатор хорошо использовать для наблюдения за влиянием изменений жизненного цикла мандата
Security System-Wide Statistics (Статистика системной безопасности)	Kerberos Authentications (Аутентификации технологии Kerberos)	Каждые 15 мин (рекомендуемый)	Определяет количество загрузки аутентификации, возлагаемой на KDC. Этот индикатор хорошо использовать для анализа тенденций
Security System-Wide Statistics (Статистика системной безопасности)	KDC TGS Requests (Запросы KDC TGS)	Каждые 15 мин (рекомендуемый)	Указывает количество мандатов Ticket-Granting Ticket (TGT) (мандатов на выдачу мандатов), выпускаемых KDC. Этот индикатор рекомендуется использовать для наблюдения за влиянием изменений жизненного цикла мандата

Производительность основной операционной системы Счетчики производительности, которые находятся в списке в табл. 14-4, выполняют мониторинг индикаторов основной операционной системы и имеют прямое влияние на производительность Active Directory.

Табл. 14-4. Индикаторы основной операционной системы

Объект	Счетчик	Интервал	Пороговая величина	Значимость превышения значения пороговой величины
Memory (Память)	Page Faults/sec (Страничные ошибки/с)	Каждые 5 мин	700/с	Высокий процент страничных ошибок характерен при недостаточной физической памяти

(*см. след. стр.*)

Табл. 14-4. (*окончание*)

Объект	Счетчик	Интервал	Пороговая величина	Значимость превышения значения пороговой величины
PhysicalDisk (Физический диск)	Current Disk Queue Length	Каждую минуту	Два усредненных в течение трех интервалов	Выполняет мониторинг томов, содержащих файл Ntds.dit и файлы .log. Этот счетчик определяет незавершенную работу диска запросов ввода/вывода. Чтобы решить эти проблемы, необходимо увеличить объем диска и пропускную способность контроллера
Processor (Процессор)	% DPC Time (Instance=_Total) (% Время DPC (Instance=_Total))	Каждые 15 мин	10	Определяет работу, которая была отложена, поскольку контроллер домена был задействован в других процессах или был слишком перегружен. Превышение пороговой величины свидетельствует о вероятной перегруженности процессора
System (Система)	Processor Queue Length (Длина очереди процессора)	Каждую минуту	Шесть усредненных в течение пяти интервалов	Центральный процессор недостаточно быстрый для обработки запросов по мере их появления. Если топология репликации правильная и условие не вызвано преодолением отказа из другого контроллера домена, следует рассмотреть как один из вариантов обновление центрального процессора
Memory (Память)	Available MBytes (Доступное количество мегабайт)	Каждые 15 мин	4 Мбайт	Определяет объем израсходованной памяти. Существует вероятность сбоя
Processor (Процессор)	% Processor Time (Instance=_Total) (% Время процессора (Instance=_Total))	Каждую минуту	85% усредненных в течение трех интервалов	Уведомляет о перегрузке центрального процессора. Определите, вызвана ли загрузка CPU Active Directory, изучив объект Process (Процесс), счетчик % Processor Time (% Время процессора), экземпляр Isass
System (Система)	Context Switches/sec (Переключения контекста/с)	Каждые 15 мин	70 000	Определяет чрезмерные переходы. Возможно, задействовано слишком много приложений или служб, либо их нагрузка на систему очень высокая. Рассмотрите возможность разгрузки части этих запросов
System (Система)	System Up Time (Время работы системы)	Каждые 15 мин		Важный счетчик для оценки надежности контроллера домена

Мониторинг Active Directory с помощью Event Viewer

Помимо использования Reliability And Performance Monitor (Монитор производительности и надежности) для мониторинга Active Directory, следует также просматривать содержимое журналов регистрации событий с помощью административного инструмента Event Viewer (Просмотр событий). По умолчанию Event Viewer отображает следующие пять журналов.

- **Application (Приложение)** Содержит информацию о событиях, зарегистрированных приложениями или программами.
- **Security (Безопасность)** Содержит данные о допустимых и недопустимых попытках входа в систему, а также события, связанные с использованием ресурсов, в частности такие, как открытие и удаление файлов или других объектов.
- **Setup (Установка)** Содержит информацию о событиях, зарегистрированных операционной системой и приложениями во время установки.
- **System (Система)** Содержит информацию о событиях, зарегистрированных компонентами системы Windows.
- **Forwarded Events (Перенаправленные события)** Используется для хранения событий, собранных из других удаленных компьютеров. Для сбора событий из удаленных компьютеров необходимо сконфигурировать подписку.

Кроме того, для серверов с системой Windows Server 2008, сконфигурированной как контроллеры домена, журналы регистрации событий будут отображаться под узлом Applications and Services Logs (Журналы регистрации приложений и служб) инструмента Event Viewer (Просмотр событий).

- **Directory Service (Служба каталогов)** Содержит события, зарегистрированные Active Directory.
- **DFS Replication (Репликация DFS)** Содержит события, зарегистрированные системой Distributed File System (Распределенная файловая система). Этот журнал регистрации будет предоставлять информацию, связанную с репликацией SYSVOL.

Если контроллер домена Windows Server 2008 является сервером DNS, то будет отображаться еще один журнал.

- **DNS Server (Сервер DNS)** Содержит события, зарегистрированные службой Сервера DNS.

Для просмотра журналов регистрации событий щелкните кнопку Event Viewer (Просмотр событий) в папке Administrative Tools (Инструменты администрирования). Выберите журнал регистрации событий той службы, для которой хотите выполнить мониторинг. На левой панели на рис. 14-6 перечислены все журналы регистрации событий для контроллера домена, где функционирует система Windows Server 2008, которая также является сервером DNS.

В журнале регистрации событий просмотрите типы событий для Errors (Ошибки) и Warnings (Предупреждения). Для отображения подробных сведений о событии в журнале дважды щелкните его кнопкой мыши. На рис. 14-7 приведены подробные сведения события Warning (Предупреждение) (*ID события 2886*) из журнала Directory Service (Служба каталогов).

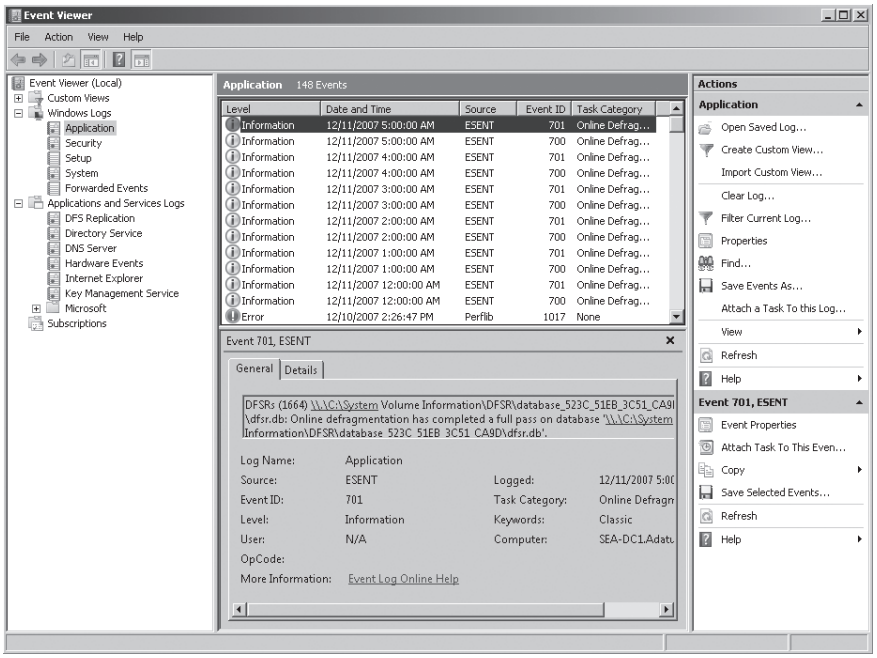

Рис. 14-6. Инструменты администрирования Event Viewer (Просмотр событий) с журналами регистрации событий

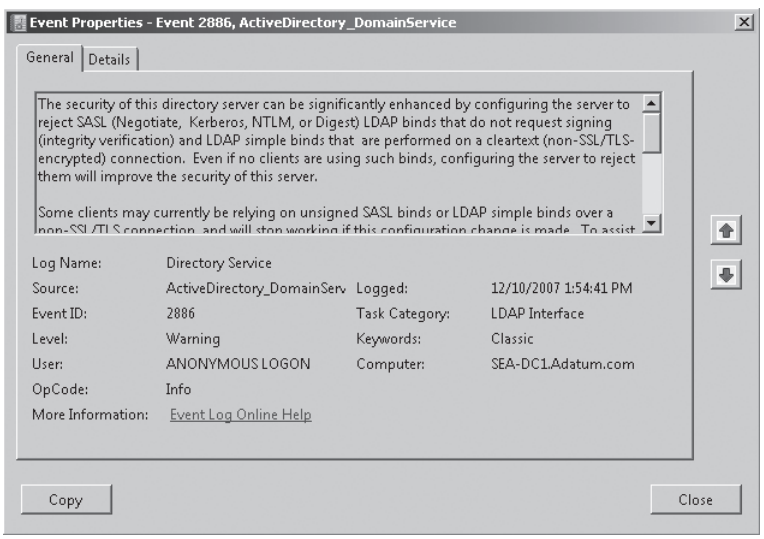

Рис. 14-7. Окно Event Properties (Свойства события) для записи журнала регистрации событий

Что должно подвергаться мониторингу

Для мониторинга общего состояния системы Active Directory нужно выполнить мониторинг индикаторов производительности, связанной со службами и сервером. Необходимо убедиться в том, что Active Directory и контроллеры домена функционируют оптимальным образом.

При разработке решения мониторинга следует выполнить мониторинг следующих компонентов производительности.

- **Служба Active Directory** Эти индикаторы производительности подвергаются мониторингу с помощью счетчиков службы Directory Service (Служба каталогов) и событий трассировки в Reliability And Performance Monitor (Монитор производительности и надежности).
- **Репликация Active Directory** Производительность репликации важна для того, чтобы гарантировать поддержку целостности данных в домене.
- **Хранилище базы данных Active Directory** Томы диска, содержащие файл базы данных Ntds.dit и файлы .log, имеют достаточно свободного пространства, чтобы позволить нормальный рост и функциональность.
- **Производительность DNS и состояние сервера** Поскольку Active Directory полагается на DNS как на локатор службы, сервер DNS и служба должны действовать так, чтобы система Active Directory отвечала требованиям уровня службы.
- **File Replication Service (FRS) (Служба репликации файлов) и Distributed File System Replication (DFSR) (Репликация распределенной файловой системы)** Служба FRS должна выполняться так, чтобы гарантировать работу совместно используемым системным томом (SYSVOL) репликации через домен. Если Windows Server 2008 находится в функциональном режиме, то можно использовать DFST для репликации SYSVOL. Здесь мониторинг нужен для гарантий надлежащей производительности.
- **Состояние системы контроллера домена** Мониторинг этой области должен повлиять на общее состояние системы, включая счетчики памяти, утилизацию процессора и разделение по страницам. Необходимо также убедиться в том, что подходящие параметры времени и часового пояса синхронизированы между всеми серверами, что является решающим фактором для репликации и надлежащей аутентификации.
- **Состояние леса** Мониторинг этой области нужен для того, чтобы убедиться в надежности и доступности сайта.
- **Мастера операций и глобальные роли каталога** Для каждой роли мастера Operations Master (Мастер операций) выполните мониторинг, чтобы убедиться в состоянии сервера и в глобальной доступности каталога.

Из первоисточника: мониторинг Active Directory, часть 2

Мониторинг Active Directory — это обширная и важная тема для исследования. Как уже объяснялось ранее, целостный мониторинг Active Directory необходим. В Windows есть приложения и программы, которые являются периферийными по отношению к Active Directory и нуждаются в мониторинге. Таким образом, появилась возможность отслеживать общее состояние Active Directory. В частности, сюда включается синхронизация времени во избежание задержек на промежутки времени более пяти минут между контроллерами домена (если задержка более пяти минут, то расхождение может сделать недействительным мандат Kerberos и лишить контроллеры домена и пользователей возможности произвести аутентификацию). Кроме того, потребуется мониторинг таких важных служб Active Directory, как NTFRS, DFSR и RDC W32Time. Все они обеспечивают поддержку системе Active Directory или зависят от нее. Другие не менее важные аспекты, например, доступное пространство на системном диске и объем базы данных Active Directory, также целесообразно отслеживать.

Утилизацию центрального процессора Knowledge Consistency Checker (KCC) (Проверка последовательности знаний) обычно не подвергают мониторингу, но в некоторых случаях это делать весьма полезно — особенно в крупных инфраструктурах Active Directory. Следует отметить, что KCC — это проверка, отвечающая за подлинность и построение топологии Active Directory с помощью создания требуемых объектов подключения. Хотя производительность KCC значительно улучшилась по сравнению с версией Windows 2000, было бы интересно провести мониторинг использования центрального процессора KCC в контроллерах домена, расположенных в концентраторах инфраструктуры Active Directory.

Чтобы определить активность KCC, следует изменить уровень диагностики KCC до трех. Для этого установите значение ключа системного реестра Knowledge Consistency Checker равным 3. Ключ системного реестра находится в системном реестре HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics. После установки уровня на 3 KCC будет создавать записи журнала Event Log (Журнал регистрации событий) в Directory Service Event Log (Журнал регистрации событий службы каталогов) при каждом его запуске. События 1009 и 1013 с исходным именем NTDS KCC будут показывать время запуска и время остановки KCC соответственно. Тем временем можно проследить использование центрального процессора и увидеть воздействие KCC на данный процессор. Это может быть выгодно для распределения нагрузки, например, между серверами, вычисляющими топологию и обрабатывающими запросы аутентификации.

Важно помнить, что при мониторинге Active Directory нужно оценивать систему целостно, что, в свою очередь, поможет избежать многих побочных эффектов и проблем, поскольку вы привыкнете к работе с системой Active Directory в целом, а не с каждым компонентом программного обеспечения отдельно.

Ален Лиссуар

Репликация мониторинга

Если организация имеет более одного контроллера домена, то для мониторинга нужна репликация Active Directory. Репликация между контроллерами домена зачастую подвергается мониторингу с помощью Repadmin.exe, Dcdiag.exe и журнала регистрации Directory Service (Служба каталогов) (описан ранее с Event Viewer (Просмотр событий)).

Repadmin — это инструмент командной строки, сообщающий о сбоях в ссылке репликации между двумя партнерами репликации. Следующая команда отображает партнеров репликации и любые сбои ссылки репликации для контроллера домена DC1 в домене Contoso.com:

```
repadmin/showrepldc1.contoso.com
```

Dcdiag — это инструмент командной строки, который может проверить регистрацию DNS контроллера домена. Выполните проверку и убедитесь в том, что идентификаторы безопасности (Security Identifier, SID) в заголовках контекста наименования (naming context, NC) имеют соответствующие разрешения на репликацию, проанализируйте состояние контроллеров домена в лесе или на предприятии. Для получения полного списка опций Dcdiag введите *dcdiag*. Следующая команда проверяет приложение на наличие ошибок между контроллерами домена:

```
dcdiag/test:replications
```

В заключение журнал регистрации Directory Service (Служба каталогов) сообщает об ошибках репликации, возникающих после установленной ссылки репликации. В частности, необходимо просмотреть журнал регистрации Directory Service на наличие события репликации, в котором типом события является Error (Ошибка) или Warning (Предупреждение). Далее рассмотрены примеры наиболее распространенных ошибок репликации, поскольку они содержатся в журнале регистрации Directory Service (Службы каталогов).

- **Event ID 1311 (Идентификатор события 1311)** Информация о конфигурации репликации в инструменте администрирования Active Directory Sites And Services (Сайты и службы Active Directory) не полностью отображает физическую топологию сети. Эта ошибка указывает на то, что один или несколько контроллеров домена или серверы-плацдармы (bridgehead) находятся в автономном режиме или что в серверах-плацдармах отсутствуют требуемые контексты именования.
- **Event ID 1265 (Access denied) (Идентификатор события 1265 (Доступ запрещен))** Эта ошибка может возникнуть в том случае, если локальному контроллеру домена не удалось аутентифицировать партнера репликации при создании ссылки репликации или попытке выполнить репликацию через существующую ссылку. Обычно ошибка происходит в то время, когда контроллер домена был отключен от остальной части сети в течение длительного времени, а его пароль учетной записи компьютера не синхронизирован с паролем учетной записи компьютера, сохраненным в каталоге партнера репликации.

Из первоисточника: мониторинг репликации Active Directory

Мониторинг репликации Active Directory осуществляется несколькими способами. Конечно, подлинность конфигурации можно проверить с помощью Dcdiag и убедиться в том, что Active Directory отвечает всем условиям для правильной репликации. Это является проактивной проверкой, с помощью которой можно провести мониторинг до появления проблем. Можно также выполнить мониторинг репликации Active Directory «после случившегося» путем проверки неисправностей в репликации. В данном случае мониторинга можно достичь при проверке событий в журнале регистрации событий или особых неисправностей репликации с помощью REPADMIN.

Еще одним способом проверки подлинности репликации Active Directory является прочтение таких совместно используемых параметров в контроллере домена Active Directory, как роли FSMO. Если система работает нормально, без сбоев, то роли FSMO, о которых было уведомлено для данного домена в конкретном лесе, всегда должны быть одинаковыми для всех контроллеров домена внутри данного формата и леса. Собирая всю информацию на уровне каждого контроллера домена и сообщая о ней центрально (то есть путем выгрузки результатов в совместно используемый ресурс), роль FSMO сможет легко провести сравнение. Любая противоречивость в роли FSMO обнаружит проблему репликации для контроллера домена, сообщающего разные результаты.

Последний, не менее важный способ мониторинга репликации Active Directory может быть основан на инжекции изменения. Эта технология обеспечивает обновление данного назначенного объекта AD для мониторинга репликации. Например, можно написать сценарий, основанный на ADSI, изменяющий объект AD в выбранном контроллере домена. (Сценарий может выполняться регулярно внутри контекста Task Scheduler (Планировщика задач).) Изменение, например, состоит из операции записи даты и времени в атрибуте строки *description* пользовательского объекта. Поскольку Active Directory выполняет репликацию этого типа изменения автоматически, ожидается, что такая информацию будет в какой-то момент видна обновленной во всех остальных контроллерах домена Active Directory. Тем временем все остальные контроллеры домена могут регулярно выполнять добавочный сценарий, который прочитывает этот же объект и сравнивает атрибут даты/времени *description* со значением атрибута *whenChanged*.

Таким образом, последний сценарий может определить успешную репликацию последнего ожидаемого изменения (атрибут *description*, содержащий обновленное значение даты/времени). Затем он может просчитать время, затраченное на то, чтобы появилось изменение репликации, путем определения разницы во времени между атрибутом *description*, содержащим исходную запись даты/времени, и датой/временем, содержащимися в атрибуте *whenChanged*.

Это позволит установить время ожидания репликации каталога, которое уведомит о соответствии разработки и инфраструктуры Active Directory вашим ожиданиям относительно скорости изменения репликации, что является частью требований к системе. Следовательно, это очень эффективный способ проверки того, насколько удачно решение, во время разработки, позволяющий выполнить некоторые действия, чтобы соответствовать SLA-репликации.

Конечно же, для подобного мониторинга требуется написание сценария. Обратившись к разделу технического описания на веб-сайте *http://www.lissware.net*, вы получите основанные на ADSI примеры создания собственных сценариев для выполнения этого действия.

Microsoft Active Directory Management Pack для Microsoft Operations Manager (MOM) 2005 и Operations Manager 2007 реализует именно эту логику и применяет MOM для объединения и сравнения результатов, собранных во всех контроллерах домена в лесе, для определения времени ожидания репликации.

Ален Лиссуар

Поддержка базы данных Active Directory

Одним из важнейших заданий управления является поддержка базы данных Active Directory. Обычно вам редко приходится управлять Active Directory непосредственно, поскольку регулярное автоматическое управление базой данных будет поддерживать ее состояние практически во всех ситуациях, кроме исключительных случаев. В автоматические процессы входят дефрагментация в режиме онлайн базы данных Active Directory, а также процесс сборки мусора с целью очищения удаленных элементов. Для непосредственного управления базой данных Active Directory в Windows Server 2008 предусмотрен инструмент Ntdsutil.

Сборка мусора

Одним из важнейших автоматических процессов, выполняемых с целью поддержки базы данных Active Directory, является сборка мусора. Этот процесс происходит во всех контроллерах домена каждые 12 ч. Во время его выполнения восстанавливается свободное пространство в базе данных Active Directory.

Процесс сборки мусора начинается с удаления устаревших записей из базы данных. Устаревшие записи — это остатки объектов, удаленных из Active Directory, например учетная запись пользователя, которая удаляется не сразу. Поэтому атрибуту *isDeleted* в объекте задается значение *true*, объект обозначается как устаревший и большинство атрибутов удаляются из него. Сохраняются только несколько атрибутов, необходимых для идентификации объекта. В частности, это глобально уникальный идентификатор (Globally Unique Identifier, GUID), SID, порядковый номер обновления (Update Sequence Number, USN) и известное имя. Эта устаревшая запись затем реплицируется в другие контроллеры домена в домене. Каждый контроллер домена поддерживает копию объекта

с устаревшими записями до завершения жизненного цикла этой записи. По умолчанию жизненный цикл устаревших записей составляет 180 дней. Во время последующей сборки мусора после завершения жизненного цикла устаревших записей объект удаляется из базы данных.

Затем процесс сборки мусора удаляет из журнала регистрации все ненужные файлы транзакции. Каждое внесенное в базу данных Active Directory изменение сначала записывается в журнал регистрации транзакции, а затем фиксируется в базе данных. Процесс сборки мусора удаляет все журналы регистрации транзакции, которые не содержат незафиксированных транзакций.

Как уже упоминалось, сборка мусора выполняется на каждом контроллере домена с интервалом 12 ч, который можно изменить вместе с атрибутом *garbageCollPeriod*. Чтобы изменить этот параметр, можно использовать Adsiedit.msc. Откройте ADSI Edit (Правка ADSI) в меню Administrative Tools (Инструменты администрирования) и подключитесь к Configuration (Конфигурация). Затем разверните CN=Configuration, CN=Services, CN=Windows NT и выберите CN=Directory Service. Щелкните CN=Directory Service правой кнопкой мыши, найдите атрибут *garbageCollPeriod* и сконфигурируйте нужное значение. Следует отметить, что в большинстве случаев вам не придется изменять данный параметр. На рис. 14-8 этот атрибут показан в ADSI Edit (Правка ADSI).

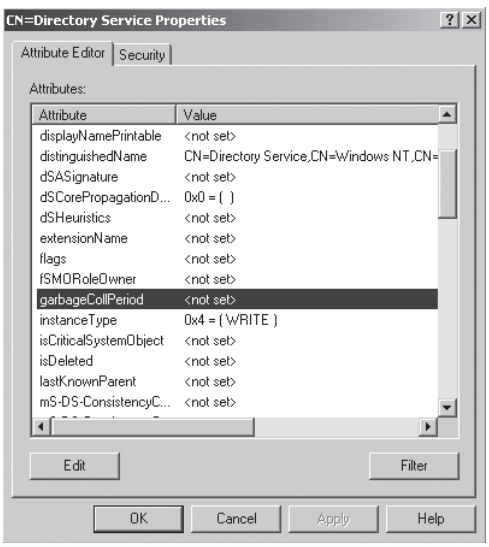

Рис. 14-8. Атрибут *garbageCallPeriod* в ADSI Edit (Правка ADSI)

Дефрагментация в режиме онлайн

Завершающим этапом в процессе сборки мусора является дефрагментация в режиме онлайн базы данных Active Directory. В результате ее выполнения очищается пространство в базе данных и преобразуется хранилище объектов Active Directory. Дефрагментация в режиме онлайн применяется для управления объектами в базе данных.

Во время нормального функционирования система базы данных Active Directory оптимизируется, благодаря чему изменения в нее можно вносить

с максимальной скоростью. Когда объект удаляется из Active Directory, страница базы данных, на которой он хранится, загружается в память компьютера и объект удаляется со страницы. При добавлении объектов в Active Directory они записываются на страницы базы данных без оптимизации хранилища для дальнейшего извлечения этой информации. После нескольких часов внесения изменений в базу данных с максимальной скоростью хранилище данных может быть не оптимизировано. Например, база данных может содержать пустые страницы, с которых были удалены объекты, много страниц с некоторыми удаленными элементами либо объекты Active Directory, расположенные на разных страницах по всей базе данных.

Процесс онлайн-дефрагментации очищает базу данных и возвращает ее в более оптимизированное состояние. Если некоторые записи на странице базы данных были удалены, то записи с других страниц могут быть перемещены на страницу для оптимизации хранилища и извлечения информации. Объекты, которые должны храниться вместе, перемещаются на одну страницу базы данных или на смежные страницы. Одним из ограничений процесса онлайн-дефрагментации является то, что он не уменьшает размер базы данных Active Directory. Если из Active Directory удалено большое количество объектов, то в процессе дефрагментации возможно создание в базе данных пустых страниц, поскольку объекты перемещаются по базе данных. Однако процесс онлайн-дефрагментации не может удалить такие пустые страницы. Для этого необходимо использовать процесс дефрагментации в автономном режиме.

Процесс дефрагментации онлайн выполняется каждые 12 ч как часть процесса сборки мусора. По его завершении в журнале регистрации Directory Service (Службы каталогов) делается запись об удачном завершении процесса. На рис. 14-9 приведен пример сообщения журнала регистрации событий.

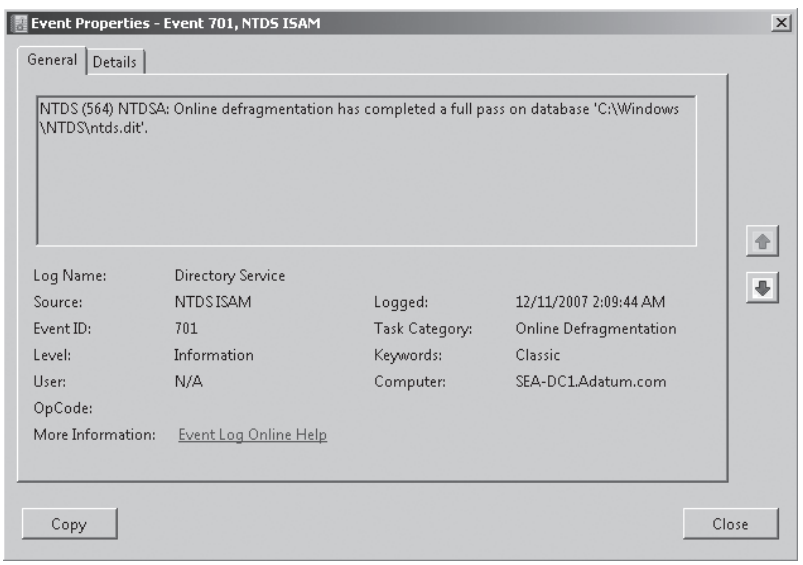

Рис. 14-9. Сообщение журнала регистрации Directory Service (Службы каталогов), указывающее на успешную онлайн-дефрагментацию

Дефрагментация базы данных Active Directory в автономном режиме

Как уже упоминалось ранее, процесс онлайн-дефрагментации не уменьшает размер базы данных Active Directory. Обычно это не является проблемой, поскольку страницы базы данных, очищаемые при его выполнении, используются повторно, в то время как новые объекты добавляются в Active Directory. Однако в некоторых случаях, возможно, дефрагментацию в автономном режиме потребуется применять с целью уменьшения общего размера базы данных. Например, если вы удаляете глобальный каталог из контроллера домена, то для очистки пространства дефрагментацию следует выполнить в автономном режиме. Дефрагментация в автономном режиме особенно актуальна в среде с несколькими доменами, где глобальный каталог может стать очень объемным. Дефрагментацию, возможно, потребуется использовать в автономном режиме и в том случае, если вы удалили множество объектов из домена Active Directory.

Вот как выполняется дефрагментация в автономном режиме.

1. Выполните резервное копирование информации Active Directory в контроллере домена. Этот процесс описан в главе 15.
2. Для контроллеров домена Windows Server 2008 откройте консоль Services (Службы) и остановите службу Active Directory Domain Services (Службы домена Active Directory) и все связанные службы, следуя подсказке (или введите в командной строке *net stop ntds*).

ПРИМЕЧАНИЕ При использовании Windows Server 2000/2003 перезагрузите контроллер домена. При перезагрузке сервера нажмите F8 для отображения Advanced Boot Options (Дополнительные опции загрузки) и выберите Directory Services Restore Mode (Режим восстановления служб каталогов). После перезагрузки сервера войдите в систему, используя локальную учетную запись Administrator (Администратор). Используйте пароль, введенный как пароль для Directory Services Restore Mode (Режим восстановления служб каталогов), при поддержке контроллера домена.

3. Откройте командную строку и введите *ntdsutil*.
4. В строке Ntdsutil введите *Activate Instance NTDS* (Активировать экземпляр NTDS).
5. В строке Ntdsutil введите *files*.
6. В строке File Maintenance (Поддержка файлов) введите *info*. Эта опция отображает текущую информацию о пути и размере базы данных Active Directory, а также файлы журнала регистрации.
7. Введите *compact to drive:\directory*. Выберите накопитель и каталог, имеющие достаточно пространства для хранения целой базы данных. Если имя пути каталога содержит пробелы, то путь должен быть заключен в кавычки.
8. В процессе дефрагментации в автономном режиме создается новая база данных с именем Ntds.dit в заданном местоположении. Поскольку эта база данных копируется в новое место, она подвергается дефрагментации.
9. После завершения дефрагментации дважды введите *quit*, и вы вернетесь в командную строку.

10. Скопируйте файл Ntds.dit, подвергшийся дефрагментации, в базу данных Active Directory и удалите старые файлы журнала регистрации.
11. Перезапустите контроллер домена.

ПРИМЕЧАНИЕ Если вы производите дефрагментацию базы данных после удаления из Active Directory большого количества объектов, то эту процедуру необходимо повторить на всех контроллерах домена.

Управление базой данных Active Directory с помощью Ntdsutil

Инструмент Ntdsutil можно использовать не только для дефрагментации базы данных Active Directory в автономном режиме, но и для управления базой данных Active Directory другими способами. Ntdsutil можно применить и для выполнения низкоуровневых задач, связанных с восстановлением базы данных Active Directory. Все опции восстановления базы данных являются опциями без разрушения — то есть инструменты восстановления попытаются устранить проблемы с базой данных Active Directory, но это никогда не будет сделано путем удаления данных.

Восстановление журналов регистрации транзакций

Восстановление журналов регистрации транзакций означает их принудительный повторный запуск контроллером домена. Эта опция выполняется контроллером домена автоматически, когда он повторно запускается после вынужденного завершения работы. Кроме того, можно принудительно применить программируемое восстановление с помощью инструмента Ntdsutil.

ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ Принцип использования транзакций в Active Directory подробно описывается в главе 15.

Восстановление журналов регистрации транзакций осуществляется следующим образом.

1. Перезагрузите сервер и выберите опцию загрузки в режиме Directory Services Restore Mode (Режим восстановления служб каталогов). Вы также можете остановить службу Active Directory Domain Services (Службы домена Active Directory) для контроллеров домена Windows Server 2008. Для выполнения всех операций базы данных Ntdsutil потребуется остановить AD DS.
2. Откройте командную строку и введите *ntdsutil*.
3. В строке Ntdsutil введите *Activate Instance NTDS* (Активировать экземпляр NTDS).
4. В строке Ntdsutil введите *files*.
5. В строке File Maintenance (Поддержка файлов) введите *recover*.

Опция восстановления всегда должна выполняться первой, поскольку она гарантирует, что база данных совместима с журналами регистрации транзакций. После восстановления при необходимости можно выполнить другие опции базы данных.

Проверка целостности базы данных

Проверка целостности базы данных означает, что она проверяется на низком (двоичном) уровне на предмет неисправности. В процессе выполнения данной операции проверяются на совместимость также заголовки базы данных и все таблицы. Поскольку проверке подлежит каждый байт крупной базы данных, это занимает много времени. Перейдите в окно инструмента Ntdsutil и в строке File Maintenance (Поддержка файлов) введите *integrity*.

Семантический анализ базы данных

Семантический анализ отличается от проверки целостности тем, что он не позволяет изучать базу данных на двоичном уровне, а предполагает проверку ее совместимости с семантикой Active Directory. В процессе анализа базы данных изучается каждый ее объект, чтобы убедиться в том, что каждый объект имеет GUID, соответствующий идентификатор SID и содержит правильные метаданные репликации.

Чтобы произвести семантический анализ базы данных, выполните следующие действия.

1. Откройте командную строку и введите *ntdsutil*.
2. В строке Ntdsutil введите *Activate Instance NTDS* (Активировать экземпляр NTDS).
3. В строке Ntdsutil введите *semantic database analysis* (семантический анализ базы данных).
4. В строке семантической проверки введите *verbose on*. Этот параметр конфигурирует Ntdsutil на запись дополнительной информации на экран при выполнении семантической проверки.
5. В строке семантической проверки введите *go*.

Перемещение базы данных и журнала регистрации транзакций

Инструмент Ntdsutil можно также использовать для перемещения базы данных Active Directory и журналов регистрации транзакций. Например, если журналы регистрации транзакций и база данных расположены на одном и том же жестком диске, то, возможно, вы захотите переместить один из компонентов на другой жесткий диск. Если жесткий диск, содержащий файл базы данных, заполнен, то вам придется переместить базу данных.

Для перемещения базы данных и журнала регистрации транзакций в другое расположение в режиме Directory Services Restore Mode (Режим восстановления служб каталогов) выполните следующие действия.

1. Откройте командную строку и введите *ntdsutil*.
2. В строке Ntdsutil введите *Activate Instance NTDS* (Активировать экземпляр NTDS).
3. В строке Ntdsutil введите *files*.

4. Чтобы увидеть, где в данное время расположены файлы, в строке Ntdsutil введите *info*. Эта команда выводит список расположений файлов для базы данных и всех журналов регистрации.
5. Чтобы переместить файл базы данных, в строке поддержки файлов введите *move db to directory*, где *directory* — это назначенное расположение для файлов. Указанная команда перемещает базу данных в заданное расположение и реконфигурирует системный реестр для получения доступа к файлу в новом расположении.
6. Для перемещения журналов регистрации транзакций в строке поддержки файлов введите *move logs to directory*.

Резюме

В этой главе описаны процессы и некоторые инструменты, необходимые для мониторинга Active Directory и состояния системы контроллеров домена. Путем реализации регулярного мониторинга можно идентифицировать потенциально разрушительные и дорогостоящие проблемы с производительностью до их возникновения. Эффективный мониторинг Active Directory позволит также получить важные данные о тенденциях изменения производительности. Мониторинг является одним из способов запуска необходимых задач по поддержке инфраструктуры Active Directory. При отсутствии ошибок в журнале регистрации событий и различного рода предупреждений для эффективного функционирования базы данных Active Directory следует реализовать регулярную программу ее поддержки. В главе также рассмотрены процессы онлайн-дефрагментации и дефрагментации в автономном режиме, а также процесс сборки мусора, позволяющий избавиться от не полностью удаленных (с устаревшими записями) объектов Active Directory.

Дополнительные ресурсы

Далее перечислены источники, из которых вы можете получить дополнительные сведения по затронутой в главе теме.

Информация по теме

- Глава 15 «Аварийное восстановление Active Directory» содержит подробные сведения о хранении данных в Active Directory, а также о выполнении резервного копирования и восстановлении базы данных Active Directory.
- Статья «Монитор надежности и производительности Windows» на сайте *http://technet2.microsoft.com/windowsserver2008/en/library/ec5b5e7b-5d5c-4d04-98ad-55d9a09677101033.mspx?mfr=true*.
- Статья «AD DS: Службы домена Active Directory, допускающие повторный запуск» на сайте *http://technet2.microsoft.com/windowsserver2008/en/library/822ff47d-bd55-4c08-abc1-2d66336e33e51033.mspx?mfr=true*.

- Статья «Windows Vista: надежность и производительность» на сайте *http://technet.microsoft.com/en-us/windowsvista/aa905077.aspx*.
- Статья «Утилита поддержки служб каталога Active Directory (Ntdsutil.exe)» на сайте *http://technet2.microsoft.com/windowsserver/en/library/819bea8b-3889-4479-850f-1f031087693d1033.mspx?mfr=true*.
- Статья «Перемещение файлов базы данных Active Directory» на сайте *http://technet2.microsoft.com/windowsserver/en/library/af6646aa-2360-46e4-81ca-d51707bf01eb1033.mspx?mfr=true*.
- Статья «Ручное перемещение SYSVOL» на сайте *http://technet2.microsoft.com/windowsserver/en/library/300796c6-8148-49af-a327-b5dca853ac4f1033.mspx?mfr=true*.
- Статья «Практический опыт для поддержки SYSVOL» на сайте *http://support.microsoft.com/kb/324175*.
- Статья «Руководство пакета управления Microsoft Active Directory» на сайте *http://www.microsoft.com/downloads/details.aspx?familyid=2B9D3613-5516-4F44-8550-B21E054F5047&displaylang=en*.
- Статья «Мониторинг Active Directory с помощью MOM» на сайте *http://download.microsoft.com/documents/uk/technet/downloads/technetmagazine/issue4/36_monitoring_ad_with_mom.pd*.