NetIQ® eDirectory™ 8.8 SP8

Руководство по новым возможностям

Сентябрь 2013 г.

Уведомление

НАСТОЯЩИЙ ДОКУМЕНТ И ОПИСАННОЕ В НЕМ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПОСТАВЛЯЮТСЯ В СООТВЕТСТВИИ С УСЛОВИЯМИ ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ИЛИ СОГЛАШЕНИЯ О НЕРАЗГЛАШЕНИИ. ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, УКАЗАННЫХ В ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ ИЛИ СОГЛАШЕНИИ О НЕРАЗГЛАШЕНИИ, NETIQ CORPORATION ПРЕДОСТАВЛЯЕТ ЭТОТ ДОКУМЕНТ И ОПИСАННОЕ В НЕМ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ ПРЯМЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ ЛЮБОГО ВИДА, ВКЛЮЧАЯ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОМУ НАЗНАЧЕНИЮ, НО НЕ ОГРАНИЧИВАЯСЬ ИМИ. В НЕКОТОРЫХ ШТАТАХ НЕ РАЗРЕШЕН ОТКАЗ ОТ ПРЯМЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ В ОПРЕДЕЛЕННЫХ СЛУЧАЯХ, ПОЭТОМУ ЭТО ЗАЯВЛЕНИЕ МОЖЕТ ВАС НЕ КАСАТЬСЯ.

Для простоты любой модуль, адаптер или другой подобный материал («Модуль») лицензирован в соответствии с условиями и положениями Лицензионного соглашения для применимой версии продукта NetIQ или программного обеспечения, с которым он связан или взаимодействует. Получая доступ к этому Модулю, копируя или используя его, Вы соглашаетесь выполнять данные условия. Если Вы не согласны с условиями Лицензионного соглашения, Вам запрещается получать доступ к Модулю, использовать или копировать его. В таком случае Вы должны уничтожить все копии Модуля и обратиться в NetIQ за дальнейшими инструкциями.

Данный документ и описанное в нем программное обеспечение запрещается сдавать в прокат, продавать или безвозмездно передавать без предварительного письменного разрешения NetIQ Corporation, если иное не разрешено законом. За исключением случаев, явно изложенных в настоящем лицензионном соглашении или соглашении о неразглашении, никакую часть этого документа или описанного в нем программного обеспечения нельзя воспроизводить, хранить в системах поиска или передавать в любой форме или любыми средствами (электронными, механическими или какими-либо иными) без предварительного письменного согласия NetIQ Corporation. Некоторые компании, имена и данные, которые указаны в этом документе, используются в целях иллюстрации и могут не относиться к реальным компаниями, лицам или данным.

В этом документе могут быть технические неточности или опечатки. В представленную здесь информацию периодически вносятся изменения. Эти изменения могут быть включены в новые редакции настоящего документа. NetIQ Corporation в любое время может внести изменения в программное обеспечение, описанное в настоящем документе, или усовершенствовать его.

Ограниченные права Правительства США: если данное программное обеспечение или данная документации приобретены Правительством США либо от его имени или генеральными подрядчиками либо субподрядчиками Правительства США (на любом уровне), то в соответствии с правилами 48 C.F.R. 227.7202-4 (регламентируют приобретения Министерства обороны) и 48 C.F.R. 2.101 и 12.212 (регламентируют приобретения государственных органов за исключением Министерства обороны) права правительства в отношении данного программного обеспечения и данной документации, включая его права на их использование, изменение, воспроизведение, выпуск, представление, показ и раскрытие, во всех их аспектах являются предметом прав и ограничений коммерческой лицензии, изложенной в данном лицензионном соглашении.

оглавление

Об этой книге и библиотеке

Руководство по новым возможностям описывает новые возможности NetIQ eDirectory.

Последнюю версию *руководства по новым возможностям NetIQ eDirectory 8.8 SP8* см. на веб-сайте документации NetIQ eDirectory 8.8.

Предполагаемая аудитория

Руководство предназначено для сетевых администраторов.

Другая информация в библиотеке

В данной библиотеке представлены перечисленные ниже информационные ресурсы.

Руководство по администрированию XDASv2

Приведено описание конфигурации и использования XDASv2 для аудита eDirectory и NetIQ Identity Manager.

Руководство по установке

Описана установка eDirectory. Целевая аудитория данного руководства — администраторы сети.

Руководство по администрированию

Описание управления и настройки eDirectory.

Руководство по поиску и устранению неполадок

Описание устранения неполадок eDirectory.

Руководство по настройке платформ Linux

В данном руководстве описаны процедуры анализа и настройки eDirectory на платформах Linux, которые помогут добиться превосходной производительности во всех развертываниях.

Эти руководства доступны на веб-сайте документации NetIQ eDirectory 8.8 (https://www.netiq.com/documentation/edir88/).

Информацию об утилите управления eDirectory см. в документе *Руководство по администрированию NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/).

О NetIQ Corporation

Мы — глобальная компания, которая разрабатывает корпоративное программное обеспечение, уделяя основное внимание трем постоянным проблемам в вашей среде: изменениям, сложности и риску. Мы работаем над тем, чтобы помочь вам контролировать их.

Наша точка зрения

Адаптация к изменениям и управление сложностью и риском — ничего нового

Из всех проблем, с которыми вы сталкиваетесь, указанные три проблемы, вероятно, являются самыми существенными препятствиями к тому, чтобы получить необходимый вам контроль для безопасного измерения, наблюдения и управления в отношении физических сред, виртуальных сред и сред облачных вычислений.

Обеспечение работы критически важных бизнес-сервисов: лучше и быстрее

Мы считаем, что единственный способ обеспечить своевременное и экономичное предоставление сервисов — предоставить ИТ-организациям максимально возможный контроль. По мере того как организации меняются, и технологии, необходимые для управления этими изменениями, становятся все более сложными, постоянные проблемы будут только углубляться.

Наша философия

Продавать интеллектуальные решения, а не просто программное обеспечение

Чтобы обеспечить надежный контроль, сначала мы должны понять реальные сценарии, в которых изо дня в день работают ИТ-организации, наподобие вашей. Для нас это единственная возможность разрабатывать практичные, интеллектуальные ИТ-решения, которые обеспечат доказанные и измеримые результаты. И это гораздо более оправдано с точки зрения удовлетворенности результатами работы, чем просто продавать программное обеспечение.

Мы стремимся помочь вам быть более успешными.

В своей работе мы ставим ваш успех на первое место. На всех этапах создания продукта — от начала разработки до развертывания — мы понимаем, что вам нужны хорошо работающие ИТ-решения, которые могут беспрепятственно интегрироваться с имеющимися ресурсами, постоянная поддержка и обучение после развертывания, а также люди, с которыми по-настоящему легко работать. Все это ради изменений. И наконец, ваш успех означает наш общий успех.

Наши решения

- Определение подлинности и управление доступом
- Управление доступом
- Управление безопасностью

- Управление системами и приложениями
- Управление рабочей нагрузкой
- Управление сервисами

Контактная информация службы поддержки продаж

С вопросами о продуктах, ценах и возможностях обращайтесь к местному партнеру. Если вам не удается связаться с партнером, обратитесь в службу поддержки продаж.

Интернациональный (Worldwide).	www.netiq.com/about_netiq/officelocations.asp
США и Канада:	1-888-323-6768
Электронная почта:	info@netiq.com
iFolder:	www.netiq.com

Контактная информация службы технической поддержки

С особыми вопросами о продукте обращайтесь в нашу службу технической поддержки.

Интернациональный (Worldwide).	www.netiq.com/support/contactinfo.asp
Северная и Южная Америка:	1-713-418-5555
Европа, Ближний Восток, Африка:	+353 (0) 91-782 677
Электронная почта:	support@netiq.com
iFolder:	www.netiq.com/support

Контактная информация службы документации

Наша цель — предоставить документацию, которая соответствует вашим потребностям. Если вы хотите поделиться своими предложениями по улучшению, перейдите по ссылке **Добавить комментарий** в нижней части любой HTML-страницы документации www.netiq.com/documentation. Также можно связаться с нами по электронной почте Documentation-Feedback@netiq.com. Мы высоко ценим ваше мнение. Ваши отзывы всегда желательны для нас.

Информация для доступа к интерактивному сообществу пользователей

Qmunity — интерактивное сообщество NetIQ — сеть совместной работы, которая позволяет связаться с вашими коллегами и экспертами по NetIQ. В сообществе Qmunity вы можете получить информацию из первых рук, найти полезные ссылки и ресурсы, пообщаться с экспертами по NetIQ. Таким образом, у вас есть возможность овладеть знаниями,

необходимыми для реализации полного потенциала инвестиций в ИТ, на которые вы полагаетесь. Для получения дополнительных сведений посетите сайт http://community.netiq.com.

1 Компоненты и усовершенствования в пакете обновления 8

В этой главе содержится описание функций и усовершенствований eDirectory 8.8 SP8.

1.1 Улучшенное масштабирование

Для более быстрой синхронизации данных и обработки значений устаревшего состояния, а также для снижения нагрузки на память при обработке событий журнала в eDirectory 8.8 SP8 применены описанные ниже усовершенствования масштабируемости.

В этой версии некоторые фоновые процессы оптимизированы для более крупных, динамичных сред. В том числе следует отметить оптимизацию существующих фоновых процессов и предоставление параметров для настройки систем в соответствии со структурой среды.

1.1.1 Управление фоновыми процессами

Администраторы могут управлять фоновыми процессами путем настройки следующих политик в окне "Параметры задержки фонового процесса" в NetIQ iMonitor:

- **CPU** — указывает предельное процентное значение компьютерных ресурсов и предельную длительность сна процесса (skulker, purger или обработка устаревших состояний).
- **Жесткое ограничение** — статическое значение задержки для процессов синхронизации, очистки и значений устаревшего состояния.

Дополнительные сведения о настройке фоновых процессов см. в разделе "Настройка фоновых процессов" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.1.2 Процесс Skulker

Чтобы увеличить количество потоков для одновременной репликации на несколько серверов, можно использовать процесс skulker и вручную задать максимальное количество потоков. Этот параметр применяется ко всем разделам сервера.

Дополнительные сведения о настройке процесса skulker см. в разделе "Настройка потоков синхронизации вручную" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.1.3 Асинхронная репликация

Для ускорения репликации следующие операции теперь выполняются параллельно:

- Обработка кэша изменений
- Отправка пакетов на удаленный сервер

Новый параметр **Асинхронная исходящая синхронизация (мс)** позволяет избежать перегрузки принимающего сервера. По умолчанию этот параметр отключен. Этот параметр зависит от среды. Если нужно включить этот параметр, задайте значение `100`, а затем отрегулируйте по необходимости.

Дополнительные сведения о настройке асинхронной исходящей синхронизации см. в разделе "Настройка асинхронной исходящей синхронизации" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.1.4 Репликация на основе политик

Администраторы могут создавать политику (XML-файл), указывающую способ репликации изменений. Например, это может быть полезным при распространении кольца реплик по нескольким расположениям. При опечатках или неверном синтаксисе политики используется метод репликации по умолчанию.

Дополнительные сведения см. в разделе "Репликация на базе политики" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.1.5 Значения устаревшего состояния

Устаревшее состояние, созданное в результате удаления, переименования или перемещения объектов, обрабатывается быстрее, чем в прежних версиях eDirectory. Например, для обновления, для которого в прежних версиях требовалось 5 циклов, теперь может требоваться всего 2 цикла.

Кроме того, теперь процесс устаревших состояний может работать параллельно с процессом синхронизации.

1.1.6 Отслеживание количества значений устаревшего состояния и показателей кэша с помощью iMonitor

iMonitor отображает количество объектов со значениями устаревшего состояния в каждом состоянии. Кроме того, отображается количество объектов в кэше изменений раздела при просмотре объекта раздела с помощью iMonitor на данном сервере. Это помогает отслеживать состояние синхронизации и обработки значений устаревшего состояния.

1.1.7 Распределенные справочные ссылки (DRL)

Для оптимизации обработки значений устаревшего состояния в eDirectory больше не используются следующие атрибуты DRL:

- `UsedBy`
- `ObitUsedBy`

1.1.8 Кэширование журнала событий

Система событий журнала изменена и допускает использование памяти и диска для сохранения событий в очереди. Это позволяет снизить объем памяти, потребляемой процессом ndsd.

События журнала усовершенствованы следующим образом:

- **Кэширование**

  Когда размер журнала событий в памяти превышает определенный предел (макс. 32 МБ = 8 блоков по 4 МБ), eDirectory начинает использовать кэш на жестком диске.

- **Переменные**

  Журнал событий использует следующие настраиваемые пользователем переменные:

  - NDSD_EVENT_DISK_CACHE
  - NDSD_EVENT_DISK_CACHE_DIR

- **Сжатие**

  Улучшенный алгоритм сжатия позволяет сократить объем данных на жестком диске. Степень сжатия составляет примерно 20:1.

1.1.9 Поддержка твердотельных дисков (SSD)

Эта версия поддерживает корпоративные твердотельные диски, обладающие повышенной производительностью.

1.1.10 Дополнительный расчет стоимости ссылки (ARC)

В этой версии ARC по умолчанию включен.

Дополнительные сведения см. в разделе "Дополнительный расчет стоимости ссылок" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.1.11 Интервал обновления входа

Новый параметр "Интервал отключения обновления входа" позволяет администраторам указать интервал времени (в секундах), в течение которого eDirectory не обновляет атрибуты входа.

ПРИМЕЧАНИЕ. Этот параметр применяется только ко входу в NetIQ Directory Services (NDS).

Дополнительные сведения см. в разделе "Настройка агента DS" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.2 Усовершенствования LDAP

Этот выпуск включает следующие усовершенствования LDAP.

1.2.1 Контроль изменения по разрешению

С помощью этого параметра можно расширить существующую операцию изменения LDAP. При попытке удаления несуществующего атрибута или добавления значения в существующий атрибут работа продолжается без отображения сообщения об ошибке.

Дополнительные сведения см. в разделе "Настройка разрешительного управления изменениями" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.2.2 Поддержка времени в обобщенном формате

Поддержка времени в обобщенном формате позволяет отображать время в формате `ГГГГММДДччммсс.0Z`.

Обратите внимание, что `0Z` означает поддержку долей секунд согласно Active Directory. Поскольку в eDirectory не поддерживается отображение долей секунд, всегда отображается *0* во избежание ошибок в среде с одновременным использованием.

Дополнительные сведения см. в разделе "Настройка поддержки единого времени" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

1.2.3 Управление удалением поддеревьев

В этой версии поддерживается элемент управления для удаления поддеревьев, дающий возможность удалять любые объекты-контейнеры. Ранее можно было удалять только конечные объекты дерева. Тем не менее, удаление контейнеров разделов не поддерживается.

1.3 Поддержка IPv6

Эта версия поддерживает сети и с IPv4, и с IPv6. По умолчанию IPv6 автоматически включается при установке eDirectory. При обновлении с предыдущей версии eDirectory необходимо вручную включить поддержку IPv6.

eDirectory 8.8 SP8 поддерживает следующие режимы IPv6:

- Двойной стек
- Туннелирование
- Только IPv6

eDirectory 8.8 SP8 не поддерживает следующие типы IPv6-адресов:

- Адреса локальных ссылок
- IPv6-адреса, сопоставленные с IPv4
- IPv4-адреса, совместимые с IPv6

eDirectory 8.8 SP8 поддерживает следующие форматы адресации:

- [::]
- [::1
- [2015::12]
- [2015::12]:524

1.4 Улучшенный аудит

В этой версии расширены возможности аудита XDAS путем поддержки IP-адресов клиентов в событиях.

2 Платформы, поддерживаемые для установки eDirectory

eDirectory 8.8 SP8 — это межплатформенный выпуск, предназначенный для повышения стабильности eDirectory.

2.1 Устаревшие платформы

eDirectory 8.8 SP8 не поддерживает следующие платформы:

- NetWare
- 32- и 64-разрядные версии eDirectory в Solaris
- 32-разрядная версия eDirectory в AIX
- 32-разрядная версия eDirectory в Linux
- 32-разрядная версия eDirectory в Windows

2.2 Linux

Необходимо устанавливать eDirectory на одну из следующих платформ:

- SLES 11 SP1, SP2 и SP3 (64-разрядные версии)
- SLES 10 SP4 (64-разрядная версия)
- RHEL 5.7, 5.8 и 5.9
- RHEL 6.2, 6.3 и 6.4

Указанные выше операционные системы могут выполняться в виртуальном режиме на следующих гипервизорах:

- VMware ESXi
- Xen (на платформах SLES 10 и SLES 11 с соответствующими пакетами поддержки)

ПРИМЕЧАНИЕ. eDirectory 8.8 с пакетом обновления 8 поддерживается службой виртуализации SLES 10 XEN, на которой запускается гостевая ОС SLES 10. Следующие обновления доступны на веб-сайте NetIQ Update (https://update.novell.com):

- SUSE-Linux-Enterprise-Server-X86_64-10-0-20061011-020434
- SLES10-Updates

Для регистрации и обновления SUSE Linux Enterprise 10 см. Регистрация SUSE Linux Enterprise в NetIQ Customer Center (http://www.suse.com/products/register.html). После установки последнего обновления убедитесь, что минимальный уровень установленного обновления — 3.0.2_09763-0.8.

- Виртуализация Windows Server 2008 R2 с использованием Hyper-V

Версия используемой SUSE Linux указана в файле `/etc/SuSE-release`.

Убедитесь, что в системах Red Hat установлены последние исправления glibc с веб-сайта Red Hat Errata (http://rhn.redhat.com/errata). Минимально допустимая версия библиотеки glibc – 2.1.

2.3 Windows

Необходимо устанавливать eDirectory на одну из следующих платформ:

- Windows Server 2008 (x64) (Standard/Enterprise/Data Center Edition) с пакетами обновления
- Windows Server 2008 R2 (Standard/Enterprise/Data Center Edition) с пакетами обновления
- Windows 2012 Server

ЗАМЕЧАНИЕ

- Для установки eDirectory 8.8 с пакетом обновления 8 (SP7) на Windows Server 2008 R2 необходимо использовать учетную запись, для которой предоставлены административные права.
- Версии Windows для настольных компьютеров не поддерживаются.

3 Усовершенствования в области установки и обновления

В этой главе описываются новые и улучшенные возможности в области установки и обновления NetIQ eDirectory 8.8.

В следующей таблице перечислены новые возможности и платформы, на которых они поддерживаются.

Возможность	Linux	Windows
Различные форматы пакетов для установки eDirectory 8.8	✓	✗
Настраиваемое расположение установки файлов приложения	✓	✓
Настраиваемое расположение установки файлов данных	✓	✓
Настраиваемое расположение установки файлов конфигурации	✓	✗
Установка без прав root	✓	✗
Улучшенная поддержка установки в высокодоступные кластеры	✓	✓
Поддержка FHS	✓	✗
Поддержка LSB	✓	✗
Проверка состояния сервера	✓	✓
Интеграция SecretStore	✓	✓
Установка eDirectory Instrumentation	✓	✓

Эта глава содержит следующие сведения:

3.1 Различные форматы пакетов для установки eDirectory 8.8

В Linux можно на выбор использовать различные форматы файлов для установки eDirectory 8.8. Форматы файлов перечислены в таблице ниже.

Тип пользователя и расположение установки	Linux
Пользователь root	
Расположение по умолчанию	RPM
Настраиваемое расположение	TAR-файл
Пользователь без прав root	
Настраиваемое расположение	Tar-файл

Дополнительную информацию об установке с помощью Tar-файлов см. в *руководстве по установке eDirectory 8.8 с пакетом обновления 8*.

3.2 Установка eDirectory 8.8 в настраиваемое расположение

В eDirectory 8.8 можно выбирать расположение для установки файлов приложения, данных и конфигурации.

Один из сценариев установки eDirectory 8.8 в настраиваемом расположении предусматривает наличие установленной более ранней версии eDirectory и необходимость тестирования eDirectory 8.8 перед обновлением до этой версии. Это дает возможность протестировать новую версию, не затрагивая существующую настройку eDirectory. Затем можно выбрать сохранение существующей версии или обновление до eDirectory 8.8.

ПРИМЕЧАНИЕ. Субагенты SLP и SNMP устанавливаются в расположение по умолчанию.

В этом разделе описывается выбор расположения для установки различных файлов:

3.2.1 Выбор расположения для файлов приложения

При установке eDirectory можно выбрать расположение файлов программы.

Linux

Чтобы установить eDirectory 8.8 в настраиваемое расположение, можно использовать TAR-файл установки и распаковать eDirectory 8.8 в нужный каталог.

Windows

Можно настроить расположение файлов приложения в мастере установки eDirectory 8.8.

3.2.2 Выбор расположения для файлов данных

При настройке eDirectory можно выбрать расположение для сохранения файлов данных. К файлам данных относятся все файлы в каталогах `data`, `dib` и `log`.

Linux

Чтобы настроить расположение файлов данных, можно использовать программу ndsconfig с параметром `-d` или `-D`.

Параметр	Описание
-d *расположение*	Создает папку `DIB` (база данных eDirectory) в указанном расположении.
	ПРИМЕЧАНИЕ. Этот параметр действовал и в версиях eDirectory до 8.8.
-D *расположение*	Создает папки `data` (содержит данные, такие как pid и ID сокетов), `dib` и `log` в указанном расположении.

Windows

В Windows будет предложено ввести путь к папке DIB при установке. Введите нужный путь на ваше усмотрение.

3.2.3 Выбор расположения для файлов конфигурации

При настройке eDirectory можно выбрать расположение для сохранения файлов конфигурации.

Linux

Чтобы настроить расположение файла конфигурации `nds.conf`, используйте программу ndsconfig с параметром `--config-file`.

Для установки других файлов конфигурации (например, `modules.conf`, `ndsimon.conf` и `ice.conf`) в другое расположение выполните следующие действия:

1. Скопируйте все файлы конфигурации в новое расположение.
2. Укажите новое расположение с помощью следующей команды:

   ```
   ndsconfig set n4u.nds.configdir расположение
   ```

Windows

В Windows невозможно использовать настраиваемое расположение файлов конфигурации.

3.3 Установка без прав root

eDirectory 8.8 и более поздних версий поддерживает установку и настройку серверов eDirectory пользователями без прав root. Более ранние версии eDirectory могли устанавливаться только пользователем с правами root, причем на хосте мог выполняться только один экземпляр eDirectory.

В eDirectory 8.8 или более поздних версиях пользователь может использовать TAR-файл для установки eDirectory. Один и тот же пользователей или несколько пользователей могут установить несколько экземпляров двоичных файлов eDirectory. Тем не менее, для установки служб системного уровня, таких как NICI, SNMP и SLP, требуются права root. NICI является обязательным компонентом для работы eDirectory, а SNMP и SLP — необязательные. Кроме того, при установке пакета пользователь с правами root может установить только один экземпляр.

После установки пользователь, не имеющий прав root, может настроить экземпляры сервера eDirectory с помощью своего собственного TAR-файла или двоичной установки. Это означает, что может быть несколько экземпляров серверов eDirectory на одном и том же хосте, поскольку любой пользователь, независимо от наличия прав root, может настроить несколько экземпляров сервера eDirectory на одном хосте с помощью установки пакета или TAR-файла. Дополнительные сведения о поддержке нескольких экземпляров см. в разделах "Несколько экземпляров" и "Обновление нескольких экземпляров" в *Руководстве по установке NetIQ eDirectory 8.8 SP8*.

Установка и настройка без прав root применимы только к платформам Linux. Дополнительные сведения об установке и настройке без прав root см. в разделе "Установка eDirectory 8.8 без прав root" в *Руководстве по установке NetIQ eDirectory 8.8 SP8*.

3.4 Улучшенная поддержка установки в высокодоступные кластеры

В eDirectory 8.8 SP8 упрощена установка и управление eDirectory в кластерах Linux и Windows. Улучшена поддержка кластеров и поддерживается высокая доступность. eDirectory также обеспечивает высокую доступность путем синхронизации реплик. Также можно использовать и кластеры для дополнительного повышения доступности.

Дополнительные сведения об установке eDirectory в кластеры см. в *Руководстве по установке NetIQ eDirectory 8.8 SP8*.

3.5 Поддержка стандартов

eDirectory 8.8 поддерживает следующие стандарты:

- Раздел 3.5.1, "Поддержка FHS" на стр. 25
- Раздел 3.5.2, "Поддержка LSB" на стр. 26

3.5.1 Поддержка FHS

Во избежание конфликтов с файлами приложений других продуктов в eDirectory 8.8 поддерживается стандарт Filesystem Hierarchy Standard (FHS). Эта возможность доступна только для Linux.

В eDirectory эта структура каталогов используется только при установке в расположение по умолчанию. Если выбрано настраиваемое расположение, то структура каталогов будет такой: *настраиваемое расположение/путь по умолчанию*.

Например, если выбрать установку в каталог `eDir88`, то внутри каталога `eDir88` сохранится такая же структура каталогов, например, файлы man page будут находиться в каталоге `/eDir88/opt/novell/man`.

В следующей таблице показаны изменения в структуре каталогов.

Типы файлов, хранящихся в каталоге	Имя каталога и путь
Исполняемые двоичные файлы и статические сценарии консоли	`/opt/novell/eDirectory/bin`
Исполняемые двоичные файлы для использования в правами root	`/opt/novell/eDirectory/sbin`
Файлы статических и динамических библиотек	`/opt/novell/eDirectory/lib`
Файлы конфигурации	`/etc/opt/novell/eDirectory/conf`
Считываемые и записываемые файлы, динамические данные при выполнении, например, DIB	`/var/opt/novell/eDirectory/data`
Файлы журналов	`/var/opt/novell/eDirectory/log`
Файлы man page Linux	`/opt/novell/man`

Экспорт переменных среды

Реализация FHS в eDirectory 8.8 требует обновления переменных среды, связанных с путем, и из экспорта. Из-за этого возникают следующие проблемы:

- Необходимо помнить все экспортированные пути, то есть при каждом открытии оболочки нужно экспортировать эти пути и приступить к использованию программ.
- Если нужно использовать более одного набора двоичных файлов, нужно открыть несколько оболочек или часто переназначать пути различным наборам двоичных файлов.

Чтобы решить эту проблему, можно использовать сценарий `/opt/novell/eDirectory/bin/ndspath`:

- Используйте сценарий ndspath в качестве префикса программы и запускайте программу следующим образом:

  ```
  custom_location/opt/novell/eDirectory/bin/ndspath utility_name_with_parameters
  ```

- Экспортируйте пути в текущей оболочке следующим образом:

```
. custom_location/opt/novell/eDirectory/bin/ndspath
```

- Введя указанную выше команду, запускайте программы обычным образом. Вызовите сценарий вашего профиля bashrc или аналогичные. Поэтому при каждом входе в систему или при каждом открытии новой оболочки можно сразу использовать программы.

3.5.2 Поддержка LSB

eDirectory 8.8 поддерживает Linux Standard Base (LSB). *Для* соответствия LSB также рекомендуется поддержка FHS. Все пакеты eDirectory в Linux теперь имеют префикс *novell*. Например, `NDSserv` теперь называется `novell-NDSserv`.

3.6 Проверка состояния сервера

В eDirectory 8.8 появились проверки состояния сервера, чтобы убедиться в работоспособности сервера перед обновлением.

Проверки состояния сервера по умолчанию запускаются вместе с каждым обновлением и выполняются до начала обновления. Кроме того, можно запустить диагностическую программу ndscheck для проверки состояния.

3.6.1 Необходимость проверки состояния

В прежних версиях eDirectory при обновлениях не проверялась работоспособность серверов. Если сервер работал нестабильно, операция обновления не выполнялась, а система eDirectory становилась неработоспособной. В некоторых случаях не удавалось сделать откат к состоянию, которое было до начала обновления.

Новая программа для проверки состояния устраняет эту проблему, проверяя готовность сервера к обновлению.

3.6.2 Как определяется работоспособность сервера?

Программа проверки состояния выполняет определенные проверки для выяснения работоспособности дерева. Дерево объявляется работоспособным при удачном прохождении всех проверок.

3.6.3 Выполнение проверок состояния

Проверки состояния сервера можно проводить двумя способами:

- "При обновлении" на стр. 27
- "Автономная программа" на стр. 27

ПРИМЕЧАНИЕ. Для запуска программы проверки требуются права администратора. Наименьшим уровнем прав, необходимым для запуска программы, является уровень Public. Тем не менее, с правом Public недоступны некоторые объекты протокола NetWare Core Protocol (NCP) и сведения о разделах.

При обновлении

Проверки состояния по умолчанию запускаются при каждом обновлении eDirectory.

Linux

При каждом обновлении перед его началом запускаются проверки состояния.

Чтобы пропустить проверки по умолчанию, используйте параметр -j при запуске команды nds-install.

Windows

Проверки состояния выполняются мастером установки. Можно включить или отключить проверки при появлении соответствующего запроса.

Автономная программа

Можно в любое время запустить проверку состояния сервера с помощью автономной программы. В следующей таблице описываются программы для проверки состояния.

Таблица 3-1 *Программы для проверки состояния*

Платформа	Имя программы
Linux	ndscheck Синтаксис: `ndscheck -h hostname:port -a admin_FDN -F logfile_path --config-file configuration_file_name_and_path` **ПРИМЕЧАНИЕ.** Можно указать либо `-h`, либо `--config-file`, но не оба параметра одновременно.
Windows	ndscheck

3.6.4 Типы проверок состояния

При обновлении или при запуске программы ndscheck проводятся следующие проверки состояния:

- Базовая работоспособность сервера
- Состояние разделов и реплик

Если запустить программу ndscheck, результаты проверки состояния будут показаны на экране и записаны в файл `ndscheck.log`. Дополнительные сведения о файлах журнала см. в Раздел 3.6.6, "Файлы журналов" на стр. 29.

Если проверка осуществляется в ходе обновления, то после проверки, на основе серьезности ошибок, предлагается либо продолжить процесс обновления, либо его отменить. Подробное описание этих ошибок см. в Раздел 3.6.5, "Категории состояния работоспособности" на стр. 28.

Базовая работоспособность сервера

Это первый этап проверки состояния. Программа проверки состояния проверяет следующее:

1. Служба eDirectory запущена. База данных DIB открыта, из нее можно прочесть базовые данные о деревьях, например, имя дерева.
2. Сервер прослушивает соответствующие номера портов.

   Для LDAP программа получает номера портов TCP и SSL и проверяет, прослушивает ли сервер эти порты.

   Аналогичным образом, программа получает номера портов HTTP и HTTPS и проверяет, прослушивает ли сервер эти порты.

Состояние разделов и реплик

После проверки состояния сервера проверяется состояние разделов и реплик:

1. Проверка состояния реплик на локальных разделах.
2. Считывает кольцо реплик каждого раздела на сервере, проверяет состояние всех серверов в кольце реплик и состояние ON всех реплик.
3. Проверка синхронизации времени всех серверов кольца реплик. При этом выявляются различия времени между серверами.

3.6.5 Категории состояния работоспособности

На основе ошибок, обнаруженных при проверке состояния сервера, устанавливается одна из трех категорий состояния. Состояние проверок записывается в файл журнала. Дополнительные сведения см. в Раздел 3.6.6, "Файлы журналов" на стр. 29.

Три категории состояния: Обычное, Предупреждение и Критическое.

Обычное

Состояние сервера определяется как "обычное" при успешном прохождении всех проверок.

Сразу после проверки начинается обновление.

Предупреждение

Состояние сервера определяется как "предупреждение" при наличии незначительных ошибок.

Если проверка проводится в ходе обновления, то предлагается либо продолжить обновление, либо отменить его.

Предупреждения обычно возникают в следующих случаях:

1. Сервер не прослушивает порты LDAP и HTTP в обычном или в безопасном режиме (или в обеих режимах).
2. Не удается подключиться к неглавным серверам в кольце реплик.
3. Серверы в кольце реплик рассинхронизированы.

Критическое

Состояние сервера определяется как "критическое" при наличии критических ошибок.

Если проверка проводится в ходе обновления, то обновление отменяется.

Критическое состояние обычно возникает в следующих случаях:

1. Не удается прочитать или открыть DIB. Возможно, данные DIB заблокированы или повреждены.
2. Не удается подключиться ко всем серверам в кольце реплик.
3. Локальные разделы заняты.
4. Реплика не находится во включенном состоянии.

3.6.6 Файлы журналов

При всех операциях проверки (запущенные как автономно, так и в ходе обновления) состояние записывается в файл журнала.

Содержимое файла журнала аналогично сообщениям, отображаемым на экране при проверке.

Файл журнала проверки состояния содержит следующие данные:

- Состояние проверок работоспособности (обычное, предупреждение или критическое).
- URL-адреса сайта поддержки NetIQ.

В следующей таблице приводится расположение файлов журнала на различных платформах.

Таблица 3-2 *Расположение файлов журнала проверки состояния*

Платформа	Имя файла журнала	Расположение файла журнала
Linux	`ndscheck.log`	Зависит от расположения, указанного командой `ndscheck -F`. Если параметр `-F` не был использован, расположение файла `ndscheck.log` определяется другими параметрами в командной строке ndscheck: 1. Если был использован параметр `-h`, то файл `ndscheck.log` сохраняется в домашнем каталоге пользователя. 2. Если был использован параметр `--config-file`, то файл `ndscheck.log` сохраняется в каталоге log экземпляра сервера. Также можно выбрать один экземпляр из списка экземпляров.
Windows	`ndscheck.log`	*`каталог_установки`*

3.7 Интеграция SecretStore с eDirectory

eDirectory 8.8 позволяет настроить Novell SecretStore 3.4 в ходе настройки eDirectory. В более ранних версиях по сравнению с eDirectory 8.8 приходилось устанавливать SecretStore вручную.

SecretStore - это просто и безопасное решение для управления паролями. Оно позволяет использовать единый вход в eDirectory для доступа к большинству приложений для Linux, Windows, больших серверов и веб-приложений.

После проверки подлинности eDirectory приложения, поддерживающие SecretStore, сохраняют и получают необходимые учетные данные. Применение SecretStore исключает необходимость запоминать или синхронизировать несколько паролей для доступа к защищенным приложениям, веб-сайтам и большим ЭВМ.

Для настройки SecretStore 3.4 вместе с eDirectory можно выполнить следующие действия:

- **Linux:**

  Используйте команду `ndsconfig add -m ss`. Здесь `ss` обозначает SecretStore. Это необязательный параметр. Если не указать имя модуля, устанавливаются все модули. Если не нужно устанавливать SecretStore, передайте значение `no_ss`, указав параметр `-m no_ss`.

- **Windows:**

  При установке eDirectory можно выбрать настройку модуля SecretStore. По умолчанию этот параметр выбран.

Дополнительную информацию об использовании SecretStore см. в *Руководстве по администрированию Novell SecretStore 3.4* (https://www.netiq.com/documentation/secretstore34/).

3.8 Установка eDirectory Instrumentation

Ранее решение eDirectory Instrumentation входило в состав пакета Novell Audit. Начиная с eDirectory 8.8 SP3 решение eDirectory Instrumentation необходимо устанавливать отдельно.

Дополнительную информацию об установке, настройке и удалении eDirectory Instrumentation см. в разделе "eDirectory Instrumentation" в *Руководстве по установке NetIQ eDirectory 8.8 SP8*.

3.9 Получение дополнительной информации

Дополнительные сведения о компонентах, описанных в этой главе, см. в следующих источниках:

- *Руководство по установке NetIQ eDirectory 8.8 SP8*
- *Руководство по администрированию NetIQ eDirectory 8.8 SP8*
- Linux: файлы man page `nds-install`, `ndsconfig` и `ndscheck`

4 NICI – резервное копирование и восстановление

Инфраструктура Novell International Cryptography Infrastructure (NICI) хранит ключи и данные пользователей в файловой системе, а также в системных и пользовательских каталогах и файлах. Эти каталоги и файлы защищены путем настройки соответствующих разрешений доступа к ним с помощью механизма, предоставляемого операционной системой. Для этого используется программа установки NICI.

При удалении NICI из системы не удаляются системные и пользовательские каталоги и файлы. Поэтому восстанавливать эти файлы в предыдущее состояние следует лишь для восстановления после катастрофического сбоя системы или после человеческой ошибки. Следует помнить, что перезапись существующего набора пользовательских каталогов и файлов NICI может привести к неработоспособности приложения.

Ключ базы данных, необходимый для открытия DIB, заключен в ключи NICI. Если резервное копирование eDirectory выполняется независимо от резервного копирования NICI, то он не используется.

Изменения по сравнению с прежним механизмом резервного копирования и восстановления NICI

Ранее резервное копирование и восстановление NICI выполнялось вручную. В новой версии добавлено решение для резервного копирования и восстановления NICI. В решение для резервного копирования eDirectory добавлен параметр (`-e`) (eMBox и DSBK), обеспечивающий следующие возможности:

1. Резервное копирование ключей NICI при запущенном резервном копировании eDirectory
2. Восстановление ключей NICI при запущенном восстановлении eDirectory

Для получения дополнительных сведений см. раздел "Резервное копирование и восстановление NICI" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

5 Программа ndspassstore

ndspassstore — это новая программа, позволяющая сохранять зашифрованный пароль пользователям sadmin и eDirectory. Эта программа доступна для платформ Linux и Windows. Эта программа принимает имя пользователя и пароль в качестве входных данных и сохраняет их в виде зашифрованных пар "ключ-значение".

В этой версии эта программа служит для настройки пароля администратора.

По умолчанию эта платформа находится в папке `C:\Novell\NDS` в Windows и `/opt/novell/eDirectory/bin` в Linux.

Описание команды

Для использования программы ndspassstore введите следующую команду в консоли сервера:

```
ndspassstore -a <adminContext> -w <пароль>
```

Параметр	Использование
-a adminContext	Этот параметр используется для приема adminContext (это полное имя пользователя с правами администратора).
-w пароль	Этот параметр используется, чтобы принять пароль пользователя для проверки подлинности.

6 Несколько экземпляров

Раньше можно было настроить только один экземпляр NetIQ eDirectory на одном хосте. Благодаря поддержке нескольких экземпляров в eDirectory 8.8 можно настроить следующее:

- Несколько экземпляров eDirectory на одном хосте
- Несколько деревьев на одном хосте
- Несколько реплик одного и того же дерева или раздела на одном хосте

В состав eDirectory 8.8 также входит программа (ndsmanage) для удобного отслеживания экземпляров.

В следующей таблице перечислены платформы, поддерживающие несколько экземпляров:

Возможность	Linux	Windows
Поддержка нескольких экземпляров	✓	✗

Эта глава содержит следующие сведения:

6.1 Необходимость нескольких экземпляров

Необходимость использования нескольких экземпляров обусловлена следующим:

- Используйте все возможности мощного оборудования, настроив несколько экземпляров eDirectory.
- Проведите пилотную установку на одном хосте перед вложением средств в оборудование.

6.2 Примеры сценариев для развертывания нескольких экземпляров

Несколько экземпляров, принадлежащие к одному или к нескольким деревьям, можно эффективно использовать в следующих сценариях.

eDirectory в среде крупных компаний

- В крупных компаниях можно обеспечить балансировку нагрузки и высокую доступность служб eDirectory.

  Например, при наличии трех серверов реплик, на которых службы LDAP запущены на портах 1524, 2524 и 3524, можно настроить новый экземпляр eDirectory и обеспечить высокодоступную службу LDAP на новом порту 636.
- Можно использовать все возможности мощного оборудования в организациях, настроив несколько экземпляров на одном хосте.

Ознакомительное использование eDirectory

- **Учебные заведения** Многие желающие (студенты) могут ознакомиться с работой eDirectory на одном и том же хосте, используя несколько экземпляров.
- **Обучение администрированию eDirectory:**
  - Участники могут обучаться администрированию, используя несколько экземпляров.
  - Преподаватели могут использовать один хост для обучения целого класса учащихся. У каждого учащегося может быть собственное дерево.

6.3 Использование нескольких экземпляров

В eDirectory 8.8 настраивать несколько экземпляров очень просто. Чтобы эффективно использовать несколько экземпляров, необходимо спланировать установку, а затем настроить экземпляры.

- Раздел 6.3.1, "Планирование установки" на стр. 36
- Раздел 6.3.2, "Настройка нескольких экземпляров" на стр. 36

6.3.1 Планирование установки

Для эффективного использования этой функции мы рекомендуем спланировать экземпляры eDirectory и убедиться в том, что каждый экземпляр имеет необходимые идентификаторы (имя узла, номер порта, имя сервера) или файл конфигурации.

При настройке нескольких экземпляров необходимо спланировать следующее:

- Расположение файла конфигурации
- Расположение различных данных (например, файлов журналов)
- Расположение DIB
- Интерфейс NCP™, уникальным образом идентифицирующий порты для каждого экземпляра и для других служб (LDAP, LDAPS, HTTP и HTTPS)
- Уникальное имя сервера для каждого экземпляра

6.3.2 Настройка нескольких экземпляров

Можно настроить несколько экземпляров eDirectory с помощью программы ndsconfig. В следующей таблице перечислены параметры ndsconfig, которые следует использовать при настройке нескольких экземпляров.

ПРИМЕЧАНИЕ. Для всех экземпляров используется один и тот же ключ сервера (NICI).

Параметр	Описание
--config-file	Указывает абсолютный путь и имя файла для хранения файла конфигурации `nds.conf`. Например, чтобы файл конфигурации находился в каталоге `/etc/opt/novell/eDirectory/`, используйте параметр `--config-file /etc/opt/novell/eDirectory/nds.conf`.
-b	Указывает номер порта для прослушивания новым экземпляром. **ПРИМЕЧАНИЕ.** Используются только параметры `-b` и `-B`.

-B	Указывает номер порта и IP-адрес или интерфейс. Например:
	
	`-B eth0@524`
	
	или
	
	`-B 100.1.1.2@524`
	
	ПРИМЕЧАНИЕ. Используются только параметры `-b` и `-B`.

-D	Создает каталоги `data`, `dib` и `log` в расположении, указанном для нового экземпляра.
S	Указывает имя сервера.

С помощью указанных выше параметров можно настроить новый экземпляр eDirectory.

Также можно настроить новый экземпляр с помощью программы ndsconfig. Дополнительные сведения см. в "Создание экземпляра с помощью ndsmanage" на стр. 38.

6.4 Управление несколькими экземплярами

В этом разделе содержатся следующие сведения.

6.4.1 Программа ndsmanage

Программа ndsmanage позволяет выполнять следующие действия:

- Отображение списка настроенных экземпляров
- Создание нового экземпляра
- Следующие действия с выбранным экземпляром
  - Отображение списка реплик на сервере
  - Запуск экземпляра
  - Остановка экземпляра

- Выполнение DSTrace (ndstrace) для экземпляра
- Удаление конфигурации экземпляра

- Запуск и остановка всех экземпляров

Отображение списка экземпляров

В следующей таблице описывается вывод списка экземпляров eDirectory.

Таблица 6-1 *Использование ndsmanage для вывода экземпляров*

Синтаксис	Описание
ndsmanage	Отображение списка экземпляров, настроенных вами.
ndsmanage -a|--all	Отображение списка экземпляров всех пользователей определенной копии eDirectory.
ndsmanage *имя пользователя*	Отображение списка экземпляров, настроенных определенным пользователем.

Для каждого экземпляра отображаются следующие поля:

- Путь к файлу конфигурации
- Полное доменное имя и порт сервера
- Состояние (активен экземпляр или нет)

ПРИМЕЧАНИЕ. Эта программа отображает все экземпляры, настроенные для одного двоичного файла.

Для получения дополнительных сведений см. 6-1 на стр. 38.

Создание экземпляра с помощью ndsmanage

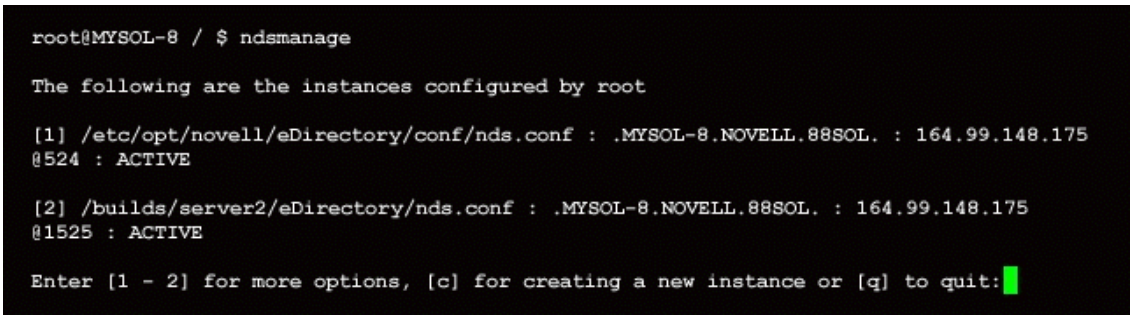
Создание нового экземпляра с помощью ndsmanage:

1 Введите следующую команду:

```
ndsmanage
```

Если настроено два экземпляра, появится следующее окно:

Рисунок 6-1 *Экран вывода данных программы ndsmanage*



2 Введите c для создания нового экземпляра.

Можно либо создать новое дерево, либо добавить сервер в существующее дерево. Следуйте инструкциям на экране для создания нового экземпляра.

Выполнение действий с определенным экземпляром

С каждым экземпляром можно выполнять следующие действия:

- "Запуск определенного экземпляра" на стр. 39
- "Остановка определенного экземпляра" на стр. 39
- "Удаление конфигурации экземпляра" на стр. 40

Кроме того, можно запустить DSTrace для выбранного экземпляра.

Запуск определенного экземпляра

Чтобы запустить настроенный вами экземпляр, выполните следующие действия:

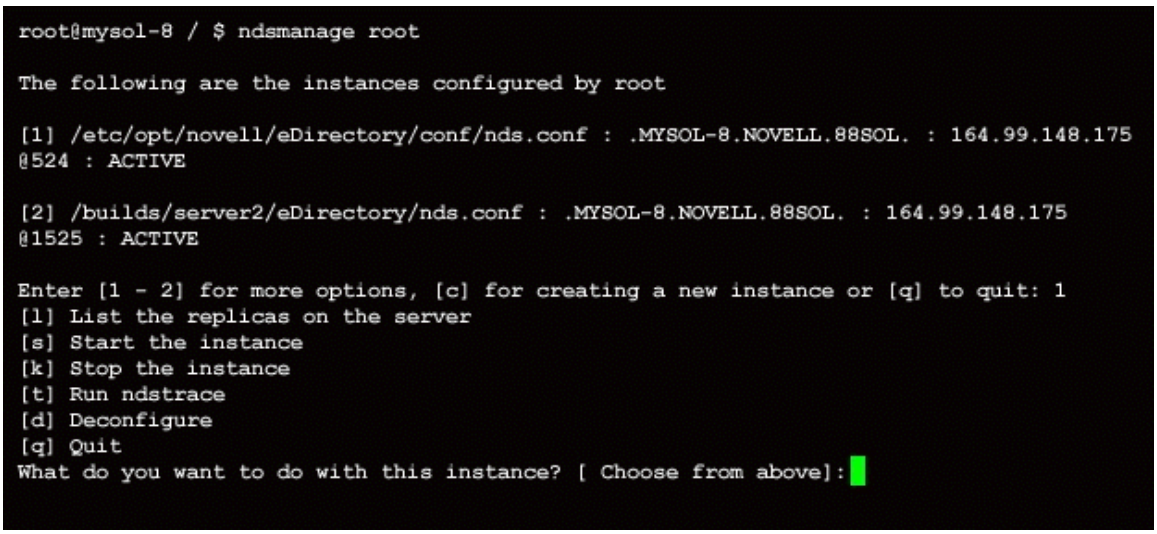
1 Введите следующую команду:

```
ndsmanage
```

2 Выберите экземпляр, который нужно запустить.

Меню расширяется для включения команд, которые можно выполнить для определенного экземпляра.

Рисунок 6-2 *Экран программы ndsmanage с командами для экземпляров*



3 Введите s для запуска экземпляра.

Также можно ввести в командной строке следующую команду:

```
ndsmanage start --config-file настроенный вами файл конфигурации экземпляра
```

Остановка определенного экземпляра

Чтобы остановить настроенный вами экземпляр, выполните следующие действия:

1 Введите следующую команду:

```
ndsmanage
```

2 Выберите экземпляр, который нужно остановить.

Меню расширяется для включения команд, которые можно выполнить для определенного экземпляра. Дополнительные сведения см. в "Экран программы ndsmanage с командами для экземпляров" на стр. 39.

3 Введите `k` для остановки экземпляра.

Также можно ввести в командной строке следующую команду:

```
ndsmanage stop --config-file настроенный вами файл конфигурации экземпляра
```

Удаление конфигурации экземпляра

Чтобы удалить конфигурацию экземпляра, выполните следующие действия:

1 Введите следующую команду:

```
ndsmanage
```

2 Выберите экземпляр, конфигурацию которого нужно удалить.

Меню расширяется для включения команд, которые можно выполнить для определенного экземпляра. Дополнительные сведения см. в "Экран программы ndsmanage с командами для экземпляров" на стр. 39.

3 Введите `d` для удаления конфигурации.

Запуск и остановка всех экземпляров

Можно запустить или остановить все экземпляры, настроенные вами.

Запуск всех экземпляров

Чтобы запустить все настроенные вами экземпляры, введите следующую команду:

```
ndsmanage startall
```

Сведения о запуске определенного экземпляра см. в "Запуск определенного экземпляра" на стр. 39.

Остановка всех экземпляров

Чтобы остановить все настроенные вами экземпляры, введите следующую команду:

```
ndsmanage stopall
```

Сведения об остановке определенного экземпляра см. в "Остановка определенного экземпляра" на стр. 39.

6.4.2 Идентификация определенного экземпляра

При настройке нескольких экземпляров каждому из них назначается имя хоста, номер порта и уникальный путь к файлу конфигурации. Для идентификации используется сочетание имени хоста и номера порта.

Для большинства программ поддерживаются параметры `-h` *`имя_сервера`*`:`*`порт`* или `--config-file` *`расположение файла конфигурации`*, при помощи которых можно указать определенный экземпляр. Дополнительные сведения см. в файлах man page программ.

6.4.3 Вызов программы для определенного экземпляра

Чтобы запустить программу для определенного экземпляра, нужно указать идентификатор этого экземпляра в команде. Идентификаторами экземпляров являются пути к файлам конфигурации, а также сочетание имени хоста и номера порта. Для этого можно использовать параметры `--config-file` *`расположение файла конфигурации`* или `-h` *`имя_хоста`*`:`*`порт`*.

Если не указать в команде идентификаторы экземпляров, программа отобразит различные принадлежащие вам экземпляры и предложит выбрать экземпляр, для которого нужно выполнить программу.

Например, чтобы запустить DSTrace для определенной программы с помощью команды `--config-file`, введите следующее:

```
ndstrace --config-file configuration_filename_with_location
```

6.5 Примеры сценария для использования нескольких экземпляров

Мария — пользователь, не имеющий прав root. Ей нужно настроить два дерева на одном и том же сервере для одного и того же двоичного файла.

6.5.1 Планирование установки

Мария указывает следующие идентификаторы экземпляров.

- **Экземпляр 1:**

Номер порта для прослушивания этим экземпляром	1524
Путь к файлу конфигурации	`/home/maryinst1/nds.conf`
Каталог DIB	`/home/mary/inst1/var`

- **Экземпляр 2:**

Номер порта для прослушивания этим экземпляром	2524
Путь к файлу конфигурации	`/home/mary/inst2/nds.conf`
Каталог DIB	`/home/mary/inst2/var`

6.5.2 Настройка экземпляров

Чтобы настроить экземпляры по указанным выше идентификаторам, Мария должна ввести следующие команды:

- **Экземпляр 1:**

```
ndsconfig new -t mytree -n o=novell -a cn=admin.o=company -b 1524 -D
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

- **Экземпляр 2:**

  ```
  ndsconfig new -t corptree -n o=novell -a cn=admin.o=company -b 2524 -D
  /home/mary/inst2/var --config-file /home/mary/inst2/nds.conf
  ```

6.5.3 Вызов программы для экземпляра

Если Марии требуется запустить программу DSTrace для экземпляра 1, прослушивающего порт 1524 с файлом конфигурации `/home/mary/inst1/nds.conf` и файлом DIB в папке `/home/mary/inst1/var`, она может запустить эту программу следующим образом:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

или

```
ndstrace -h 164.99.146.109:1524
```

Если Мария не указывает идентификаторы экземпляра, то программа отображает все экземпляры, принадлежащие ей, и предлагает выбрать экземпляр.

6.5.4 Отображение списка экземпляров

Если Марии требуется подробная информация об экземплярах на хосте, она может запустить программу ndsmanage.

- Отображение всех экземпляров, принадлежащих Марии:

  ```
  ndsmanage
  ```

- Отображение всех экземпляров, принадлежащих Джону (имя пользователя - john):

  ```
  ndsmanage john
  ```

- Отображение всех экземпляров всех пользователей определенной копии eDirectory:

  ```
  ndsmanage -a
  ```

6.6 Получение дополнительной информации

Дополнительные сведения о поддержке нескольких экземпляров см. в следующих документах:

- *Руководство по установке NetIQ eDirectory 8.8 SP8*
- Для Linux: файлы man page для ndsconfig и ndsmanage

7 Проверка подлинности в eDirectory посредством SASL-GSSAPI

Механизм SASL-GSSAPI для NetIQ eDirectory 8.8 позволяет проходить проверку подлинности eDirectory посредством LDAP с помощью билета Kerberos, без ввода пароля пользователя eDirectory. Билет Kerberos следует получить путем проверки подлинности на сервере Kerberos.

Эта функция наиболее полезна для пользователей приложений LDAP в среде с уже существующей инфраструктурой Kerberos. Поэтому такие пользователи должны иметь возможность входа на сервер LDAP без отдельного пароля для LDAP.

Для этого в eDirectory применен механизм SASL-GSSAPI.

Текущая реализация SASL-GSSAPI совместима с RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222) и поддерживает только Kerberos v5 в качестве механизма проверки подлинности.

Эта глава содержит следующие сведения:

7.1 Основные понятия

7.1.1 Что такое Kerberos?

Kerberos — это стандартный протокол для проверки подлинности в сети. В основе этого протокола лежит модель доверия между сторонами. Используются общие секреты и шифрование с симметричным ключом.

Дополнительные сведения см. в RFC 1510 (http://www.ietf.org/rfc/rfc1510.txt?number=1510).

7.1.2 Что такое SASL?

Протокол SASL предоставляет уровень абстракции проверки подлинности для приложений. Это платформа, к которой можно подключать модули проверки подлинности.

Дополнительные сведения см. в RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.1.3 Что такое GSSAPI?

Интерфейс GSSAPI предоставляет службу проверки подлинности и другие службы безопасности путем стандартного набора API. Он поддерживает различные механизмы проверки подлинности. Наиболее распространенным является Kerberos v5.

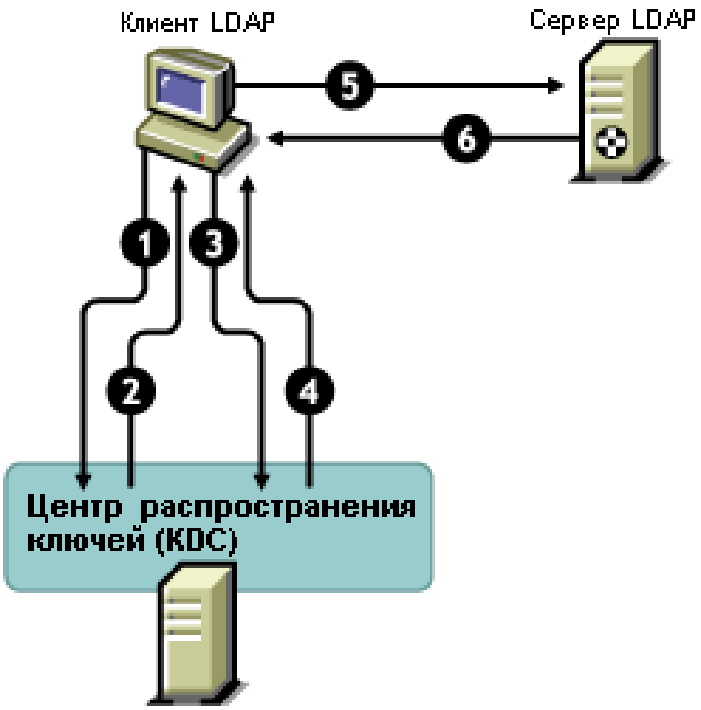
Дополнительные сведения об API GSS см. в RFC 1964 (http://www.ietf.org/rfc/rfc1964.txt?number=1964).

Данная реализация SASL-GSSAPI описана в разделе 7.2 RFC 2222 (http://www.ietf.org/rfc/rfc2222.txt?number=2222).

7.2 Как GSSAPI работает с eDirectory?

На следующей схеме показана работа GSSAPI с сервером LDAP.

Рисунок 7-1 *Каким образом работает GSSAPI?*



На приведенном выше рисунке числа обозначают следующее:

1. Пользователь eDirectory отправляет запрос через клиент LDAP на сервер центра распространения ключей Kerberos (KDC) для получения первоначального билета, который называется "билетом для получения билетов" (TGT).

KDC Kerberos может использовать решения МТИ или Microsoft*.

2. KDC выдает TGT в ответ на запрос клиента LDAP.
3. Клиент LDAP отправляет TGT обратно в KDC и запрашивает билет службы LDAP.
4. KDC выдает билет службы LDAP в ответ на запрос клиента LDAP.
5. Клиент LDAP выполняет операцию ldap_sasl_bind для сервера LDAP и отправляет билет службы LDAP.
6. Сервер LDAP проверяет билет службы LDAP с помощью механизма GSSAPI и, в зависимости от результата, отправляет клиенту LDAP ответ об успешном или неуспешном выполнении операции ldap_sasl_bind.

7.3 Настройка GSSAPI

1. Подключаемый модуль iManager для SASL-GSSAPI не будет работать, если в iManager не настроено подключение к eDirectory по протоколу SSL/TLS. Безопасное подключение необходимо для защиты главного ключа области и ключей участников.

   По умолчанию в iManager настраивается подключение к eDirectory по протоколу SSL/TLS. Если нужно настроить метод входа Kerberos для GSSAPI в дереве, отличном от дерева с конфигурацией iManager, нужно настроить подключение iManager к eDirectory по протоколу SSL/TLS.

   Дополнительные сведения о настройке в iManager подключения к eDirectory по протоколу SSL/TLS см. в *Руководству по администрированию NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).

   Подключаемый модуль iManager для SASL-GSSAPI (`kerberosPlugin.npm`) входит в файлы `eDir_88_iMan26_Plugins.npm` и `eDir_88_iMan27_Plugins.npm`. Загрузите эти NPM-файлы с веб-сайта Novell Download (http://download.novell.com).

2. Чтобы использовать билет Kerberos для проверки подлинности и входа на сервер eDirectory, необходимо:
   - **2a** Расширить схему Kerberos.
   - **2b** Создать контейнер области.
   - **2c** Извлечь ключ участника или общий ключ из KDC.
   - **2d** Создать объект участника LDAP.
   - **2e** Сопоставить имя участника Kerberos с объектом пользователя.

Для получения дополнительных сведений см. раздел "Настройка GSSAPI для eDirectory" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

7.4 Каким образом LDAP использует GSSAPI?

После настройки GSSAPI этот интерфейс добавляется вместе с другими методами SASL в атрибут `supportedSASLMechanisms` в `rootDSE`. `Корневой элемент rootDSE (DSA [Directory System Agent] Specific Entry)` - это элемент, который располагается в корне дерева

информации о каталоге (Directory Information Tree - DIT). Для получения дополнительных сведений см. раздел "Работа LDAP с eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

LDAP-сервер опрашивает SASL на предмет установленных механизмов при получении своей конфигурации и автоматически поддерживает любые установленные механизмы. LDAP-сервер также сообщает о текущих поддерживаемых механизмах SASL в своем `rootDSE` с помощью атрибута `supportedSASLMechanisms`.

Поэтому при настройке GSSAPI этот механизм используется по умолчанию. Тем не менее, чтобы явным образом выполнить операцию LDAP посредством механизма SASL GSSAPI, можно указать GSSAPI в командной строке.

Например, для поиска в OpenLDAP с помощью механизма GSSAPI введите следующую команду:

```
ldapsearch -Y GSSAPI -h 164.99.146.48 -b "" -s base
```

7.5 Основные термины

В следующей таблице перечисляется распространенная терминология, связанная с Kerberos и GSSAPI.

Таблица 7-1 *Терминология Kerberos/GSSAPI*

Термин	Определение
Центр распространения ключей (KDC)	Сервер Kerberos, выполняющий проверку подлинности пользователей и выдающий ключи.
Участник системы защиты	Объект (пользователь или экземпляр службы), зарегистрированный в KDC.
Область	Домен или группа объектов, обслуживаемые набором KDC.
Билет службы (ST)	Запись, содержащая информацию о клиенте, информацию о службе и ключ сеанса, зашифрованный с помощью открытого ключа объекта определенной службы
Билет для получения билетов (TGT)	Билет, с помощью которого клиент может получить другие билеты Kerberos.

8 Принудительное применение универсальных паролей с учетом регистра

В NetIQ eDirectory 8.8 можно включить универсальный пароль и включить учет регистра в паролях при доступе к серверу eDirectory 8.8 с помощью следующих клиентов и программ:

- Novell Client 4.9 и более поздних версий
- Программы администрирования, обновленные до eDirectory 8.8
- NetIQ iManager 2.7 и более поздних версий (кроме использования под управлением Windows)

Пароли с учетом регистра можно использовать в любой версии LDAP SDK.

В следующей таблице перечислены платформы, поддерживающие пароли с учетом регистра:

Возможность	Linux	Windows
Принудительное применение универсальных паролей с учетом регистра	✓	✓

Эта глава содержит следующие сведения:

8.1 Необходимость паролей с учетом регистра

Использование паролей с учетом регистра повышает безопасность при входе в каталоги. Например, если задан пароль "aBc" с учетом регистра, то все попытки входа с паролями "Abc", "abc" или "ABC" будут неудачными.

В eDirectory 8.8 и более поздних версиях можно включить учет регистра в паролях для всех клиентов, обновленных до eDirectory 8.8.

Применяя пароли с учетом регистра, можно запретить устаревшим клиентам Novell доступ к серверу eDirectory 8.8. Для получения дополнительных сведений см. Раздел 8.4, "Предотвращение доступа устаревших клиентов к серверу eDirectory 8.8" на стр. 50.

8.2 Как включить учет регистра в паролях

В eDirectory 8.8 и более поздних версиях можно включить учет регистра в паролях для всех клиентов путем включения универсального пароля. Универсальный пароль отключен по умолчанию.

8.2.1 Необходимые условия

По умолчанию LDAP и другие серверные программы сначала используют вход NDS, а затем, если он безуспешен, вход по простому паролю. Для использования пароля с учетом регистра вход должен осуществляться через службу NMAS. Поэтому нужно настроить для переменной среды `NDSD_TRY_NMASLOGIN_FIRST` значение "true", чтобы включить пароли с учетом регистра.

Выполните следующую процедуру для включения паролей с учетом регистра:

1. Установите переменную среды
   - Linux:

     Добавьте следующий текст в конце строки `/opt/novell/eDirectory/sbin/pre_ndsd_start`.

     ```
     NDSD_TRY_NMASLOGIN_FIRST=true
     export NDSD_TRY_NMASLOGIN_FIRST
     ```

   - Windows:

     Щелкните правой кнопкой мыши "Мой компьютер" и выберите "Свойства". Перейдите на вкладку "Дополнительно" и нажмите кнопку "Переменные среды". В разделе "Системные переменные" добавьте переменную и установите для нее значение "true".
2. Перезапустите сервер eDirectory.

ПРИМЕЧАНИЕ. При использовании проверки подлинности NMAS увеличивается время входа в систему.

8.2.2 Включение учета регистра в пароле

1. Войдите в eDirectory, используя существующий пароль.

   При новой установке существующий пароль — тот, который был указан при настройке eDirectory 8.8.

   Например, ваш пароль — "novell".

   ПРИМЕЧАНИЕ. В этом пароле не учитывается регистр.
2. Включите универсальный пароль.

   Для получения дополнительных сведений см. раздел "Развертывание универсального пароля" в *Руководстве по администрированию Novell Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).
3. Выйдите из eDirectory.
4. Войдите в eDirectory, используя существующий пароль с нужным регистром.

   У указанного сейчас пароля будет учитываться регистр.

Например, можно ввести "NoVELL".

Теперь ваш пароль — "NoVELL". После этого войти в систему, используя пароль "novell" или любые другие сочетания заглавных и строчных букв, отличных от "NoVELL", будет невозможно.

При переходе на пароли с учетом регистра см. Раздел 8.3.1, "Переход на пароли с учетом регистра" на стр. 49.

В новых паролях будет учитываться регистр в зависимости от того, на каком уровне (на уровне объекта или раздела) включен универсальный пароль.

8.2.3 Управление паролями с учетом регистра

Можно управлять учетом регистра в паролях, включая и отключая универсальный пароль с помощью iManager. Для получения дополнительных сведений см. раздел "Развертывание универсального пароля" в *Руководстве по администрированию Novell Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

8.3 Обновление устаревших клиентов Novell и программ

Ниже перечислены последние версии клиентов Novell и программ NetIQ:

- Novell Client 4.9
- Программы администрирования в eDirectory 8.8
- NetIQ iManager 2.7 и более поздние версии

Клиенты и программы более ранних версий по сравнению с перечисленными считаются устаревшими.

Можно использовать пароли с учетом регистра для устаревших клиентов Novell после их обновления до последних версий. В eDirectory 8.8 переход с существующих паролей на пароли с учетом регистра осуществляется очень просто и гибко. Для получения дополнительных сведений см. Раздел 8.3.1, "Переход на пароли с учетом регистра" на стр. 49.

Если не обновить устаревшие клиенты до последних версий, доступ этих клиентов к eDirectory 8.8 можно заблокировать на уровне сервера. Для получения дополнительных сведений см. Раздел 8.4, "Предотвращение доступа устаревших клиентов к серверу eDirectory 8.8" на стр. 50.

8.3.1 Переход на пароли с учетом регистра

Универсальный пароль по умолчанию отключен, поэтому существующие пароли не будут затронуты до включения универсального пароля в iManager. Пошаговые инструкции см. в разделе Раздел 8.2, "Как включить учет регистра в паролях" на стр. 48.

В следующем примере поясняется переход на пароли с учетом регистра.

Сеанс входа 1: универсальный пароль отключен по умолчанию.

- Войдите в систему, используя существующий пароль. Например, ваш пароль — "netiq".

- В этом пароле не учитывается регистр. Для входа в систему можно указывать и "netiq", и "NetIQ".
- После входа в системы включите универсальный пароль. Для получения дополнительных сведений см. раздел "Развертывание универсального пароля" в *Руководстве по администрированию Novell Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html).

Сеанс входа 2: универсальный пароль был включен в прошлом сеансе.

- Войдите в систему, используя существующий пароль. Например, предположим, вы ввели пароль "noVell".
- Если включить универсальный пароль, в пароле начинает учитываться регистр. Запомните пароль в точности в том виде, в каком вы ввели его на этот раз.

Сеанс входа 3 и последующие попытки входа.

- Вход в систему с паролем netIQ будет успешным.
- Если вы попытаетесь войти в систему с паролем NetIQ (или любой другой версией, кроме noVell), вход будет запрещен.

8.4 Предотвращение доступа устаревших клиентов к серверу eDirectory 8.8

В eDirectory 8.7.1 и 8.7.3 можно было запретить устаревшим клиентам Novell устанавливать и изменять пароль NDS. В eDirectory 8.8 также можно запретить им входить в eDirectory 8.8 и проверять пароли.

Чтобы разрешить или запретить устаревшим клиентам Novell доступ к eDirectory 8.8 необходимо настроить вход в NDS с помощью iManager или LDAP.

В этом разделе содержатся следующие сведения.

8.4.1 Необходимость предотвращения доступа устаревших клиентов к серверу eDirectory 8.8

В паролях устаревших клиентов Novell не учитывается регистр. Поэтому, если нужно принудительно использовать пароли с учетом регистра в eDirectory 8.8 или более поздних версиях, может потребоваться заблокировать доступ устаревших клиентов к каталогу.

В версиях до Novell Client 4.9 универсальный пароль не поддерживался. Это было обусловлено тем, что изменения пароля применялись непосредственно к паролю NDS, а не к NMAS. При использовании универсального пароля изменение паролей с помощью устаревших клиентов может вызвать проблему, называемую "искажением паролей". Это означает, что пароль NDS и универсальный пароль не синхронизированы. Чтобы избежать этой проблемы, можно заблокировать изменения пароля клиентами версии до 4.9.

Дополнительные сведения о запрете доступа устаревших клиентов к серверу eDirectory 8.8 см. в следующем разделе Управление конфигурациями входа NDS.

8.4.2 Управление конфигурациями входа NDS

Настроив вход NDS, можно разрешить или запретить устаревшим клиентам Novell доступ к серверу eDirectory 8.8. Можно управлять конфигурациями входа NDS с помощью iManager 2.6 и LDAP.

В eDirectory 8.8 и более поздних версиях можно настроить установку и изменение паролей с помощью LDAP и iManager.

Этот раздел содержит информацию о следующем:

Конфигурации NDS на различных уровнях

Можно настроить вход в NDS на одном из следующих уровней:

- Уровень разделов
- Уровень объектов

Если ни на одном из уровней не задана настройка, то настройка регистрации NDS разрешена на всех уровнях.

Настройка на уровне объекта приоритетнее настройки на уровне раздела. Описание см. в следующей таблице:

Таблица 8-1 *Конфигурация NDS*

Конфигурация на уровне объектов	Конфигурация на уровне разделов	Конфигурация
Не указано	Включено	Включено
Включено	Не указано	Включено
Не указано	Отключено	Отключено
Отключено	Не указано	Отключено
Включено	Включено	Включено
Включено	Отключено	Включено
Отключено	Включено	Отключено
Отключено	Отключено	Отключено

На всех уровнях (объект и раздел) можно настроить вход в NDS для следующего:

- Вход в каталог с помощью пароля NDS или проверка пароля NDS
- Установка нового пароля и изменение существующего пароля

Вход в каталог или проверка пароля NDS

Пароль входа/проверки NDS означает:

- Вход в каталог с помощью пароля NDS.
- Просмотр существующего пароля в каталоге.

Пароль входа/проверки NDS включен по умолчанию. Если отключить ключ входа/проверки, вы не сможете входить в последнюю версию eDirectory и проверять пароль. Можно включить и отключить пароль входа/проверки NDS на уровне раздела и на уровне объектов. При отключенном пароле входа/проверки невозможно устанавливать или изменять пароли NDS.

Можно настроить пароль входа/проверки NDS с помощью iManager и LDAP. Дополнительные сведения см. в разделах "Управление конфигурациями NDS с помощью iManager" на стр. 52 и "Управление конфигурациями NDS с помощью LDAP" на стр. 53.

Установка нового пароля или изменение существующего пароля NDS

Установка/изменение пароля NDS означает:

- Установка нового пароля для объекта.
- Изменение существующего пароля для объекта.

Установка/изменение пароля NDS включено по умолчанию. Если ключ установки/изменения отключен, вы не сможете устанавливать новые пароли и изменять существующие пароли в eDirectory. Можно включить и отключить установку/изменение пароля NDS на уровне раздела и на уровне объектов. При отключенном пароле входа/проверки невозможно устанавливать или изменять пароли.

Ранее устанавливать и изменять пароли NDS можно было только с помощью LDAP. Теперь это можно сделать и с помощью iManager. Дополнительные сведения см. в разделах "Управление конфигурациями NDS с помощью iManager" на стр. 52 и "Управление конфигурациями NDS с помощью LDAP" на стр. 53.

Управление конфигурациями NDS с помощью iManager

В этом разделе содержатся следующие сведения.

Можно включить параметры login/verify key или set/change key в конфигурации входа NDS.

Включение и отключение конфигурации NDS для раздела

Включение входа NDS для клиентов более ранних версий по сравнению с eDirectory 8.8:

1. В iManager нажмите кнопку *Роли и задачи*  .
2. Выберите *NMAS > Universal Password Enforcement (Требование универсального пароля)*.
3. В подключаемом модуле применения универсального пароля выберите *Настройка NDS для раздела*.
4. Следуйте инструкциям в мастере настройки NDS для раздела, чтобы настроить управление именем пользователя и паролем на уровне раздела.

   Справка доступна в каждом экране мастера.

Включение и отключение конфигурации NDS для объекта

Включение входа NDS для клиентов более ранних версий по сравнению с eDirectory 8.8:

1. В iManager нажмите кнопку *Роли и задачи*  .
2. Выберите *NMAS > Universal Password Enforcement (Требование универсального пароля)*.
3. В мастере выберите *Конфигурация NDS для объекта*.
4. Следуйте инструкциям в мастере настройки NDS для объекта, чтобы настроить управление именем пользователя и паролем на уровне объекта.

   Справка доступна в каждом экране мастера.

Управление конфигурациями NDS с помощью LDAP

ЗАМЕЧАНИЕ. Настоятельно рекомендуем использовать iManager, а не LDAP, для управления конфигурациями NDS.

Можно управлять конфигурациями NDS через LDAP, применяя атрибут eDirectory к контейнеру корневого элемента раздела или объекту. Атрибуты входят в состав схемы eDirectory 8.7.1 и более поздних версий и не поддерживаются в eDirectory 8.7 и более ранних версиях.

Метод, который используется устаревшими клиентами для настройки конфигураций входа NDS, называется управлением входом NDAP. Метод, используемый для настройки паролей NDS, называется управлением паролями NDAP.

В этом разделе содержатся сведения о следующем:

- "Включение и отключение конфигурации NDS для раздела" на стр. 53
- "Включение и отключение конфигурации NDS для объекта" на стр. 54

Включение и отключение конфигурации NDS для раздела

Управление паролем входа и проверки

Используйте атрибут `ndapPartitionLoginMgmt`, чтобы включить или отключить вход NDS и проверить управление паролями для раздела.

Значение атрибута `ndapPartitionLoginMgmt`	Описание
Отсутствует или не указан	Управление входом NDAP включено.
0	Управление входом NDAP отключено.
1	Управление входом NDAP включено.

Настройка и изменение пароля NDS

Используйте атрибут `ndapPartitionPasswordMgmt`, чтобы включить или отключить установку и изменение паролей NDS для разделов.

Значение атрибута `ndapPartitionPasswordMgmt`	Описание
Отсутствует или не указан	Управление паролями NDAP включено.
0	Управление паролями NDAP отключено.
1	Управление паролями NDAP включено.

Включение и отключение конфигурации NDS для объекта

Пароль входа/проверки NDS

Используйте атрибут `ndapLoginMgmt`, чтобы включить или отключить вход NDS и проверить управление объектом.

Значение атрибута `ndapLoginMgmt`	Описание
Отсутствует или не указан	Управление входом NDAP зависит от конфигурации на уровне раздела.
0	Управление входом NDAP отключено, если оно отключено на уровне раздела.
1	Управление входом NDAP включено независимо от конфигурации на уровне раздела.

Настройка и изменение пароля NDS

Используйте атрибут `ndapPasswordMgmt`, чтобы включить или отключить установку и изменение паролей NDS для объектов.

Значение атрибута `ndapPasswordMgmt`	Описание
Отсутствует или не указан	Управление паролями NDAP зависит от конфигурации на уровне раздела.
0	Управление паролями NDAP отключено, если оно отключено на уровне раздела.
1	Управление паролями NDAP включено независимо от конфигурации на уровне раздела.

ПРИМЕЧАНИЕ. Дополнительные сведения о создании и управлении политиками приоритетной синхронизации см. в разделах "Использование программ LDAP в Linux" и "Программа импорта, экспорта и преобразования NetIQ" в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

8.4.3 Действия с разделом

При разделении раздела конфигурации NDS не наследуются дочерним разделом. При слиянии разделов конфигурации NDS родительского раздела сохраняются в итоговом разделе.

8.4.4 Применение паролей с учетом регистра в смешанном дереве

Если существует дерево на сервере eDirectory 8.8 или более поздней версии и на сервере eDirectory 8.7 или более ранней версии, и эта два сервера имеют общий раздел, то отключение конфигурации входа NDS на этом разделе приведет к непредсказуемым результатам. В сервере версии 8.8 этот параметр будет применен принудительно, вследствие чего устаревшие клиенты не будут иметь доступ к каталогу. Но в сервере версии 8.7 этот параметр не будет применен, поэтому можно будет получить доступ к каталогу посредством сервера версии 8.7.

8.5 Получение дополнительной информации

Дополнительные сведения о паролях с учетом регистра см. в следующих документах:

- Встроенная справка iManager
- Раздел "Развертывание универсального пароля" в *Руководстве по администрированию NetIQ Password Management 3.3* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/allq21t.html)

9 Поддержка политики паролей Microsoft Windows Server 2008

В прежних версиях eDirectory пользователи могли использовать либо политику Microsoft по умолчанию, либо устаревший синтаксис Novell. В NetIQ eDirectory 8.8 SP8 поддерживаются политики паролей, соответствующие требованиям Microsoft Windows Server 2008 и отличающиеся от прежних политик Microsoft в отношении сложности паролей. Можно использовать iManager для создания политики паролей с помощью нового синтаксиса Microsoft Windows Server 2008 и настроить эту политику нужным образом.

Эта глава содержит следующие сведения:

9.1 Создание политик паролей Windows Server 2008

Можно использовать iManager для создания политик паролей, соответствующих требованиям Microsoft Windows Server 2008, и назначит пользователей в среде eDirectory новой политике. Подробные инструкции по созданию политик паролей см. в *Руководстве по администрированию NetIQ Password Management 3.3.2* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html).

ПРИМЕЧАНИЕ

- Перед созданием новой политики паролей с использованием синтаксиса Microsoft Server 2008 необходимо установить наиболее позднюю версию подключаемого модуля Novell iManager Password Management. Сведения об установке подключаемых модулей iManager см. в *Руководстве по администрированию NetIQ iManager 2.7* (https://www.netiq.com/documentation/imanager/imanager_admin/data/hk42s9ot.html).
- Также необходимо включить универсальный пароль и расширенные правила паролей для политики, которую нужно создать или настроить.

9.2 Управление политиками паролей в Windows Server 2008

Можно управлять политиками паролей, соответствующими требованиям по сложности паролей Windows Server 2008, с помощью iManager. Для получения дополнительных сведений см. раздел "Управление паролей с помощью политик" в *Руководстве по администрированию Novell Password Management 3.3.2* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/ampxjj0.html).

9.3 Получение дополнительной информации

Дополнительные сведения о политиках паролей в eDirectory см. в следующих документах:

- Встроенная справка iManager
- *Руководство по администрированию Novell Password Management 3.3.2* (http://www.netiq.com/documentation/password_management33/pwm_administration/data/bookinfo.html)
- *Руководство по администрированию Novell Modular Authentication Services 3.3.4* (http://www.netiq.com/documentation/nmas33/admin/data/a20gkue.html)

10 Приоритетная синхронизация

Приоритетная синхронизация — это новая функция NetIQ eDirectory 8.8, дополняющая существующий процесс синхронизации в eDirectory. Приоритетная синхронизация служит для мгновенной синхронизации измененных важных данных, таких как пароли.

Применять приоритетную синхронизацию следует в случаях, когда обычная синхронизация слишком медленна. Процесс приоритетной синхронизации работает быстрее процесса обычной синхронизации. Приоритетная синхронизация поддерживается только между двумя или более серверами eDirectory 8.8 или более поздних версий, на которых размещен один и тот же раздел.

В следующей таблице перечислены платформы, поддерживающие приоритетную синхронизацию:

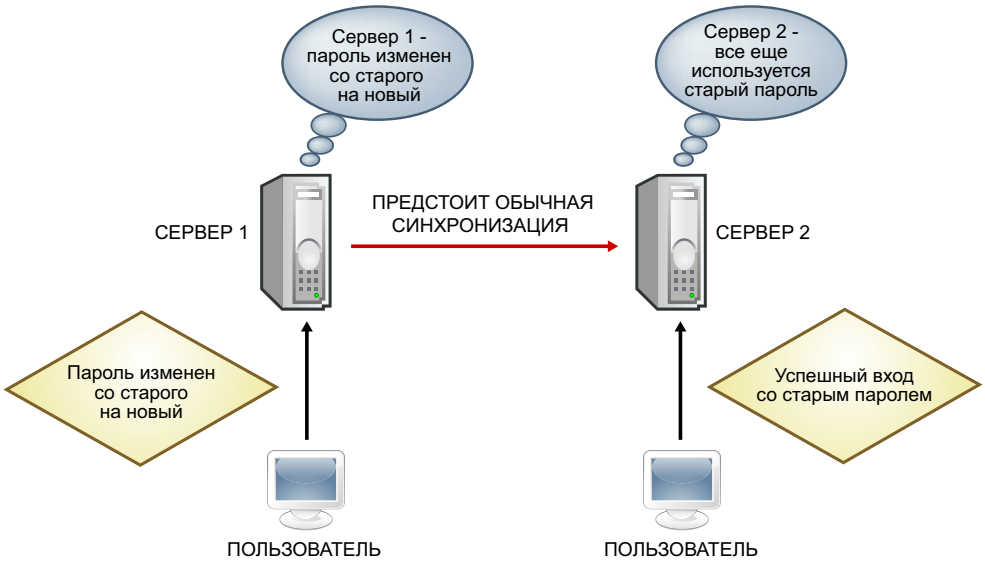
Список функций	Linux	Windows
Приоритетная синхронизация	✓	✓

Эта глава содержит следующие сведения:

10.1 Необходимость приоритетной синхронизации

Обычная синхронизация занимает определенное время, в течение которого измененные данные не будут доступны на других серверах. Например, предположим, что в вашей среде разные приложения обмениваются данными с каталогом. Вы изменяете пароль на сервере Server1. При обычной синхронизации проходит некоторое время перед синхронизацией этого изменения с сервером Server2. Поэтому пользователь сможет пройти проверку подлинности с помощью приложения, обменивающегося данными с сервером Server2, используя прежний пароль.

Рисунок 10-1 *Необходимость приоритетной синхронизации*



В крупной среде требуется мгновенная синхронизация при изменении важных данных объекта. Процесс приоритетной синхронизации решает эту задачу.

10.2 Использование приоритетной синхронизации

Для приоритетной синхронизации изменений данных требуется выполнить следующие действия:

1. Включите приоритетную синхронизацию, настройте количество потоков и размер очереди с помощью iMonitor.
2. Определите политики приоритетной синхронизации, указав важные атрибуты с помощью iManager.
3. Примените политики приоритетной синхронизации к разделам с помощью iManager.

10.3 Получение дополнительной информации

Дополнительные сведения о приоритетной синхронизации см. в следующих документах:

- *Руководство по администрированию NetIQ eDirectory 8.8 SP8*
- Встроенная справка iManager и iMonitor

11 Шифрование данных

В NetIQ eDirectory 8.8 и более поздних версиях можно зашифровать определенные данные на диске и при их передаче между серверами eDirectory 8.8. Это обеспечивает более надежную защиту конфиденциальных данных.

В следующей таблице перечислены платформы, поддерживающие шифрование данных:

Возможность	Linux	Windows
Зашифрованные атрибуты	✓	✓
Зашифрованная репликация	✓	✓

Эта глава содержит следующие сведения:

11.1 Шифрование атрибутов

В eDirectory 8.8 можно шифровать конфиденциальные данные, хранящиеся на диске. Зашифрованные атрибуты — это серверная функция.

Доступ к зашифрованным атрибутам возможен только по безопасным каналам, если не включен доступ и по обычным каналам. Для получения дополнительных сведений см. Раздел 11.1.3, "Доступ к зашифрованным атрибутам" на стр. 62.

В этом разделе содержатся следующие сведения.

Зашифрованные атрибуты поддерживаются только в eDirectory 8.8 и более поздних версиях.

11.1.1 Необходимость шифрования атрибутов

До eDirectory 8.8 данные хранились на диске в виде незашифрованного текста. Требовалось защитить данные и предоставлять доступ к данным только по безопасным каналам.

Эту функцию можно использовать в случаях, когда нужно защитить конфиденциальные данные, например данные кредитных карт клиентов банка.

11.1.2 Методики шифрования атрибутов

Можно шифровать атрибуты, создавая и определяя политики зашифрованных атрибутов, и применяя эти политики к серверам. Можно создавать, определять, применят и управлять политиками зашифрованных атрибутов с помощью iManager и LDAP.

1 Создайте и определите политику зашифрованных атрибутов:

   1a Определите атрибуты для шифрования.

   1b Определите схему шифрования для атрибутов.

2 Примените политику шифрования атрибутов к серверу.

11.1.3 Доступ к зашифрованным атрибутам

Доступ к зашифрованным атрибутам возможен только по безопасным каналам, таким как порт LDAP SSL или порт HTTPS. Можно разрешить доступ к зашифрованным атрибутам по незащищенным каналам с помощью подключаемого модуля iManager. Дополнительные сведения см. в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

11.2 Шифрование репликации

Зашифрованная репликация относится к шифрованию данных, передаваемых между двумя или более серверами eDirectory 8.8.

Зашифрованная репликация дополняет обычную синхронизацию eDirectory.

В этом разделе содержатся следующие сведения.

- Раздел 11.2.1, "Необходимость шифрования репликации" на стр. 62
- Раздел 11.2.2, "Включение шифрования репликации" на стр. 63

11.2.1 Необходимость шифрования репликации

До eDirectory 8.8 данные при репликации передавались в виде незашифрованного текста. Требовалось защитить передаваемые конфиденциальные данные путем шифрования, особенно если реплики были разнесены географически и подключены через Интернет.

Эту функцию можно использовать в следующих сценариях:

- Если серверы каталогов распределены географически и подключены друг к другу посредством глобальной сети или Интернета, и необходимо шифровать передаваемые данные.
- Если нужно защитить лишь некоторые разделы дерева, можно выбрать разделы с конфиденциальными данными для шифрования при репликации.
- Если требуется использовать зашифрованную репликацию между определенными репликами раздела, содержащего конфиденциальные данные.
- Если есть основания считать используемую сеть ненадежной, имеет смысл защитить конфиденциальные данные при репликации.

11.2.2 Включение шифрования репликации

Можно включить шифрование репликации с помощью iManager. Можно включить зашифрованную репликацию на уровне раздела и на уровне реплики.

ЗАМЕЧАНИЕ. Перед включением зашифрованной репликации убедитесь, что и исходный сервер, и сервер назначения обладают сертификатами по умолчанию. Если сертификаты были изменены, например, переименованы, зашифрованная репликация не будет работать.

11.3 Получение дополнительной информации

Дополнительные сведения о шифровании данных в eDirectory см. в следующих документах:

- *Руководство по администрированию NetIQ eDirectory 8.8 SP8*
- Встроенная справка iManager и iMonitor

12 Производительность при пакетной нагрузке

В NetIQ eDirectory 8.8 повышена производительность при обработке массовой нагрузки.

Сведения о повышении производительности при массовой нагрузке см. в следующих разделах *Руководства по администрированию NetIQ eDirectory 8.8 SP8*:

- "Параметры кэша eDirectory"
- "Параметр размера транзакций LBURP"
- "Увеличение количества асинхронных запросов в ICE"
- "Увеличенное количество потоков записи LDAP "
- "Отключение проверки схемы в ICE"
- "Отключение шаблонов ACL"
- "Фоновый компоновщик"
- "Включение/отключение встроенного кэша"
- "Увеличение времени ожидания LBURP"
- "Offline Bulkload Utility"

13 Подключаемые модули iManager ICE

До NetIQ eDirectory 8.8 некоторые параметры командной строки программы Novell Import Conversion Export (ICE) не имели соответствующих параметров в подключаемом модуле iManager.

В следующей таблице перечислены платформы, поддерживающие эту функцию:

Возможность	Linux	Windows
Расширения ICE iManager	✓	✓

Мастер ICE в составе iManager 2.7 с eDirectory 8.8 предоставляет следующие возможности:

- Добавление отсутствующей схемы
- Сравнение схемы
- Создание файла порядка

13.1 Добавление отсутствующей схемы

В eDirectory 8.8 с помощью iManager можно добавить отсутствующую схему в схему сервера. Этот процесс включает сравнение источника и назначения. Если в исходной схеме есть дополнительная схема, она будет добавлена в схему назначения. Источник может быть файлом или LDAP-сервером, а назначение должно быть LDAP-сервером.

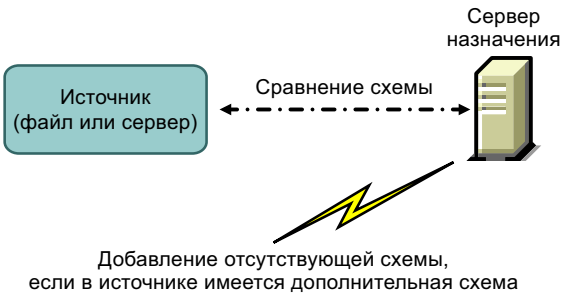
С помощью мастера ICE в iManager можно добавить отсутствующую схему с помощью следующих параметров:

- Добавить схему из файла
- Добавить схему с сервера

13.1.1 Добавить схему из файла

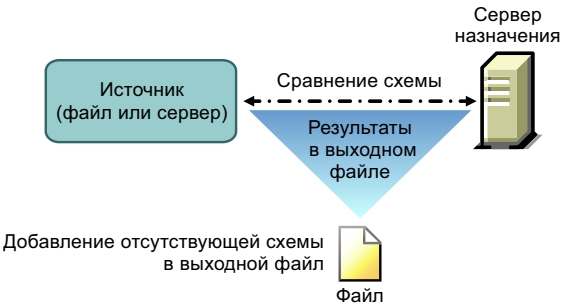
ICE может сравнить схему в исходном расположении и в месте назначения. Источник может быть файлом или LDAP-сервером, а назначение должно быть LDAP-сервером. Исходный файл схемы может быть в формате LDIF или SCH.

Рисунок 13-1 *Сравнить и добавить схему из файла*



Чтобы только сравнить схемы, но не добавлять дополнительную схему на сервер назначения, выберите *Не добавлять, а сравнивать*. В этом случае дополнительная схема не добавляется на сервер назначения, но различия между схемами доступны по ссылке в конце операции.

Рисунок 13-2 *Сравнить схему и добавить результаты в выходной файл*



Для получения дополнительных сведений см. раздел "Программы управления NetIQ eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

13.1.2 Добавить схему с сервера

Источник и место назначения — серверы LDAP.

Чтобы только сравнить схемы, но не добавлять дополнительную схему на сервер назначения, выберите *Не добавлять, а сравнивать*. В этом случае дополнительная схема не добавляется на сервер назначения, но различия между схемами доступны по ссылке в конце операции.

Для получения дополнительных сведений см. раздел "Программы управления NetIQ eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

13.2 Сравнение схемы

С помощью iManager можно сравнивать схему в исходном расположении и в месте назначения. Источник может быть файлом или сервером, а назначение должно быть LDIF-файлом.

iManager сравнивает схему между исходным расположением и местом назначения, а затем сохраняет результаты в выходном файле.

С помощью мастера ICE в iManager можно сравнить схему с помощью следующих параметров:

- Сравнить файлы схемы
- Сравнить схему между севером и файлом

13.2.1 Сравнить файлы схемы

Параметр *Сравнить файлы схемы* сравнивает схему между исходным файлом и файлом назначения, а затем сохраняет результаты в выходном файле. Чтобы добавить отсутствующую схему в файл назначения, примените записи выходного файла к файлу назначения.

Для получения дополнительных сведений см. раздел "Программы управления NetIQ eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

13.2.2 Сравнить схему между севером и файлом

Параметр *Сравнить схему между сервером и файлом* сравнивает схему между исходным сервером и файлом назначения, а затем сохраняет результаты в выходном файле. Чтобы добавить отсутствующую схему в файл назначения, примените записи выходного файла к файлу назначения.

Для получения дополнительных сведений см. раздел "Программы управления NetIQ eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

13.3 Создание файла порядка

Этот параметр создает файл команд, используемый совместно с обработчиком разделителей для импорта данных из файла данных с разделителями. Мастер помогает создать файл команд, содержащий список атрибутов для определенного класса объектов.

Для получения дополнительных сведений см. раздел "Программы управления NetIQ eDirectory" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

13.4 Получение дополнительной информации

Дополнительные сведения об этой функции см. в следующих источниках:

- *Руководство по администрированию NetIQ eDirectory 8.8 SP8*
- Встроенная справка iMonitor

14 Резервное копирование на базе LDAP

Резервное копирование на базе LDAP впервые реализовано в NetIQ eDirectory 8.8. Эта функция используется для поочередного резервного копирования атрибутов и значений атрибутов объектов.

В следующей таблице перечислены платформы, поддерживающие эту функцию:

Возможность	Linux	Windows
Резервное копирование на базе LDAP	✓	✓

Эта функция позволяет выполнять добавочное резервное копирование: объект копируется лишь в том случае, если он был изменен.

Резервное копирование на базе LDAP предоставляет набор интерфейсов для резервного копирования и восстановления объектов eDirectory, доступ к которым реализуется через LDAP Libraries for C посредством расширенных операций LDAP.

Дополнительные сведения о SDK LDAP Libraries for C см. в документации по LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

Пример резервного копирования и восстановления объектов eDirectory с помощью LDAP см. в образце кода backup.c (http://developer.novell.com/ndk/doc/samplecode/cldap_sample/extensions/backup.c.html).

14.1 Необходимость резервного копирования на базе LDAP

Резервное копирование на базе LDAP устраняет проблемы, присущие существующей методике резервного копирования и восстановления.

Эта функция устраняет следующие проблемы:

- Предоставляет стандартный интерфейс, с помощью которого приложения для резервного копирования сторонних разработчиков могут работать на всех платформах, поддерживаемых решением eDirectory.
- Предоставляет решение для добавочного резервного копирования объектов.

14.2 Получение дополнительной информации

Дополнительные сведения об этой функции см. в следующих источниках:

- Библиотеки LDAP для C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html)
- Образец кода: backup.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/backup.c.html)

15 Получение списка действующих разрешений LDAP

API получения списка действующих разрешений LDAP появился в NetIQ eDirectory 8.8 SP6.

В следующей таблице перечислены платформы, поддерживающие эту функцию:

Возможность	Linux	Windows
Получение списка действующих разрешений LDAP	✓	✓

Эту функцию можно использовать для получения действующих разрешений заданного DN для заданного целевого DN при заданном наборе атрибутов. Эта функция предоставляет интерфейс для получения списка прав через LDAP Libraries for C посредством расширенных операций LDAP.

Дополнительные сведения о SDK LDAP Libraries for C см. в документации по LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/ldaplibc/data/hevgtl7k.html).

15.1 Необходимость интерфейса для получения списка действующих разрешений LDAP

Интерфейс получения списка действующих разрешений LDAP пытается устранить эти проблемы с API.

Эта функция устраняет следующие проблемы:

- Для получения действующих прав нескольких атрибутов достаточного одного запроса к каталогу.
- Сокращается время отправки запроса в каталог для получения действующих прав нескольких атрибутов.
- Идентификация ошибок в запросе или в каталоге.

15.2 Получение дополнительной информации

Дополнительные сведения об этой функции см. в следующих источниках:

- Библиотеки LDAP для C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html).
- Образец кода: getpriv.c (http://developer.novell.com/documentation/samplecode/cldap_sample/extensions/getpriv.c.html).

16 Управление ведением журнала ошибок в eDirectory 8.8

Многие клиенты жаловались, что журнал ошибок в NetIQ eDirectory не особенно полезен при выявлении и устранении распространенных неполадок. Ведение журнала ошибок запускается автоматически при установке eDirectory.

Эта глава содержит следующие разделы:

16.1 Уровни важности сообщений

Каждому сообщению присваивается определенный уровень важности, что позволяет определить серьезность этого сообщения. Уровни в порядке снижения важности:

16.1.1 Неустранимая

Сообщение о неустранимой ошибке указывает на серьезную проблему, например, потерю данных или утрату функциональности.

Примеры:

- Если серверу eDirectory не удается загрузить системные модули, такие как NCPEngine и DSLoader, в журнал записывается неустранимая ошибка.
- Если серверу eDirectory не удается установить привязку с безопасному порту 636, в журнал записывается неустранимая ошибка.

16.1.2 Предупреждение

Сообщение, которое не обязательно связано с неустранимой ошибкой, но может быть причиной последующих неполадок.

Примеры:

- Ошибки подключения между любыми двумя серверами в дереве, из-за чего сервер добавляется в кэш недействующих адресов. Сервер можно восстановить из этого состояния, сбросив кэш недействующих адресов.
- Если приложение клиента LDAP осуществляет привязку и закрывает подключение без отмены привязки, то сервер LDAP должен занести в журнал соответствующее предупреждение.
- Если сервер eDirectory израсходовал все дескрипторы файлов и достиг предела, поскольку сервер не может обрабатывать входящие запросы и отвечать на них, это приводит к сбою приложения.

16.1.3 Ошибка

Сообщение, которое может быть вызвано неверной работой, но не ведущее ни к каким дальнейшим неполадкам.

Примеры:

- Если приложение клиента пытается добавить объект, атрибуты которого не определены в схеме, сервер eDirectory выдаст ошибку ERR_NO_SUCH_ATTRIBUTE.
- Если пользователь попытается войти в систему с неверным паролем, сервер eDirectory выдаст ошибку ERR_FAILED_AUTHENTICATION.

16.1.4 Информация

Сообщение, описывающее успешное выполнение действия или события на сервере eDirectory.

Примеры:

- Если модуль успешно загружается или выгружается, можно занести в журнал соответствующее информационное сообщение.
- При изменении конфигурации кэша базы данных следует заносить в журнал информационное сообщение об успешном сохранении конфигурации.

16.1.5 Отладка

Сообщение с информацией, помогающей разработчикам в отладке программ.

Примеры:

При динамическом поиске отображаются все члены динамических групп с указанием идентификаторов записей и разделов, а также DN членов. Эта информация поможет убедиться в том, что все участники возвращены на уровне eDirectory.

16.2 Настройка ведения журнала ошибок

16.2.1 Linux

Для настройки параметров журнала ошибок для сообщений на стороне сервера можно использовать параметры `n4u.server.log-levels` и `n4u.server.log-file` в файле конфигурации `/etc/opt/novell/eDirectory/conf/nds.conf`.

Настройка уровня важности

Доступные уровни важности: `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` и `LogDbg` (в порядке от наиболее важного к наименее важному). Дополнительные сведения об уровнях важности см. в Раздел 16.1, "Уровни важности сообщений" на стр. 75.

По умолчанию устанавливается уровень важности `LogFatal`. Таким образом, в журнал будут записываться только сообщения с уровнем важности "неустранимая ошибка".

Чтобы установить уровень важности, используйте параметр `n4u.server.log-levels` в файле `nds.conf`:

`n4u.server.log-levels=`*`уровень важности`*

Например:

- Чтобы установить уровень важности `LogInfo` и выше, введите следующую команду:

  `n4u.server.log-levels=LogInfo`

  При такой конфигурации в журнал будут заноситься события с уровнем важности `LogInfo` и выше (т.е. `LogFatal`, `LogWarn` и `LogErr`).
- Чтобы установить уровень важности `LogWarn` и выше, введите следующую команду:

  `n4u.server.log-levels=LogWarn`

  При такой конфигурации в журнал будут заноситься события с уровнем важности `LogWarn` и выше (`LogFatal`).

Выбор имени файла журнала

Чтобы настроить расположение файла журнала для сообщений, используйте параметр `n4u.server.log-file` в файле `nds.conf`. По умолчанию сообщения сохраняются в файле `ndsd.log`.

Например, чтобы записывать сообщения в файл `/tmp/edir.log`, введите следующее:

`n4u.server.log-file=/tmp/edir.log`

Для записи сообщений в системный журнал используйте параметр `n4u.server.log-file`:

`n4u.server.log-file=syslog`

16.2.2 Windows

- "Настройка уровня важности" на стр. 78
- "Настройка имени файла журнала и пути к нему" на стр. 78
- "Настройка размера файла журнала." на стр. 78

Настройка уровня важности

Доступные уровни важности: `LogFatal`, `LogWarn`, `LogErr`, `LogInfo` и `LogDbg` (в порядке от наиболее важного к наименее важному). Дополнительные сведения об уровнях важности см. в Раздел 16.1, "Уровни важности сообщений" на стр. 75.

Чтобы настроить уровень важности, выполните следующие действия:

1. Нажмите кнопку *Пуск*, выберите *Параметры* > *Панель управления* > *Службы NetIQ eDirectory*
2. На вкладке *Службы* выберите *dhlog.dlm*.
3. Введите уровень журнала в окне *Параметры запуска*.

   Чтобы установить уровень важности `LogErr` и выше, введите следующую команду:

   ```
   LogLevels=LogErr
   ```
4. Щелкните *Настроить*
5. На вкладке *Конфигурация ACS* щелкните "плюс" параметра *DHostLogger*.

   Параметр `LogLevel` обновляется с использованием настроенного значения.

Настройка имени файла журнала и пути к нему

1. Нажмите кнопку *Пуск*, выберите *Параметры* > *Панель управления* > *Службы NetIQ eDirectory*
2. На вкладке *Службы* выберите *dhlog.dlm*.
3. Введите путь к файлу журнала в окне *Параметры запуска* следующим образом:

   ```
   LogFile=file_path
   ```

   Например, чтобы установить путь к файлу журнала `/tmp/Err.log`, введите следующий параметр запуска:

   ```
   LogFile=/tmp/Err.log
   ```
4. Щелкните *Настроить*
5. На вкладке *Конфигурация ACS* щелкните "плюс" параметра *DHostLogger*.

   Параметр `LogFile` обновляется с использованием настроенного значения.

Настройка размера файла журнала.

1. Нажмите кнопку *Пуск*, выберите *Параметры* > *Панель управления* > *Службы NetIQ eDirectory*
2. На вкладке *Службы* выберите *dhlog.dlm*.
3. Введите путь к файлу журнала в окне *Параметры запуска* следующим образом:

   ```
   LogSize=size
   ```

   По умолчанию размер файла составляет 1 МБ.
4. Щелкните *Настроить*
5. На вкладке *Конфигурация ACS* щелкните "плюс" параметра *DHostLogger*.

   Параметр `LogSize` обновляется с использованием настроенного значения.

16.3 Сообщения DSTrace

Можно фильтровать сообщения трассировки по идентификаторам потоков и подключений, а также по уровню важности.

После применения фильтра на экране будут отображаться только те сообщения, которые удовлетворяют условиям фильтра. Все остальные сообщения для включенных тегов будут записаны в журнал `ndstrace.log`, если для файла установлено значение ON.

Одновременно можно применить только один фильтр. Фильтр необходимо указывать для каждого сеанса DSTrace.

По умолчанию устанавливается уровень важности INFO. Это означает, что будут отображаться все сообщения с уровнем важности выше INFO. Можно просмотреть уровень важности, включив тег `svty`.

Для фильтрации сообщений трассировки можно использовать iMonitor. Дополнительные сведения см. в Раздел 16.4, "Фильтрация сообщений iMonitor" на стр. 82.

16.3.1 Linux

Выполните следующую процедуру для фильтрации сообщений трассировки:

1 Для включения фильтрации введите следующую команду:

```
ndstrace tag filter_value
```

Для отключения фильтрации введите следующую команду:

```
ndstrace tag
```

Примеры включения фильтрации:

- Чтобы включить фильтрацию для потока с идентификатором 35, введите следующее:

  ```
  ndstrace thrd 35
  ```

- Для включения фильтрации по уровню важности "неустранимая ошибка" введите следующую команду:

  ```
  ndstrace svty fatal
  ```

  Возможные уровни важности: `FATAL`, `WARN`, `ERR`, `INFO` и `DEBUG`.

- Для включения фильтрации для подключения с ID 21 введите следующую команду:

  ```
  ndstrace conn 21
  ```

Примеры отключения фильтрации:

- Для отключения фильтрации на основе ID потока введите следующую команду:

  ```
  ndstrace thrd
  ```

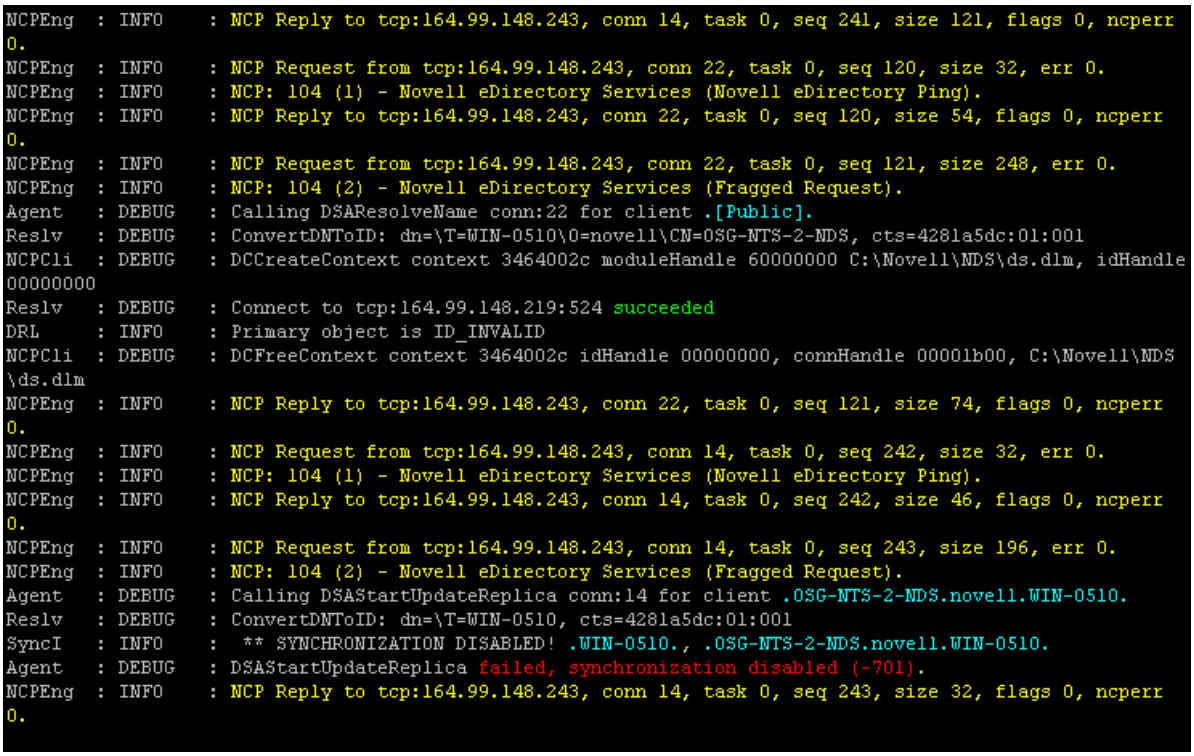
- Для отключения фильтрации на основе ID подключения введите следующую команду:

  ```
  ndstrace conn
  ```

- Для отключения фильтрации на основе важности введите следующую команду:

  ```
  ndstrace svty
  ```

Рисунок 16-1 *Пример окна сообщений трассировки с фильтрами*



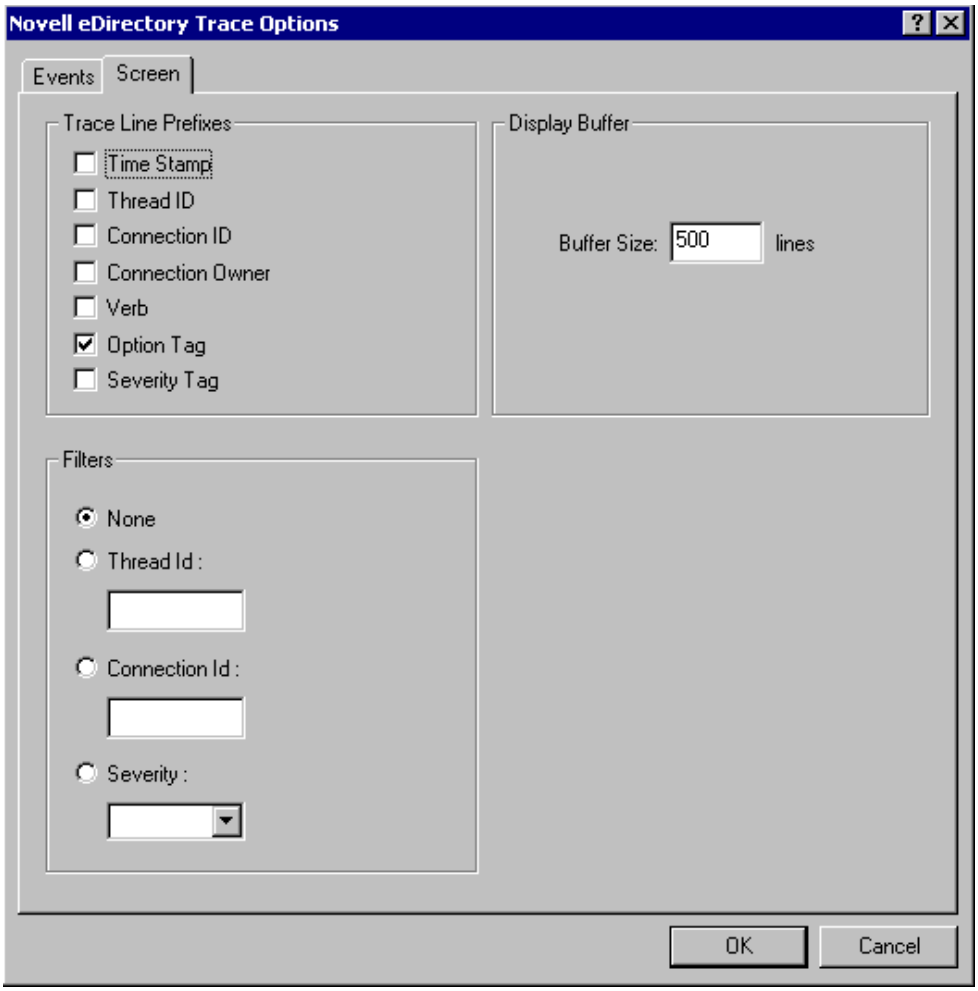
16.3.2 Windows

Выполните следующую процедуру для фильтрации сообщений трассировки:

1. Нажмите кнопку *Пуск*, выберите *Панель управления* > *Службы NetIQ eDirectory*
2. На вкладке *Службы* выберите *dstrace.dlm*.
3. Щелкните *Изменить* > *Параметры* в окне "Трассировка".

   Будет показано диалоговое окно параметров трассировки NetIQ eDirectory.

Рисунок 16-2 *Окно параметров трассировки в Windows*



4 Перейдите на вкладку *Экран*.

5 Выберите параметр фильтрации в группе *Фильтры* и введите значение.

Можно фильтровать сообщения по следующим критериям:

- *ИД* потока
- *ИД* соединения
- Серьезность

Перед выбором какого-либо фильтра убедитесь, что он включен в разделе *Префиксы строк трассировки*.

Также можно отменить фильтрацию, выбрав *Нет* или сняв флажок фильтрации.

ПРИМЕЧАНИЕ. Если выбраны параметры фильтрации *ID потока* или *ID подключения*, но введено несуществующее значения, сообщения не будут отображаться. Тем не менее, все прочие сообщения будут записаны в файл `ndstrace.log`.

16.4 Фильтрация сообщений iMonitor

Можно фильтровать сообщения трассировки iMonitor по идентификаторам потоков и подключений, а также по номерам ошибок.

Для фильтрации по идентификаторам потоков и подключений убедитесь, что соответствующие параметры включены на вкладке "Конфигурация трассировки".

Дополнительные сведения см. во встроенной справке iMonitor.

16.5 Фильтрация сообщений SAL

В SAL можно по требованию заносить в журнал расширенные сведения об ошибках. В отладочных сборках поддерживается трассировка вызовов функций с аргументами.

16.5.1 Настройка уровней важности

Можно использовать параметр `SAL_LogLevels` для настройки уровня важности сообщений SAL. `SAL_LogLevels` — это разделенный запятыми список нужных уровней журнала.

Уровни журнала перечислены в таблице ниже.

Таблица 16-1 *Параметры фильтрации сообщений SAL*

Название параметра	Описание
`LogCrit`	Критические сообщения. Этот уровень включен по умолчанию. После записи в журнал критической ошибки система отключается.
`LogErr`	Все сообщения об ошибках. Система продолжает работать, но с непредсказуемыми результатами.
`LogWarn`	Предупреждения. Это предупреждение о возможном возникновении ошибки.
`LogInfo`	Информационные сообщения.
`LogDbg`	Сообщения отладки, используемые при разработке. Эти сообщения исключаются из готовых сборок для сокращения размера двоичных файлов.
`LogCall`	Отслеживает вызовы функций. Это подмножество сообщений отладки.
`LogAll`	Включает все сообщения, кроме `LogCall`.

Если указать "-" перед определенным уровнем журнала, этот уровень будет отключен.

Примеры

Для фильтрации по всем уровням журнала, кроме `LogInfo` и `LogDbg`, выполните следующие действия:

Linux

1. Остановите `ndsd`.
2. Введите следующую команду:

   ```
   export SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

3. Запустите `ndsd`.

Windows

1. Завершите работу `DHost`.
2. Введите следующую команду в командной строке:

   ```
   set SAL_LogLevels=LogAll,-LogInfo,-LogDbg
   ```

   ```
   c:\novell\nds>dhost.exe /datadir=c:\novell\nds\DIBFiles\
   ```

3. Перезапустите `DHost`.

16.5.2 Настройка пути к файлу журнала

Можно использовать переменную среды `SAL_LogFile`, чтобы настроить расположение файла журнала. Это может быть допустимое имя файла с путем или одно из следующих значений.

- Консоль: все сообщения выводятся на консоль.
- Syslog: в Linux сообщения передаются в syslog. В Windows сообщения заносятся в файл syslog. Так ведение журналов работает по умолчанию.

  Все критические ошибки всегда записываются в syslog, если такой механизм не отключить явным образом.

17 Offline Bulkload Utility: ldif2dib

ldif2dib — это новая программа в составе NetIQ eDirectory 8.8 для массовой загрузки данных из LDIF-файлов в базу данных eDirectory. Это автономная программа, поэтому она выполняет массовую обработку быстрее, чем интерактивные программы.

В следующей таблице перечислены платформы, поддерживающие ldif2dib:

Возможность	Linux	Windows
ldif2dib	✓	✓

17.1 Необходимость использования ldif2dib

Программа ldif2dib необходима при наполнении большой базы данных пользователей записями из LDIF-файла. В этом отношении интерактивные программы, такие как ice или ldapmodify, работают медленнее, чем ldif2dib, из-за издержек, связанных с интерактивной массовой обработкой, таких как проверка схемы, преобразование протоколов и проверка доступа. ldif2dib поддерживает долгосрочную бесперебойную работу, когда необходимо наполнить крупную базу данных пользователей, и когда первоначальное время простоя не имеет значения.

17.2 Получение дополнительной информации

Для получения дополнительных сведений об этой программе см. раздел "Программа для обработки автономной массовой нагрузки" в *руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

18 Резервное копирование eDirectory с SMS

Novell Storage Management Services (SMS) — это платформа API, на основе которой работают решения для резервного копирования. Платформа SMS реализована на основе двух основных компонентов:

- Storage Management Data Requester (SMDR)
- Агент обслуживания цели (TSA)

TSA для eDirectory (`tsands`) обслуживает целевые объекты eDirectory и реализует API Novell Storage Management Services API для всех деревьев каталога. На основе `API SMS` можно создавать полнофункциональные приложения для резервного копирования.

В Linux поддерживается TSA для NDS.

19 Аудит LDAP

Аудит — одна из основных функций, необходимых администраторам при анализе каталогов. Механизм событий eDirectory поддерживает аудит eDirectory. Поскольку приложения широко используют протокол LDAP для доступа к каталогам, повсеместно требуется аудит операций LDAP.

Эта глава содержит следующие разделы:

19.1 Необходимость аудита LDAP

Такой механизм событий отсутствовал в существующем LDAP-сервере eDirectory, поэтому не было возможности получить информацию LDAP в достаточном объеме. Система событий NDS создавала события для всех действий eDirectory, но этой информации обычно было недостаточно приложениям, проводящим аудит LDAP-сервера, или информация была бесполезной для аудита. Информация, включающая протоколы и привязки, сетевые адреса, методы и типы проверки подлинности, сведения о поиске и транзакциях LDAP и т. д., то есть необходимая для аудита LDAP-серверов, была недоступна в события NDS. Разработчики приложений столкнулись с трудностью записи в приложения аудита LDAP на основе этих событий

LDAP является важным интерфейсом eDirectory, поэтому для предоставления приложениям механизма аудита LDAP-сервера eDirectory в NetIQ eDirectory 8.8 SP3 была реализована новая подсистема событий LDAP. Эта подсистема создает события LDAP со всей информацией, необходимой приложениям для аудита LDAP-сервера. Это называется аудитом LDAP.

19.2 Использование аудита LDAP

Аудит LDAP позволяет приложениям отслеживать операции LDAP, такие как добавление, изменение, поиск и т.п., и получает полезную информацию с сервера LDAP, в том числе информацию о подключении, IP-адрес клиента, к которому был подключен сервер в момент выполнения операции LDAP, идентификатор сообщения, код результата операции и т. д.

Аудит LDAP осуществляется с помощью NDK LDAP Libraries for C (http://developer.novell.com/documentation/cldap/ldaplibc/data/hevgtl7k.html) путем предоставления клиентского интерфейса посредством новых структур и событий LDAP.

19.3 Получение дополнительной информации

Дополнительные сведения о событиях аудита LDAP см. в следующих документах:

- "Настройка служб LDAP для NetIQ eDirectory"в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.
- NDK: LDAP Tools (http://developer.novell.com/documentation/cldap/ltoolenu/data/hevgtl7k.html) в документации LDAP Libraries for C.

Дополнительные сведения об инструментах LDAP документации по LDAP Libraries for C (http://developer.novell.com/ndk/doc/cldap/index.html?ldaplibc/data/a6eup29.html).

20 Аудит с помощью XDASv2

Спецификация XDASv2 обеспечивает стандартизированную классификацию событий аудита. Она определяет набор общих событий на уровне глобальной распределенной системы. XDASv2 предоставляет общий портативный формат записей аудита, который позволяет упростить объединение и анализ информации аудита из нескольких компонентов на уровне распределенной системы. События XDASv2 помещаются в иерархическую систему уведомлений, помогающую расширить стандартный или существующий набор идентификаторов событий.

Если в eDirectory 8.8 SP8 агент XDASv2 не может обмениваться данными с сервером syslog, можно настроить агент для локального кэширования событий аудита, что помогает избежать утраты данных аудита. После этого агент пытается снова отправить сохраненные события аудита; попытки продолжаются до восстановления подключения. Кэширование событий XDAS отключено по умолчанию.

Дополнительные сведения см. в *Руководстве по администрированию NetIQ XDASv2*.

21 Разное

В этой главе рассматриваются различные новые возможности NetIQ eDirectory 8.8.

21.1 Отчеты о дампах кэша iMonitor

На странице "Кэш изменений" iMonitor одновременно отображается только один объект, что затрудняет просмотр всего кэша. В eDirectory 8.8 SP8 к отчетам по умолчанию, входящим в iMonitor, добавлен новый отчет дампа изменений кэша. С помощью этого отчета можно просмотреть сразу все изменения кэша. Этот отчет помогает администраторам лучше понимать изменения на определенном сервере.

При запуска отчета дампа изменений кэша iMonitor также создает полный XML-дамп всех объектов кэша вместе с атрибутами и значениями, которые должны быть синхронизированы между серверами.

Дополнительные сведения об отчетах iMonitor см. в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.

21.2 Синтаксис крупных целочисленных значений Microsoft в iManager

В eDirectory 8.8 SP8 включен новый синтаксис для поддержки синтаксиса Microsoft для значений типа "длинное целое". Этот синтаксис можно использовать для хранения больших целочисленных значений и дат до 1970 года или после 2038 года. Для создания и управления атрибутами с таким синтаксисом можно использовать LDAP или iManager.

ПРИМЕЧАНИЕ. В eDirectory по-прежнему используется существующий синтаксис и 32-разрядные значения для внутренних отметок времени.

21.3 Кэширование объектов безопасности

Контейнер безопасности создается в корневом разделе при установке первого сервера в дереве. Этот контейнер содержит глобальные данные, политики безопасности и ключи.

После появления универсального пароля при входе пользователя в eDirectory посредством NMAS подсистема NMAS получала доступ к информации в контейнере безопасности для проверки подлинности. Если раздел с контейнером безопасности отсутствовал в локальной системе, то подсистема NMAS осуществляла доступ к серверу с этим разделом. Это отрицательно влияет на производительность проверки подлинности NMAS. Эта ситуация была еще более серьезной в случаях, когда доступ к серверу, содержащему раздел с контейнером безопасности, осуществлялся по глобальной сети.

Для устранения этой проблемы в eDirectory 8.8 данные контейнера безопасности кэшируются на локальном сервере. Поэтому для NMAS не требуется получать доступ к контейнеру безопасности, расположенному на другом компьютере, при каждом входе пользователя в систему: контейнер доступен на локальном компьютере. При этом повышается производительность. Добавление раздела с контейнером безопасности на локальный сервер повышает производительность, но может быть неосуществимо в сценариях с множеством серверов.

При изменении данных в контейнере безопасности на сервере, содержащем раздел контейнера безопасности, локальный кэш обновляется фоновым процессом, который называется фоновым компоновщиком. По умолчанию фоновый компоновщик запускается через каждые 13 часов и получает измененные данные с удаленного сервера. Если требуется немедленная синхронизация данных, можно запланировать запуск фонового компоновщика на локальном сервере с помощью iMonitor, ndstrace (в Linux) или ndscons (в Windows). Дополнительные сведения см. во встроенной справке iMonitor или на странице man page команды ndstrace.

Кэширование объектов безопасности включено по умолчанию. Чтобы отключить кэширование всех данных, удалите `CachedAttrsOnExtRef` из объекта сервера NCP.

21.4 Повышение производительности поиска в поддеревьях

Производительность поиска в поддеревьях eDirectory для крупного дерева с высокой степенью вложенности остается неизменной независимо от базового DN поиска. Эта проблема решена с помощью атрибута `AncestorID`. Атрибут `AncestorID` представляет собой список идентификаторов всех предков, связанных с каждой записью. Атрибут `AncestorID` используется при поиске в поддеревьях и ограничивает область поиска.

Этот атрибут заполняется при добавлении записи и после обновления всех записей в DIB. Повторное заполнение всех записей поддерева осуществляется после перемещения поддерева. Тем не менее, поиск по поддеревьям не будет использовать атрибут `AncestorID` при наполнении атрибута после обновления и перемещения поддерева. Поэтому производительность поиска в поддеревьях остается такой же, как в более ранних по сравнению с eDirectory 8.8 версиях.

Чтобы проверить обновление `AncestorIDs` после обновления данных:

После наполнения `AncestorIDs` версия обновления объекта NDS изменяется на 6 или более позднюю. Для просмотра можно использовать iMonitor в разделе *История DIB* информации об агенте.

Чтобы проверить обновление `AncestorIDs` после операции перемещения поддерева:

При заполнении AncestorIDs атрибут UpdateInProgress в объекте Псевдосервер содержит список идентификаторов корневого раздела поддерева. После наполнения AncestorIDs атрибут не будет отображаться в разделе Псевдосервер.

DSRepair обновляет атрибут AncestorID, если он недопустим.

21.5 Изменения localhost

Серверы eDirectory 8.8 не прослушивают адрес замыкания на себя. Программы, использующие localhost, необходимо перенастроить на использование имен серверов или преобразования IP-адресов.

Если какая-либо утилита независимого производителя определяет адреса через localhost, ее необходимо изменить, чтобы определять адреса через имя хоста или IP-адрес, а не через адрес localhost.

21.6 Обработчик 256 файлов в Solaris

Ранее в Solaris 2.*x* stdio реализация потоков могла использовать не более 256 дескрипторов файлов. Это было недостаточно для правильной работы eDirectory. В eDirectory 8.8 для устранения этого ограничения предоставлена библиотека-заглушка.

21.7 Диспетчер памяти в Solaris

В прежних версиях eDirectory на базе Solaris использовался сторонний диспетчер памяти Geodesic*. В этой версии eDirectory 8.8 не включает сторонние средства выделения памяти, а использует встроенный диспетчер памяти.

Это не влияет на производительность eDirectory. В большинстве случаев производительность повысилась или не изменилась по сравнению со сторонними средствами выделения памяти.

21.8 Вложенные группы

eDirectory 8.8 SP2 поддерживает группировку групп, то есть обеспечивается более структурированный подход к группировке. Эта функция называется вложенными группами. В настоящее время вложенность поддерживается для статических групп.

Поддерживается до 200 уровней вложенности.

Дополнительные сведения о вложенных группах см. в *Руководстве по администрированию NetIQ eDirectory 8.8 SP8*.