NetIQ® eDirectory™ 8.8 SP8

Руководство по поиску и устранению проблем

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

В документе *Руководство по поиску и устранению проблем* описано разрешение проблем с продуктом NetIQ eDirectory (eDirectory).

Последнюю версию документа *Руководство по поиску и устранению проблем NetIQ eDirectory 8.8 SP8* см. на веб-сайте интерактивной документации NetIQ eDirectory 8.8.

Целевая 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

Приведено описание управления и конфигурации eDirectory.

Руководство по новым функциям

Описаны новые функции eDirectory.

Руководства по настройке для 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.

Информацию об утилите управления eDirectory см. в документе *Руководство по администрированию NetIQ iManager 2.7*.

O 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. Дополнительную информацию см. на веб-сайтеhttp://community.netiq.com.

1 Определение кодов ошибок

Полный список и описание кодов ошибок eDirectory см. на веб-странице кодов ошибок NetIQ (http://www.novell.com/documentation/nwec/).

2 Установка и конфигурация

2.1 Установка

В этом разделе описаны различные проблемы, которые могут возникнуть при установке eDirectory 8.8, а также советы по поиску и устранению проблем.

2.1.1 При установке второго сервера eDirectory в дерево на компьютере SLES 11 происходит неустранимая ошибка в синхронизации схемы.

Сконфигурируйте дерево eDirectory и установите другой сервер в дерево. В обоих случаях выберите вариант с использованием всех доступных интерфейсов. Для обоих серверов используйте одинаковые интерфейсы. Например, 127.0.0.2. Запустите DSTrace на первом сервере с параметрами SCMA, SKLK и SYNC.

2.1.2 Не удалось выполнить установку

- В каталоге `/var/adm/messages` проверьте наличие следующего сообщения об ошибке:

  `Unable to bind to SLP Multicast Address. Multicast route not added?`

  Это сообщение отображается, если на компьютерах Linux или Solaris не настроен адрес маршрута многоадресной передачи.

  Добавьте групповой адрес маршрутизации и перезапустите демон slpuasa.

- Если в процессе установки появляется сообщение об ошибке `-632: Error description System failure`, выйдите из процесса установки.

  В файле `/etc/opt/novell/eDirectory/conf/nds.conf` увеличьте значение параметра `n4u.base.slp.max-wait`, например, до 50, и перезапустите процесс установки.

- Если при установке выводится сообщение об ошибке , выполните указанные ниже действия.

1. Проверьте, чтобы на хосте Solaris, на который устанавливается данный продукт, была включена многоадресная маршрутизация.
2. Укажите адрес IP главного сервера раздела дерева.

2.1.3 Установка занимает много времени

Если установка eDirectory в существующее дерево занимает много времени, проверьте экран DSTrace на сервере. При появлении сообщения `-625 Transport failure` необходимо перезапустить кэш адресов.

Для сброса кэша адресов выполните в консоли системы следующую команду:

```
set dstrace = *A
```

2.1.4 Администраторам контейнера не удается выполнить установку eDirectory

Программа установки eDirectory 8.8 поддерживает установку администраторами, которые имеют права супервизора на контейнер, в котором располагается сервер. Для этого первый сервер, на котором установлен продукт eDirectory 8.8, должен иметь права супервизора на [Root] для расширения схемы. В силу этого последующие серверы могут не иметь прав в отношении к [Root]. Однако в зависимости от платформы, на которую установлен продукт eDirectory 8.8, возможно, что для расширения всей схемы потребуются права супервизора на [Root] для последующих установок сервера на другие платформы.

Если планируется установить eDirectory 8.8 на нескольких платформах, убедитесь в наличии прав супервизора на [Root] для первого сервера, с которого eDirectory будет устанавливаться на ВСЕ остальные платформы. Например, если первый сервер, на котором планируется установить eDirectory 8.8, находится под управлением Linux, а eDirectory 8.8 планируется установить также и на Solaris, то первый сервер каждой из платформ должен иметь права супервизора на [Root]. Для всех последующих серверов каждой из платформ будет достаточно наличия прав администратора контейнера на тот контейнер, в котором выполняется установка сервера.

Дополнительную информацию см. в решенииNOVL83874 (http://support.novell.com/docs/Tids/Solutions/10073723.html), которое описано в документе *eDirectory 8.7.x Readme Addendum (Дополнение к файлу Readme eDirectory 8.7.x)*.

2.1.5 Не удалось выполнить установку - 1497

Предупреждение о сбое инициализации NetIQ International Cryptographic Infrastructure (NICI) свидетельствует о проблемах с файлом `NFK`. Убедитесь в том, что файл `NFK` правильный. Эта проблема может не возникать на платформах Linux, поскольку по умолчанию файл `NFK` является частью пакета NICI.

2.1.6 Наименование объектов

При использовании специальных символов при наименовании объектов появляется сообщение об ошибке `-671 No Such Parent`. При именовании объектов не используйте никаких специальных символов из указанных ниже:

\ /, * ? .

2.1.7 NICI не устанавливается в режиме сервера в Windows

В диалоговом окне «Свойства» файла `NICIFK` есть вкладка, которая называется «Безопасность». Это проблема происходит при отсутствии имен в поле группы или имен пользователей.

Чтобы обойти эту проблему, выполните описанные ниже действия.

1. Удалите файл `NICIFK`.

   Он располагается в каталоге `C:/Windows/system32/novell/nici`, если корневой каталог системы — `C:/Windows/system32`. Если корневой каталог системы — `F:/Windows/system32`, тогда этот файл находится в каталоге `F:/Windows/system32/novell/nici`.
2. Установите eDirectory.

2.1.8 При обновлении Tarball возвращается сообщение об ошибке «Cannot open or remove a file containing a running program (Невозможно открыть или удалить файл, содержащий запущенную программу)»

Если при выполнении обновления Tarball в AIX на этапе копирования файлов возвращается сообщение об ошибке `Cannot open or remove a file containing a running program (Невозможно открыть или удалить файл, содержащий запущенную программу)`, выполните указанные ниже действия для разрешения данной проблемы.

1. Запустите `/usr/sbin/slibclean` от имени пользователя root.
2. Продолжите обновление с этапа копирования файлов.

2.1.9 Проблема с eDirectory и YUM

Если eDirectory 8.8 с пакетом обновления 6 (SP6) или более поздней версии установлена на сервер Red Hat Enterprise Linux с менеджером пакетов YUM. то при использовании YUM может возникнуть проблема.

YUM и eDirectory 8.8 используют одну библиотеку `libexpat.so.0`, поэтому при запуске YUM с одном или несколькими параметрами на консоль возвращается ошибка. Чтобы устранить эту ошибку, воспользуйтесь текстовым редактором и закомментируйте следующую строку в файле `/etc/ld.so.conf.d/novell-NDSbase.conf`, а затем выполните `ldconfig`:

```
/opt/novell/eDirectory/lib64
```

После комментирования строки и выполнения `ldconfig` в окне терминала при каждом запуске eDirectory необходимо выполнять следующую команду:

```
source /opt/novell/eDirectory/bin/ndspath
```

Перезапустите eDirectory на этом же самом терминале. ndspath определит необходимые зависимости путей.

2.1.10 Проблемы производительности при выполнении eDirectory с BTRFS

Если продукт eDirectory установлен на сервере SLES в файловой системе BTRFS, то при выполнении операций LDAP или использовании NetIQ Import Conversion Export Utility (ICE) могут возникать проблемы с производительностью. Из соображений производительности рекомендуется использовать файловую систему ext3 для сервера eDirectory.

2.2 Конфигурация

В этом разделе описаны проблемы, которые могут произойти при конфигурации eDirectory 8.8.

2.2.1 Сервером каталога возвращаются ссылки на петлевые адреса

Если eDirectory настроен на «прослушивание» петлевых адресов, последние сохраняются и возвращаются клиентам при выполнении операций поиска и других операций. Данные ссылки неприменимы к клиентам, которые пытаются подключится с других компьютеров, а не с данного сервера. Поэтому клиентам не удается подключится, используя эти ссылки на петлевые адреса. Однако другие ссылки, возвращаемые клиентам данным сервером, работают.

Подключение по каждой петлевой ссылке с последующим выбором правильных ссылок может повлиять на производительность клиентов.

Чтобы разрешить эту проблему, выберите только один интерфейс, на котором будет выполняться обмен данным с eDirectory. Не выбирайте петлевые интерфейсы при установке.

2.2.2 Ошибка "Tree Name Lookup Failed: -632" при конфигурации eDirectory 8.8 в Linux

При конфигурации eDirectory 8.8 в Linux, вы можете получить сообщение об ошибке "Tree name lookup failed: -632". Чтобы разрешить эту проблему, выполните указанные ниже действия.

1 После установки пакета SLP запустите его вручную при помощи следующей команды:

```
/etc/init.d/slpuasa start
```

2 После удаления пакета SLP остановите его вручную при помощи следующей команды:

```
/etc/init.d/slpuasa stop
```

2.2.3 Добавление новых серверов

Невозможно добавить новый сервер в контекст, если длина его доменного имени превышает 255 символов. Ограничение по имени относится к полному доменному имени, а не к контексту. Длина полного доменного имени любого объекта не может превышать 255 символов.

2.2.4 Исключение каталога DIB из процессов резервного копирования или проверки на наличие вирусов

После установки eDirectory необходимо настроить среду таким образом, чтобы исключить каталог DIB на вашем сервере eDirectory из любых процессов антивирусов или программного обеспечения резервного копирования. Если не исключить каталог DIB из процессов этого типа, файлы DIB могут быть повреждены или могут иметь место ошибки `-618 FFFFFD96 INCONSISTENT DATABASE`.

Для резервного копирования каталога DIB воспользуйтесь инструментом резервного копирования eDirectory. Дополнительную информацию о резервном копировании см. в разделе "Backing Up and Restoring NetIQ eDirectory (Резервное копирование и восстановление NetIQ eDirectory)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

2.2.5 При выполнении ndsconfig в eDirectory на 32-разрядной платформе RHEL выводится ошибка

При выполнении ndsconfig в eDirectory на 32-разрядной платформе RHEL выводится указанная ниже ошибка.

```
/opt/novell/eDirectory/lib/libsal.so.1.0.0

error while loading shared libraries: /opt/novell/lib/libccs2.so: cannot
restore segment prot after reloc: Permission denied
```

Чтобы разрешить эту проблему, выполните следующие команды.

```
chcon -t textrel_shlib_t '/opt/novell/eDirectory/lib/libsal.so.1.0.0'

chcon -t textrel_shlib_t '/opt/novell/lib/libccs2.so.2.7.6'
```

2.2.6 Сертификат IP AG не создается в 64-разрядной платформе SLES 11

Рассмотрите сценарий, в рамках которого для eDirectory 8.8 SP8 настроены оба формата (IPv4 и IPv6) и только один из них (например, IPv4) имеет запись в файле `/etc/hosts`, а другой интерфейс доступен с удаленного компьютера. При настройке eDirectory на прим данных в обоих форматах IP-адресов, сертификат IP AG создается только для IP-адреса, который указан в файле `/etc/hosts`. В этом примере он создается для IPv4.

2.3 Upgrade

2.3.1 Не удается выполнить обновления, если точкой монтирования задан каталог /var/opt/novell/eDirectory/data

Не удается обновить eDirectory, используя команду `ndsconfig upgrade`, если точкой монтирования задан каталог `/var/opt/novell/eDirectory/data`. Обновление прекращается и выводится следующее сообщение об ошибке:

```
ERROR: Unable to check if the directory "/var/opt/novell/eDirectory/data_upg_bak"
already exists. If the directory exists, delete it and execute `ndsconfig upgrade -
-config-file /etc/nds.conf`to restart the upgrade operation.
```

Данная проблема возникла, поскольку при выполнении обновления каталог `/var/opt/novell/eDirectory/data` переименован в `/var/opt/novell/eDirectory/data_upg_bak`, чтобы не утратить данные клиентов. В этом случае `/var/opt/novell/eDirectory/data` — точка монтирования, которую нельзя изменить.

Чтобы разрешить эту проблему, выполните одно из указанных ниже действий.

- Измените точку монтирования на `/var/opt/novell/eDirectory`.
- Выполните указанные ниже действия.
  1. Создайте каталог `/var/opt/novell/eDirectory/data_upg_bak`.
  2. Переместите файлы из каталога`/var/opt/novell/eDirectory/data` в каталог `/var/opt/novell/eDirectory/data_upg_bak`.

  ЗАМЕЧАНИЕ. Чтобы обновление выполнялось без проблем, оставьте каталог `/var/opt/novell/eDirectory/data` пустым.

2.3.2 Обновление eDirectory после применения исправления не приводит к удалению версии исправления в системе Windows

При обновлении eDirectory после применения исправления, версия исправления не обновляется, однако обновляется базовая версия продукта.

Эта проблема наблюдается и воспроизводится для указанных ниже сценариев обновления:

Таблица 2-1 *Версии eDirectory*

Версия базового продукта	Версия исправления	Обновленная версия
eDirectory 873	87310	eDirectory 88 SP3
eDirectory 873		eDirectory 88 SP3
eDirectory 873		eDirectory 873 SP10
eDirectory 88 SP6	любое исправление	eDirectory 88 SP8

Данная проблема происходит, поскольку программы установки eDirectory и установки исправлений в Windows являются отдельными. Базовый продукт eDirectory устанавливается посредством среды NIS, а исправления, наподобие eDirectory 8.8 SP5 Patch 2, устанавливаются с использованием Nulsoft Installer Script (NSIS). Поскольку программы установки разные, обновляется только базовая версия продукта, а не исправление, установленное посредством NSIS.

Чтобы разрешить эту проблему, при выполнении обновления удалите запись об этом исправлении в реестре (например, eDirectory 8.7.3 SP9/eDirectory 8.7.3 SP10/eDirectory 8.8 SP5 patch 2 и eDirectory 8.8 SP5 patch 3).

2.4 Несколько экземпляров

При обработке нескольких экземпляров eDirectory можно столкнуться с проблемами, которые указаны ниже.

- Раздел 2.4.1, "Если первый экземпляр отключен, HTTP не работает" на стр. 23
- Раздел 2.4.2, "eDirectory не принимает данные на всех настроенных интерфейсах" на стр. 23

2.4.1 Если первый экземпляр отключен, HTTP не работает

Если на платформе Linux eDirectory настроен в аппаратной конфигурации с несколькими сетевыми картами и HTTP привязан к нескольким интерфейсам, то при отключении первого интерфейса HTTP не будет доступен с оставшихся интерфейсов.

Это происходит, потому что оставшиеся интерфейсы перенаправляют запрос на первый интерфейс, однако этот интерфейс отключен.

Чтобы разрешить эту проблему при отключении первого интерфейса, перезапустите eDirectory.

2.4.2 eDirectory не принимает данные на всех настроенных интерфейсах

Проверьте, что все интерфейсы, на которых настроен продукт eDirectory, запущены и подключены.

2.4.3 ndsd возвращается к порту по умолчанию, если указанный интерфейс неправильный

Если при использовании командndsconfig new или ndsmanage для создания второго интерфейса каталога указанный интерфейс будет неправильным, то nds попытается использовать интерфейс по умолчанию. Если указан неправильный интерфейс и порт, отличный от порта по умолчанию (например, 1524), то будет использоваться интерфейс по умолчанию с портом по умолчанию (524).

Если для n4u.server.interfaces указан неправильный интерфейс, то ndsd попытается получить информацию на первом интерфейсе. В этом случае будет использовать номер порта, указанный в n4u.server.tcp-port.

2.4.4 Перестроение каталога .edir

Каталог .edir используется для отслеживания нескольких экземпляров eDirectory. Чтобы вновь создать утраченный или поврежденный файл экземпляра (instances.$uid, где $uid указывает идентификатор пользователя в системе), необходимо создать для него отдельный файл экземпляра.

В этих файлах должен быть указан абсолютный путь к файлам nds.conf всех экземпляров, настроенных пользователем. Например, пользователь с uid 1000 должен создать файл экземпляров /etc/opt/novell/eDirectory/conf/.edir/instances.1000 со следующими записями:

```
/home/user1/instance1/nds.conf
```

```
/home/user1/instance2/nds.conf
```

3 Определение номера версии eDirectory

В следующих разделах указаны способы определения версии продукта eDirectory, который установлен на сервере:

3.1 Windows

- Запустите iMonitor.

  На странице «Сводка агента» щелкните пункт «Известные серверы». После этого в разделе «Серверы, известные базе данных» щелкните «Известные серверы». В столбце «Версия агента» отображается номер внутренней сборки каждого сервера. Например, номером версии агента для eDirectory 8.7.1 может быть 10510.64.

  Информацию о выполнении iMonitor см. в разделе "Accessing iMonitor (Доступ к iMonitor)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

- Запустите файл `NDSCons.exe`.

  На панели управления Windows дважды щелкните «NetIQ eDirectory Services (Сервисы NetIQ eDirectory)». В столбце «Сервис» выберите файл ds.dlm, затем нажмите кнопку «Настроить». На вкладках «Агент» отображается как маркетинговая строка (например, NetIQ eDirectory 8.8.1), так и номер внутренней сборки (например, 10510.64).

- Запустите утилиту eDirectory.

  Большинство утилит eDirectory в меню справки имеют параметр «О программе», который позволяет вывести номер версии утилиты (например, Merge Graft Utility 10510.35). В основное название некоторых утилит включена версия внутренней сборки (например, DSRepair - Version 10510.37).

  Чтобы загрузить утилиту eDirectory (например, DSMerge или DSRepair), дважды щелкните значок «NetIQ eDirectory Services (Сервисы NetIQ eDirectory)» на панели управления Windows. В столбце «Сервисы» выберите данную утилиту и нажмите кнопку «Запустить».

- Просмотрите свойства файла eDirectory `.dlm`.

  В проводнике Windows правой кнопкой мыши щелкните файл `.dlm`, затем в диалоговом окне «Свойства» выберите вкладку «Версия». Будет показан номер версии утилиты. Для eDirectory расположение файлов `.dlm` по умолчанию — `C:\novell\NDS`.

3.2 Linux

- Запустите ndsstat.

  Утилита ndsstat выводит информацию, относящуюся к серверам eDirectory, например имя дерева eDirectory, полнохарактерное имя сервера и версию eDirectory. В следующем примере eDirectory 8.7.1 — это версия продукта (маркетинговая строка), а 10510.65 — это двоичная версия (номер внутренней сборки).

  ```
  osg-dt-srv17:/>ndsstat
  Tree Name: SNMP-HPUX-RASH
  Server Name: .CN=osg-dt-srv17.O=novell.T=SNMP-HPUX-RASH.
  Binary Version: 10510.65
  Root Most Entry Depth: 0
  Product Version: NDS/Linux - NDS eDirectory v8.8.8 [DS]
  ```

  Информацию о запуске ndsstat см. в разделе "NetIQ eDirectory Linux Commands and Usage (Команды и использование NetIQ eDirectory в Linux)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)* или в файле man page для ndsstat (`ndsstat.1m`).

- Выполните команду `ndsd --version`.

  Информацию о запуске ndsd см. в разделе "NetIQ eDirectory Linux Commands and Usage (Команды и использование NetIQ eDirectory в Linux)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)* или в файле man page для ndsstat (`ndsstat.1m`).

- Запустите iMonitor.

  На странице «Сводка агента» щелкните пункт «Известные серверы». После этого в разделе «Серверы, известные базе данных» щелкните «Известные серверы». В столбце «Версия агента» отображается номер внутренней сборки каждого сервера. Например, номером версии агента для NetIQ eDirectory 8.8.1 может быть 10510.64.

  Информацию о выполнении iMonitor см. в разделе "Accessing iMonitor (Доступ к iMonitor)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

- Выполните команду `rpm -qi NDSserv`.

  Вывод этой команды подобен выводу команды `ndsd --version`.

4 Файлы журналов

В этом разделе приводится информация по указанным ниже файлам журнала.

4.1 modschema.log

В файле `modschema.log` содержатся результаты всех расширений схемы, которые используются при установке сервера eDirectory в существующее дерево. В каждой строке журнала указан добавляемый или изменяемый класс или атрибут, а также статус попытки изменения.

Этот журнал создается или перезаписывается при каждом запуске процесса инсталляции, поэтому в нем отражены результаты только последней попытки. Кроме расширений схемы eDirectory, в этом журнале содержатся результаты любых других расширений схемы (например, LDAP или SAS), используемых при предварительной обработке данных DSINSTALL перед добавлением нового сервера eDirectory.

Этот журнал не создается, если устанавливается автономный сервер или целевой сервер имеет eDirectory 7.0.1 или более поздней версии.

4.2 dsinstall.log

В первой части файла `dsinstall.log` перечислены установленные переменные среды. Во второй части содержатся сообщения о состоянии, документирующие процесс установки eDirectory.

4.3 ndsd.log

Файл `ndsd.log` содержит информацию о сообщениях, относящихся к серверу eDirectory, например сообщения о выключении и запуске сервера, сервисов PKI и LDAP. По умолчанию этот файл расположен в каталоге `/var/opt/novell/eDirectory/log`.

Можно повысить уровень отладки для файла `ndsd.log`, изменив указанную ниже переменную в файле `nds.conf` из файла`/etc/opt/novell/eDirectory/conf/nds.conf` .

```
n4u.server.log-levels=Logxxxx
```

Дополнительную информацию об уровнях протоколирования ndsd см. в разделе "Managing Error Logging in eDirectory 8.8 (Управление протоколированием ошибок в eDirectory 8.8)" документа *NetIQ eDirectory 8.8 SP8 What's New Guide (Руководство по новым функциям NetIQ eDirectory 8.8 SP8)*.

4.4 Процедура указания размера файла журнала в Linux

Чтобы указать размер файла журнала, воспользуйтесь параметром `n4u.server.log-file-size` в файле `nds.conf`. Размер файла не должен превышать 2 ГБ. По умолчанию задан размер 1 МБ. Однако можно задать размер меньше 1 МБ.

Эта настройка не применяется к файлу `ndsd.log`.

Когда размер файла журнала достигнет указанного верхнего предела, программа ведения журнала начнет перезаписывать файл журнала с самого начала.

5 Устранение проблем, связанных с файлами LDIF

Утилита NetIQ Import Conversion Export упрощает процесс импорта файлов LDIF в eDirectory и их экспорта из eDirectory. Дополнительную информацию см. в разделе "NetIQ Import Conversion Export Utility (Утилита NetIQ Import Conversion Export)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

Чтобы импорт LDIF работал без ошибок, необходимо запустить для файла LDIF утилиту NetIQ Import Conversion Export, которая может его прочитать и обработать. В этом подразделе описан формат и синтаксис файлов LDIF и приведены правильные примеры этих файлов.

5.1 Общие сведения о LDIF

LDIF является широко используемым форматом, описывающим информацию Каталога или операции изменения, которые можно выполнить в Каталоге. LDIF - это формат, полностью независимый от формата хранения данных любой конкретной реализации Каталога, он обычно используется для экспорта информации из Каталога и для импорта данных на серверы LDAP.

Как правило, файл LDIF создается без каких-либо сложностей. Это дает возможность использовать для переноса данных из собственного формата в Каталог LDAP такие средства, как awk или perl. Вы также можете разрабатывать процедуры для создания тестовых данных в формате LDIF.

5.1.1 Формат файлов LDIF

NetIQ Import Conversion Export импортирует необходимые отформатированные файлы LDIF 1. Ниже перечислены основные правила для файла LDIF 1.

- В первой строке, не являющейся комментарием, должен быть указан номер версии: 1.
- После строки с версией следует одна или несколько записей.
- Каждая запись состоит из полей, по одному полю на строку.
- Строки отделяются друг от друга либо символом новой строки, либо комбинацией символов новой строки и возврата каретки.
- Записи отделяются друг от друга одной или несколькими пустыми строками.

- Существуют два отличных друг от друга типа записей LDIF: записи содержимого и записи изменения. Файл LDIF может содержать неограниченное количество записей, но они все должны быть одного типа. Нельзя включать записи данных и записи изменения в один файл LDIF.
- Любая запись, начинающаяся символом (#), считается комментарием и игнорируется при выполнении файла LDIF.

5.1.2 Записи данных LDIF

Одна запись данных LDIF представляет содержимое целого элемента. В следующем примере приведен файл LDIF с четырьмя записями данных:

```
 1  version: 1
 2  dn: c=US
 3  objectClass: top
 4  objectClass: country
 5
 6  dn: l=San Francisco, c=US
 7  objectClass: top
 8  objectClass: locality
 9  st: San Francisco
10
11 dn: ou=Artists, l=San Francisco, c=US
12 objectClass: top
13 objectClass: organizationalUnit
14 telephoneNumber: +1 415 555 0000
15
16 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
17 sn: Michaels
18 givenname: Peter
19 objectClass: top
20 objectClass: person
21 objectClass: organizationalPerson
22 objectClass: iNetOrgPerson
23 telephonenumber: +1 415 555 0001
24 mail: Peter.Michaels@aaa.com
25 userpassword: Peter123
26
```

Этот файл LDIF состоит из следующих частей:

Компонент	Описание
Спецификатор версии	Первая запись файла LDIF содержит номер версии. Между двоеточием и номером версии (в данный момент установлен номер, равный 1) допускается любое количество пробелов. Если версия не указана, приложению, обрабатывающему файл LDIF, разрешено использовать версию 0 либо отклонить файл как синтаксически некорректный. Если строка версии отсутствует, то в утилитах NetIQ, которые обрабатывают LDIF, предполагается, что эта версия — 0.

Компонент	Описание
Спецификатор характерного имени	Первая строка каждой записи данных (в приведенном выше примере это строки 2, 6, 11 и 16) определяет DN (характерное имя) элемента, который она представляет. Спецификатор DN должен быть представлен в одной из следующих двух форм: ◆ dn: *характерное_имя_в_защищенном_формате_UTF-8* ◆ dn:: *характерное_имя_закодированное_в_Base64*
Разделители строк	Разделителем строк может быть либо перевод строки, либо комбинация символов перевода строки и возврата каретки. Такой подход решает общую проблему несовместимости текстовых файлов Linux и Solaris, использующими в качестве разделителя строк символ новой строки, и текстовых файлов MS-DOS и Windows, использующими в качестве разделителя строк комбинацию символов новой строки и возврата каретки.
Разделители записей	Для разделения записей используются пустые строки (строки 5, 10, 15 и 26 приведенного выше примера). Каждая запись файла LDIF, включая последнюю, должна заканчиваться пустыми строками (одной или более). Не смотря на то, что в некоторых реализациях работа с файлами LDIF без завершающего разделителя записей не вызывает трудностей, спецификация LDIF требует его наличие.
Спецификатор значения атрибута	Все остальные строки записей данных являются спецификаторами значений. Они могут принимать одну из следующих трех форм: ◆ Описание атрибута: *значение* ◆ Описание атрибута:: *значение_закодированное_в_Base64* ◆ Описание атрибута: < *URL-адрес*

5.1.3 Записи изменений LDIF

Записи изменений LDIF содержат изменения, которые нужно внести в Каталог. Любая из операций изменения LDAP (добавление, удаление, изменение и изменение DN) может быть представлена записью изменения LDIF.

В записях изменения LDIF используется тот же формат спецификаторов характерного имени и атрибута и такие же разделители записей, что и в записях данных LDIF. (См. "Записи данных LDIF" на стр. 30 для получения дополнительной информации.) Присутствие поля `changetype` является отличительной чертой записей изменений LDIF от записей данных LDIF. В поле `changetype` указывается операция, выполняемая записью изменения.

Поле `changetype` может принимать одну из указанных ниже форм.

Форма	Описание
changetype:add	Ключевое слово, указывающее, что запись изменений определяет операцию добавления LDAP.

Форма	Описание
changetype:delete	Ключевое слово, указывающее, что запись изменения выполняет операцию LDAP удаления.
changetype: moddn	Ключевое слово, указывающее, что запись изменения выполняет операцию LDAP изменения DN (в случае, если для процессора LDIF установлена привязка к серверу LDAP в качестве клиента версии 3) или операцию изменения RDN (в случае, если для процессора LDIF установлена привязка к серверу LDAP в качестве клиента версии 2).
changetype: modrdn	Синоним операции moddn.
changetype:modify	Ключевое слово, указывающее, что запись изменения выполняет операцию LDAP изменения.

Ключевое слово Add

Запись изменения добавления похожа на запись изменения содержимого (см. "Записи данных LDIF" на стр. 30) с тем лишь отличием, что поле "changetype: add" добавлено непосредственно перед всеми полями значения атрибута.

Все записи должны быть одного типа. Нельзя использовать записи данных вместе с записями изменения.

```
 1 version: 1
 2 dn: c=US
 3 changetype: add
 4 objectClass: top
 5 objectClass: country
 6
 7 dn: l=San Francisco, c=US
 8 changetype: add
 9 objectClass: top
10 objectClass: locality
11 st: San Francisco
12
14 dn: ou=Artists, l=San Francisco, c=US
15   changetype: add
16 objectClass: top
17 objectClass: organizationalUnit
18 telephoneNumber: +1 415 555 0000
19
20 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
21 changetype: add
22 sn: Michaels
23 givenname: Peter
24 objectClass: top
25 objectClass: person
26 objectClass: organizationalPerson
27 objectClass: iNetOrgPerson
28 telephonenumber: +1 415 555 0001
29 mail: Peter.Michaels@aaa.com
30 userpassword: Peter123
31
```

Ключевое слово Delete

Так как запись изменения "delete" выполняет удаление элемента, для нее требуются только два поля: поле спецификатора характерного имени и поле "changetype" с ключевым словом "delete".

Далее приведен пример файла LDIF, используемого для удаления четырех элементов, созданных с помощью файла LDIF в разделе "Ключевое слово Add" на стр. 32.

ЗАМЕЧАНИЕ. Для удаления элементов, созданных ранее, следует использовать их обратный порядок. В противном случае операция удаления не будет выполнена, поскольку записи контейнера не являются пустыми.

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 changetype: delete
 4
 5 dn: ou=Artists, l=San Francisco, c=US
 8   changetype: delete
 9
10 dn: l=San Francisco, c=US
11 changetype: delete
12
13 dn: c=US
14 changetype: delete
15
```

Ключевое слово Modify

Ключевое слово "modify" позволяет добавлять, удалять и замещать значения атрибутов уже существующего элемента. Изменение может принимать одну из следующих трех форм:

Элемент	Описание
add: attribute type	Ключевое слово, указывающее, что к элементу должны быть добавлены перечисленные спецификаторы значений атрибутов для указанного типа атрибута.
delete: attribute type	Ключевое слово, указывающее, что значения указанного типа атрибута должны быть удалены. Если вслед за полем "delete" указаны спецификаторы значений атрибутов, заданные значения будут удалены. Если вслед за полем "delete" не указаны спецификаторы значений атрибутов, будут удалены все значения. Если у атрибута нет значений, эта операция завершится неудачно, но результат будет достигнут, так как атрибуты, не имеющие значений, удаляются.

Элемент	Описание
replace: attribute type	Ключевое слово, указывающее, что значения указанного типа атрибута должны быть заменены. Любые спецификаторы значений атрибута, указанные вслед за полем "replace", становятся новыми значениями указанного типа атрибута. Если спецификаторы значений атрибутов не указаны, текущий набор значений заменяется пустым набором (что приводит к необходимости удаления атрибута). В отличие от операции удаления, если атрибут не имеет значений, операция изменения пройдет успешно. Результат в обоих случаях будет один и тот же.

Далее приведен пример типа изменения "modify", в котором в элемент "cn=Peter Michaels" добавляется дополнительный телефонный номер.

```
1 version: 1
2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
3 changetype: modify
4 # add the telephone number to cn=Peter Michaels
4 add: telephonenumber
5 telephonenumber: +1 415 555 0002
6
```

Различные операции изменения можно объединять в одном запросе LDAP. Также можно указывать несколько спецификаторов операции "modify" в одной записи LDIF. Строка, состоящая только из символа дефиса (-), используется для отметки конца спецификаций значений атрибутов каждого спецификатора изменения.

Следующий пример файла LDIF иллюстрирует использование нескольких спецификаторов в одной операции изменения:

```
 1 version: 1
 2
 3 # An empty line to demonstrate that one or more
 4 # line separators between the version identifier
 5 # and the first record is legal.
 6
 7 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 8 changetype: modify
 9 # Add an additional telephone number value.
10 add: telephonenumber
11 telephonenumber: +1 415 555 0002
12 -
13 # Delete the entire fascimiletelephonenumber attribute.
14 delete: facsimileTelephoneNumber
15 -
16 # Replace the existing description (if any exists)
17 # with two new values.
18 replace: description
```

```
19 description: guitar player
20 description: solo performer
21 -
22 # Delete a specific value from the telephonenumber
23 # attribute.
24 delete: telephonenumber
25 telephonenumber: +1 415 555 0001
26 -
27 # Replace the existing title attribute with an empty
28 # set of values, thereby causing the title attribute to
29 # be removed.
30 replace: title
31 -
32
```

Ключевое слово ModDN

Ключевое слово "modDN" позволяет переименовывать, перемещать элемент или выполнять обе процедуры сразу. Эта операция состоит из двух обязательных полей и одного необязательного.

Поле	Описание
newrdn (обязательное)	В процессе выполнения этой записи элементу присваивается новое имя. Спецификатор "newDN" должен быть представлен в одной из следующих двух форм: ◆ newrdn: *относительное_характерное_имя_в_защищенном_формате_UTF-8* ◆ newrdn:: *закодированное_относительное_характерное_имя_в_формате_Base64* Спецификатор "newRDN" требуется во всех записях LDIF с ключевым словом ModDN.
deleteoldrdn (обязательное)	Спецификатор "delete old RDN" является флагом, указывающим, нужно ли заменять старое значение RDN (относительное характерное имя) новым или нужно его сохранить. Он может принимать одну из двух форм: ◆ deleteoldrdn: 0 Означает, что старое значение RDN должно быть сохранено после переименования. ◆ deleteoldrdn: 1 Означает, что старое значение RDN должно быть удалено после переименования элемента.

Поле	Описание
newsuperior (необязательное)	Спецификатор "newsuperior" указывает имя нового родительского объекта, который будет назначен элементу в процессе выполнения записи изменения характерного имени (ключевое слово moddn). Спецификатор "newsuperior" должен быть представлен в одной из следующих двух форм: ◆ newsuperior: *характерное_имя_в_защищенном_формате_UTF-8* ◆ newsuperior:: *закодированное_характерное_имя_в_формате_Base64* Спецификатор "newsuperior" не обязательно использовать в записях LDIF с процедурой изменения характерного имени. Он предоставляется только в тех случаях, когда элемент нужно перенести из одного родительского объекта в другой.

Далее приведен пример типа изменения "Modify DN", в котором показано, как переименовывать элемент:

```
 1 version: 1
 2
 3 # Rename ou=Artists to ou=West Coast Artists, and leave
 4 # its old RDN value.
 5 dn: ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: ou=West Coast Artists
 8 deleteoldrdn: 1
 9
```

Далее приведен пример типа изменения "Modify DN", в котором показано, как переместить элемент:

```
 1 version: 1
 2
 3 # Move cn=Peter Michaels from
 4 # ou=Artists,l=San Francisco,c=US to
 5 # ou=Promotion,l=New York,c=US and delete the old RDN.
 5 dn: cn=Peter Michaels,ou=Artists,l=San Francisco,c=US
 6 changetype: moddn
 7 newrdn: cn=Peter Michaels
 8 deleteoldrdn: 1
 9 newsuperior: ou=Promotion,l=New York,c=US
10
```

В следующем примере представлен тип изменения "Modify DN" и показано, как перенести и переименовать элемент одновременно:

```
 1 version: 1
 2
 3 # Move ou=Promotion from l=New York,c=US to
 4 # l=San Francisco,c=US and rename it to
 5 # ou=National Promotion.
 5 dn: ou=Promotion,l=New York,c=US
 6 changetype: moddn
 7 newrdn: ou=National Promotion
 8 deleteoldrdn: 1
 9 newsuperior: l=San Francisco,c=US
10
```

ЗАМЕЧАНИЕ. Операция изменения RDN протокола LDAP версии 2 не поддерживает перемещение элементов. При попытке переноса элемента с помощью синтаксиса `newsuperior` LDIF с клиентом LDAP версии 2 произойдет сбой.

5.1.4 Перенос строк в файлах LDIF

Чтобы перенести строку в файле LDIF, достаточно просто вставить разделитель строк (символ новой строки или комбинацию символов перевода каретки и новой строки) и вслед за ним пробел в том месте, где нужно перенести строку. Когда анализатор LDIF обнаруживает пробел в начале строки, он объединяет данные этой строки с данными предыдущей. Пробел в начале отбрасывается.

Не следует разрывать строки в середине символа UTF-8, состоящего из нескольких байт.

Ниже приведен пример файла LDIF с перенесенной (разорванной) строкой (см. строки 13 и 14):

```
 1 version: 1
 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US
 3 sn: Michaels
 4 givenname: Peter
 5 objectClass: top
 6 objectClass: person
 7 objectClass: organizationalPerson
 8 objectClass: iNetOrgPerson
 9 telephonenumber: +1 415 555 0001
10 mail: Peter.Michaels@aaa.com
11 userpassword: Peter123
12 description: Peter is one of the most popular music
13  ians recording on our label. He's a big concert dr
14  aw, and his fans adore him.
15
```

5.1.5 Представление хэшированного пароля в файлах LDIF

Хэшированный пароль представлен как данные base64 в файле LDIF. После имени атрибута `userpassword` необходимо указать имя шифрования, используемого для хэширования пароля. Это имя должно быть заключено в фигурные скобки "{ }", как показано ниже.

Пример 1

Для паролей, хэшированных SHA:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SHA}xcbdh46ngh37jsd0naSFDedjAS30dm5 objectclass:
inetOrgPerson
```

Пример 2

Для паролей, хэшированных SSHA:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {SSHA}sGs948DFGkakdfkasdDF34DF4dS3skl5DFS5 objectclass:
inetOrgPerson
```

Пример 3

Для паролей, хэшированных Digest MD5:

```
1 version: 1 2 dn: cn=Peter Michaels, ou=Artists, l=San Francisco, c=US 3 sn:
Michaels 4 userpassword: {MD5}a45lkSDF234SDFG62dsfsf2DG2QEvgdmnk4305 objectclass:
inetOrgPerson
```

5.2 Отладка файлов LDIF

При возникновении проблем с файлом LDIF обратитесь к следующим подпунктам:

5.2.1 Разрешение опережающих ссылок

Иногда могут случайно встретиться файлы LDIF, в которых запись, добавляющая элемент, указана раньше записи, добавляющей его родительский объект. В этом случае возникает ошибка, так как при попытке сервера LDAP добавить элемент его родительский объект еще не существует.

Чтобы решить эту проблему, нужно всего лишь разрешить использование опережающих ссылок. Если использование опережающих ссылок включено, при добавлении элемента, для его родительского объекта, который еще не существует, создается метка-заполнитель, и добавление этого элемента происходит успешно. Если в дальнейшем создается родительский элемент, то опережающая ссылка заменяется на обычный элемент.

Также возможно, чтобы одна или несколько опережающих ссылок были сохранены после завершения импорта LDIF (например, если в файле LDIF никогда не будет создан родительский объект элемента). В этом случае, в ConsoleOne и iManager опережающая ссылка будет отображена как неизвестный объект. Не смотря на то, что можно осуществлять поиск опережающей ссылки, Вы не сможете прочитать ее атрибуты (кроме "objectClass"), так она не имеет ни атрибутов, ни их значений. Однако все операции LDAP будут выполняться нормально с объектами, расположенными ниже опережающей ссылки.

Идентификация элементов опережающих ссылок

Элементы опережающих ссылок принадлежат классу объектов "Unknown" (Неизвестный), а также в них установлен внутренний флаг NDS EF_REFERENCE. В ConsoleOne и iManager неизвестные элементы отмечены круглым желтым значком со знаком вопроса в центре. Для поиска неизвестных объектов можно использовать LDAP, однако для определения, является ли элемент опережающей ссылкой, доступ к параметрам флагов элементов с помощью LDAP в настоящее время невозможен.

Изменение опережающих ссылок на нормальные объекты

Вы можете изменить опережающую ссылку на нормальный объект путем его создания (например, с помощью файла LDIF или запроса клиента LDAP). При создании в eDirectory элемента, уже существующего в виде опережающей ссылки, eDirectory преобразует эту существующую ссылку в создаваемый объект.

Использование мастера NetIQ eDirectory Import Convert Export

Для включения опережающих ссылок в процессе импорта LDIF выполните следующие действия:

1. В NetIQ iManager нажмите кнопку *Функции и задачи*  .
2. Последовательно выберите пункты *Обслуживание eDirectory* > *Мастер импорта, преобразования и экспорта*.
3. Щелкните пункт *Import Data (Импорт данных)* в области *File on Disk (Файл на диске)*, затем нажмите кнопку *Далее*.
4. Выберите *LDIF* в качестве типа файла для выбора.
5. Укажите имя файла, содержащего данные для импорта, соответствующие параметры и нажмите кнопку *Далее*.
6. Укажите сервер LDAP, на который будут импортированы данные.
7. Добавьте соответствующие параметры, как указано в следующей таблице:

Параметр	Описание
Имя DNS сервера/IP-адрес	Имя DNS или IP-адрес целевого сервера LDAP
порт	Целое число в качестве номера порта целевого сервера LDAP
Файл DER	Имя файла DER, который содержит ключ сервера, используемый для аутентификации SSL
Способ регистрации	Аутентифицированная регистрация или анонимная регистрация (для элемента, указанного в поле "DN пользователя")
DN пользователя	Характерное имя элемента, который должен использоваться при выполнении привязки к определенной сервером операции привязки
Пароль	Атрибут пароля для элемента, указанного в поле "DN пользователя"

8. В разделе *Дополнительные параметры* щелкните пункт *Разрешить создание опережающих ссылок*.
9. Нажмите кнопку *Далее*, затем — кнопку *Готово*.

Порядок включения опережающих ссылок при миграции сервера данных на сервер данных.

1. В NetIQ iManager нажмите кнопку *Функции и задачи*  .
2. Последовательно выберите пункты *Обслуживание eDirectory* > *Мастер импорта, преобразования и экспорта*.
3. Выберите пункт *Миграция данных с одного сервера на другой* и нажмите кнопку *Далее*.
4. Укажите сервер LDAP, содержащий элементы, миграцию которых необходимо выполнить.
5. Добавьте соответствующие параметры, как указано в следующей таблице:

Параметр	Описание
Имя DNS сервера/IP-адрес	Имя DNS или IP-адрес исходного сервера LDAP
порт	Целое число в качестве номера порта исходного сервера LDAP
Файл DER	Имя файла DER, который содержит ключ сервера, используемый для аутентификации SSL
Способ регистрации	Аутентифицированная регистрация или анонимная регистрация (для элемента, указанного в поле "DN пользователя")
DN пользователя	Характерное имя элемента, который должен использоваться при выполнении привязки к определенной сервером операции привязки
Пароль	Атрибут пароля для элемента, указанного в поле "DN пользователя"

6 В разделе *Дополнительные параметры* щелкните пункт *Разрешить создание опережающих ссылок*.

7 Нажмите кнопку *Далее*.

8 Укажите критерии поиска (описаны ниже) для элементов, миграцию которых необходимо выполнить.

Параметр	Описание
Базовое DN	Базовое характерное имя для запроса поиска Если данное поле оставить пустым, то по умолчанию используется базовое DN "" (пустая строка).
Область	Область запроса на поиск
Фильтр	Фильтр поиска, удовлетворяющий условиям RFC 2254 По умолчанию это `objectclass=*`.
Атрибуты	Атрибуты, которые необходимо возвратить для каждого элемента поиска

9 Нажмите кнопку *Далее*.

10 Укажите сервер LDAP, на который будет выполнена миграция данных.

11 Нажмите кнопку *Далее*, затем — кнопку *Готово*.

ПРИМЕЧАНИЕ. Проверьте однородность схемы по сервисам LDAP.

Использование интерфейса командной строки утилиты NetIQ Import Conversion Export

Чтобы включить опережающие ссылки в интерфейсе командной строке, воспользуйтесь параметром "-F" целевого обработчика LDAP.

Дополнительную информацию см. в разделе "LDIF Destination Handler Options (Параметры целевого обработчика LDIF)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

5.2.2 Проверка синтаксиса файлов LDIF

Синтаксис файла LDIF до выполнения его записей можно проверить с помощью параметра исходного обработчика LDIF "Отобразить операции, но не выполнять".

Исходный обработчик LDIF всегда проверяет синтаксис записей файлов LDIF при их обработке. Эта опция отключает обработку записей и позволяет проверить синтаксис.

Использование мастера NetIQ eDirectory Import Convert Export

1. В NetIQ iManager нажмите кнопку *Функции и задачи*  .
2. Последовательно выберите пункты *Обслуживание eDirectory* > *Мастер импорта, преобразования и экспорта*.
3. Щелкните пункт *Import Data (Импорт данных)* в области *File on Disk (Файл на диске)*, затем нажмите кнопку *Далее*.
4. Выберите *LDIF* в качестве типа файла для выбора.
5. Укажите имя файла, содержащего данные для импорта, и соответствующие параметры.
6. В разделе *Дополнительные параметры* выберите пункт *Отобразить операции, но не выполнять* и нажмите кнопку *Далее*.
7. Укажите сервер LDAP, на который будут импортированы данные.
8. Добавьте соответствующие параметры, как указано в следующей таблице:

Параметр	Описание
Имя DNS сервера/IP-адрес	Имя DNS или IP-адрес целевого сервера LDAP
порт	Целое число в качестве номера порта целевого сервера LDAP
Файл DER	Имя файла DER, который содержит ключ сервера, используемый для аутентификации SSL
Способ регистрации	Аутентифицированная регистрация или анонимная регистрация (для элемента, указанного в поле "DN пользователя")
DN пользователя	Характерное имя элемента, который должен использоваться при выполнении привязки к определенной сервером операции привязки
Пароль	Атрибут пароля для элемента, указанного в поле "DN пользователя"

9 Нажмите кнопку *Далее*, затем — кнопку *Готово*.

Использование интерфейса командной строки утилиты NetIQ Import Conversion Export

Для проверки синтаксиса файла LDIF в командной строке используйте опцию "-n" целевого обработчика LDIF.

Дополнительную информацию см. в разделе "LDIF Destination Handler Options (Параметры исходного обработчика LDIF)" документа NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8).

5.2.3 Использование файла ошибок LDIF

Утилита NetIQ Import Conversion Export автоматически создает файл LDIF, куда вносятся все записи, в которых целевой обработчик обнаружил ошибки. Файл ошибок LDIF, созданный утилитой, можно редактировать, исправлять ошибки, затем повторно выполнить на сервере содержавшие ошибки операции для завершения импорта или миграции данных.

Использование мастера NetIQ eDirectory Import/Export

Эта функция доступна только в ConsoleOne.

1 В ConsoleOne последовательно выберите пункты *Мастер* > *NDS Import/Export (Импорт/экспорт NDS)*.

2 Выберите задачу, которую Вы хотите выполнить.

3 Щелкните *Расширенный*.

4 В поле *Файл журнала* укажите имя файла, в котором будут регистрироваться исходящие сообщения (включая сообщения об ошибках).

5 В поле *Определение файла вывода LDIF для ошибочных записей* укажите имя файла, в который будут вноситься вызвавшие ошибку элементы в формате LDIF.

Этот файл можно использовать для обнаружения и исправления ошибок. Исправленную версию этого файла можно также повторно применить к Каталогу.

6 Нажмите кнопку *Закрыть*.

7 Следуйте инструкциям интерактивной справки для завершения выбранной задачи.

Использование интерфейса командной строки утилиты NetIQ Import Conversion Export

Для конфигурации опций журнала ошибок в утилите командной строки, воспользуйтесь общим параметром `-l`.

Дополнительную информацию см. в разделе "General Options (Общие параметры)" документа NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8).

5.2.4 Использование флагов отладки LDAP SDK

Для того, чтобы понять некоторые трудности, связанные с LDIF, нужно понять то, как работает клиент SDK LDAP. Для исходного, целевого или обоих обработчиков можно установить следующие опции:

Значение	Описание
0x0001	Трассировка вызовов функций LDAP.
0x0002	Печать информации о пакетах.
0x0004	Печать информации об аргументах.
0x0008	Печать информации о соединениях.
0x0010	Печать информации кодирования и декодирования BER.
0x0020	Печать информации фильтра поиска.
0x0040	Печать информации о конфигурации.
0x0080	Печать информации ACL.
0x0100	Печать статистической информации.
0x0200	Печать дополнительной статистической информации.
0x0400	Печать информации оболочки.
0x0800	Печать информации синтаксического анализа.
0xFFFF (десятичное -1)	Включение опций отладки.

Чтобы включить эти функции, воспользуйтесь параметром `-e` для целевого и исходного обработчиков LDAP. Целое значение, указанное для параметра `-e`, представляет собой маску битов, включающую использование различных типов отладочной информации в LDAP SDK.

Дополнительную информацию см. в разделах "LDAP Source Handler Options (Параметры исходного обработчика LDAP)" и "LDAP Destination Handler Options (Параметры целевого обработчика LDAP)" руководства *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

5.3 Использование LDIF для расширения Схемы

Так как LDIF может выполнять операции LDAP по обновлению, LDIF можно использовать для изменения Схемы.

5.3.1 Добавление нового класса объектов

Чтобы добавить класс, просто добавьте значение атрибута, соответствующее спецификации для `NDSObjectClassDescription` атрибута `objectClasses` объекта `subschemaSubentry`.

```
NDSObjectClassDescription = "(" whsp
   numericoid whsp
   [ "NAME" qdescrs ]
   [ "DESC" qdstring ]
   [ "OBSOLETE" whsp ]
   [ "SUP" oids ]
   [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
   [ "MUST" oids ]
   [ "MAY" oids ]
   [ "X-NDS_NOT_CONTAINER" qdstrings ]
   [ "X-NDS_NONREMOVABLE" qdstrings ]
   [ "X-NDS_CONTAINMENT" qdstrings ]
   [ "X-NDS_NAMING" qdstrings ]
   [ "X-NDS_NAME" qdstrings ]
   whsp ")"
```

В следующем примере файла LDIF в схему добавляется класс объекта `person`:

```
 1 version: 1
 2 dn: cn=schema
 3 changetype: add
 4 objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard
 5   ObjectClass' SUP ndsLoginProperties STRUCTURAL MUST
 6   (cn $ sn) MAY (description $ seeAlso $ telephoneNum
 7  ber $ fullName $ givenName $ initials $ uid $ userPa
 8  ssword) X-NDS_NAMING ('cn' 'uid') X-NDS_CONTAINMENT
 9  ('organization' 'organizationalUnit' 'domain') X-NDS
10  _NAME 'Person' X-NDS_NOT_CONTAINER '1' X-NDS_NONREMO
11  VABLE '1')
12
```

Обязательные атрибуты

Обязательные атрибуты перечислены в разделе `MUST` описания класса объекта. Для класса объектов "person" обязательными атрибутами являются `cn` и `sn`.

Необязательные атрибуты

Необязательные атрибуты перечислены в разделе `MAY` описания класса объекта. Необязательными атрибутами в классе объекта `person` являются `description`, `seeAlso`, `telephoneNumber`, `fullName`, `givenName`, `initials`, `uid` и `userPassword`.

ПРИМЕЧАНИЕ. Атрибут `userPassword` невозможно использовать как необязательный атрибут (`MAY`). При попытке использовать его как обязательный атрибут (`MUST`) в новом `objectClass`, использующем формат LDIF для расширения схемы, соответствующая операция не будет выполнена.

Правила секции CONTAINMENT

Классы объектов, которые могут содержать определяемый класс объектов, приводятся в разделе X-NDS_CONTAINMENT описания классов объектов. Класс объектов person может содержаться в классах объектов organization, organizationalUnit и domain.

5.3.2 Добавление нового атрибута

Чтобы добавить атрибут, просто добавьте значение атрибута, соответствующее спецификации для NDSObjectClassDescription атрибута атрибутов subschemaSubentry.

```
NDSAttributeTypeDescription = "(" whsp
  numericoid whsp  ; AttributeType identifier
  [ "NAME" qdescrs ]  ; name used in AttributeType
  [ "DESC" qdstring ]  ; description
  [ "OBSOLETE" whsp ]
  [ "SUP" woid ]  ; derived from this other AttributeType
  [ "EQUALITY" woid]  ; Matching Rule name
  [ "ORDERING" woid]  ; Matching Rule name
  [ "SUBSTR" woid ]  ; Matching Rule name
  [ "SYNTAX" whsp noidlen whsp ] ;  Syntax OID
  [ "SINGLE-VALUE" whsp ]  ; default multi-valued
  [ "COLLECTIVE" whsp ]  ; default not collective
  [ "NO-USER-MODIFICATION" whsp ] ;  default user modifiable
  [ "USAGE" whsp AttributeUsage ] ;  default userApplications
  [ "X-NDS_PUBLIC_READ" qdstrings ]
                            ; default not public read ('0')
  [ "X-NDS_SERVER_READ" qdstrings ]
                             ; default not server read ('0')
  [ "X-NDS_NEVER_SYNC" qdstrings ]
                              ; default not never sync ('0')
  [ "X-NDS_NOT_SCHED_SYNC_IMMEDIATE" qdstrings ]
                           ;  default sched sync immediate ('0')
  [ "X-NDS_SCHED_SYNC_NEVER" qdstrings ]
                                ;  default schedule sync ('0')
  [ "X-NDS_LOWER_BOUND" qdstrings ]
                               ;  default no lower bound('0')
                                  ;(upper is specified in SYNTAX)
  [ "X-NDS_NAME_VALUE_ACCESS" qdstrings ]
                        ; default not name value access ('0')
  [ "X-NDS_NAME" qdstrings ]  ; legacy NDS name
  whsp ")"
```

В следующем примере файла LDIF в схему добавляется тип атрибута title:

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} X-NDS_NAME 'Title' X-NDS_NOT_SCHED_SYNC_IMMEDIA
7  TE '1' X-NDS_LOWER_BOUND '1')
8
```

Однозначные и многозначные атрибуты

По умолчанию используются многозначные атрибуты, пока не будет явно указана их однозначность. В следующем примере файла LDIF создается тип однозначного атрибута "title" путем добавления ключевого слова SINGLE-VALUE в разделе SYNTAX:

```
1 version: 1
2 dn: cn=schema
3 changetype: add
4 attributeTypes: ( 2.5.4.12 NAME 'title' DESC 'Standa
5  rd Attribute' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{
6  64} SINGLE-VALUE X-NDS_NAME 'Title' X-NDS_NOT_SCHED
7  _SYNC_IMMEDIATE '1' X-NDS_LOWER_BOUND '1')
8
```

Добавление необязательного атрибута к существующему классу объектов

Если добавление новых элементов Схемы является обычным действием, то изменение или расширение существующих элементов Схемы в большинстве случаев является рискованной операцией. Поскольку каждый элемент схемы определяется по уникальному идентификатору объекта (OID), то при расширении стандартного элемента схемы вы действительно создаете второе определение для элемента, даже если он по-прежнему использует исходный идентификатор объекта (OID). Это может привести к проблемам несовместимости.

Правда, иногда бывает удобно изменять элементы Схемы. Например, нужно расширить или изменить новые элементы Схемы при их переопределении в процессе разработки. Вместо добавления новых атрибутов непосредственно к классу, следует использовать вспомогательные классы только для:

- добавления атрибута к существующему классу объектов;
- добавления подкласса в существующий класс объектов.

5.3.3 Добавление или удаление вспомогательных классов

В следующем примере файл LDIF создает два новых атрибута, вспомогательный класс с этими новыми атрибутами, затем добавляет запись `inetOrgPerson` с классом `auxiliary` в качестве класса объектов для данной записи и со значениями для атрибутов класса `auxiliary`.

```
version: 1
# Add an attribute to track a bear's hair. The attribute is
# multi-valued, uses a case ignore string syntax,
# and has public read rights
# Values may include: long hair, short, curly, straight,
# none, black, and brown
# X-NDS_PUBLIC_READ '1' The 1 allows public read,
# 0 denies public read
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.10 NAME
'bearHair' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
X-NDS_PUBLIC_READ '1' )

# add an attribute to store a bear's picture
dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.186.4.11 NAME
'bearPicture' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
SINGLE-VALUE )

# create an Auxiliary class for the bearfeatures
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: (2.16.840.1.113719.1.186.6.101 NAME
'bearFeatures' MAY (bearHair $ bearPicture) AUXILIARY)
```

```
# now create a user named bobby
dn: cn=bobby,o=bearcave
changetype: add
cn: bobby
sn: bear
givenName: bobby
bearHair: Short
bearHair: Brown
bearHair: Curly
bearPicture:< file:///c:/tmp/alien.jpg
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: bearFeatures

# now create a person named john that will later be changed
# into a bear when bearFeatures is added to its objectClass
# list
dn: cn=john,o=bearcave
changetype: add
cn: John
sn: bear
givenName: john
objectClass: top
objectClass: person
objectClass: inetOrgPerson

# now morph john into a bear by adding bearFeatures
dn: cn=john,o=bearcave
changetype: modify
add: objectClass
objectClass: bearFeatures
-
add: bearHair
bearHair: long
bearHair: black
#bearPicture:< file:///c:/tmp/john.jpg>
-

# to morph john back to a person, simply delete the
# objectClass bearFeatures
dn: cn=john,o=bearcave
changetype: modify
delete: objectClass
objectClass: bearFeatures
```

При удалении вспомогательных классов нет необходимости удалять все значения, связанные с классом `auxiliary`, когда класс `auxiliary` удаляется из списка objectClass. eDirectory выполняет это автоматически.

Если класс `auxiliary` имел атрибуты `MUST`, все они должны быть указаны в той же операции изменения, которая добавляет класс `auxiliary` в список классов объекта. В противном случае изменение выполнено не будет.

Известные проблемы с синтаксическим анализом XML

XML-обработка любой записи LDIF (в формате LDIF или записи, сформированные с сервера LDAP) не будет выполнена, если отдельные записи не будут удовлетворять всем правилам XML, указанным в файле XML.

5.4 Ограничения ldif2dib

5.4.1 Файлы в формате LDIF, защищенные простым паролем

В Windows при отправке файлов LDIF, защищенных простым паролем, ldif2dib может завершиться со сбоем, если ключи NICI в папках `system` and *`Administrator`* не синхронизированы.

Чтобы решить данную проблему, выполните указанные ниже действия для получения доступа к ключам в папке `nici/system`.

1. Перейдите в папку `C:\Windows\system32\novell\nici\` (для 32-разрядной версии NICI).

   или

   Перейдите в каталог `C:\Windows\system32\novell\nici\` (для 64-разрядной версии NICI).
2. Выполните резервное копирование файлов в папке *`Administrator`*.
3. Перейдите на вкладку *Безопасность* в окне "Свойства" системной папки.
4. Выберите *Дополнительные параметры* и перейдите на вкладку *Владелец*.
5. Выберите пункт *Администратор*.
6. Вернитесь на вкладку *Безопасность* и добавьте администратора в список.
7. Повторите шаги Действ. 3—Действ. 6 для получения доступа на чтение для всех файлов, находящихся в системной папке.
8. Замените файлы в папке *`Administrator`* файлами папки `system`.
9. После завершения отправки скопируйте резервные копии файлов в папку *`Administrator`*.
10. Верните в исходное значение права администратора на доступ к папке `system` и находящимся в ней файлам.

5.4.2 Схема

В файле LDIF должны быть указаны все классы объектов, к которым принадлежит элемент. Также необходимо включить классы, к которым принадлежит элемент в результате наследования классов. Например, элемент типа `inetOrgPerson` имеет в файле LDIF следующий синтаксис:

- `objectclass: inetorgperson`
- `objectclass: organizationalPerson`
- `objectclass: person`
- `objectclass: top`

5.4.3 Шаблоны ACL

Объекты, загружаемые пакетно с помощью утилиты `ldif2dib`, не добавляются со списками ACL, указанными в шаблонах ACL для класса данного объекта.

5.4.4 обработчик сигналов

Автономную операцию пакетной загрузки можно временно приостановить, нажав клавишу s или S. Для остановки пакетной загрузки можно использовать клавишу Esc.

6 Поиск и устранение проблем SNMP

В данном разделе содержится информация о поиске и устранении проблем SNMP на всех платформах.

6.1 SNMP-ловушки могут создаваться не так, как ожидается

Ловушки отправляются, только когда соответствующий командный запрос получается сервером. В любых иных случаях они не отправляются. Например, `ndsDeleteAttribute` отправляется только в том случае, если отправлен запрос `ndsRemoveEntry` (номер запроса 108). Однако приложение всегда может прочитать списки ACL и проверить, имеет ли пользователь достаточные права для выполнения операции удаления. В этом случае ловушка `ndsDeleteAttribute` не создается. Однако можно использовать iMonitor для просмотра статистики команд на конкретном сервере.

Чтобы получить ловушки для всех случаев, установите интервал времени равным нулю.

Можно включить отправку ловушек только при наступлении условий сбоя. Можно включить получение ловушек при всех условиях.

ndssnmpsa должен перезапускаться при перезапуске основного агента

Для перезапуска ndssnmpsa остановите ndssnmpsa и запустите его вновь.

Для остановки ndssnmpsa введите следующую команду:

Linux: `/etc/init.d/ndssnmpsa stop`

Для запуска ndssnmpsa введите следующую команду:

Linux: `/etc/init.d/ndssnmpsa start`

6.2 Объект "Группа SNMP"

Если при установке объекта "Группа SNMP" произойдет сбой, для устранения проблемы введите с консоли сервера следующую команду:

```
ndsconfig add -m snmp
```

6.3 Ошибки инициализации SNMP

Компонент инициализации eDirectory SNMP. Код ошибки: -255

или

Сбой инициализации. Код ошибки: -255

Возможная причина — не указан `имя_хоста:порт` или `IP_адрес:порт` в качестве параметра команды `SERVER` в конфигурационном файле eDirectory SNMP.

Конфигурационный файл eDirectory SNMP — `ndssnmp.cfg`. Он расположен в следующих каталогах:

- Linux: `/etc/opt/novell/eDirectory/conf/ndssnmp/`
- Windows: *`install_directory`*`\SNMP\`

6.4 Субагент SNMP не запускается

При запуске субагента SNMP возможен возврат ошибки сегментации. Это может быть вызвано наличием лишних пробелов в файле `ndssnmp.cfg`. Удалите пробелы и запустите ndssnmpsa.

6.5 Отчеты со статистикой LDAP SNMP не создаются

Если анонимная привязка отключена, отчеты со статистикой LDAP SNMP не создаются.

Для решения этой проблемы:

1. Разрешите анонимную привязку.
2. Запустите субагент.
3. Отключите/запретите анонимную привязку.

6.6 Ошибка сегментации при доступе к субагенту

Если пользователь пытается запустить субагент (`ndssnmpsa`), используя неправильный пароль eDirectory, будет возвращена ошибка сегментации.

Чтобы избежать появления этой ошибки, перед запуском субагента удостоверьтесь, что введен верный пароль к eDirectory.

6.7 Проблемы с SNMP

6.7.1 Проблемы с протоколом после обновления eDirectory 8.7.3 до eDirectory 8.8

После обновления eDirectory 8.7.3 до eDirectory 8.8 может произойти следующая ошибка:

```
%%% Attempting to restart the NetIQ eDirectory SNMP subagent (ndssnmpsa)...
Starting NDS SNMP Subagent ...
Initialization failure. Error code : -255
Please Wait...
Done

%%% Unable to start ndssnmpsa... Please try starting it manually...
```

Эта ошибка происходит в связи с тем, что eDirectory 8.8 не прослушивает localhost. В более ранних версиях файл `ndssnmp.cfg` имел настройку по умолчанию `SERVER localhost`.

Для решения проблемы следует вручную отредактировать файл `ndssnmp.cfg`, включив в него имя хоста сервера eDirectory, который должен отслеживаться.

Например, в файле `ndssnmp.cfg` введите следующую строку:

```
SERVER test-server
```

test-server — это имя хоста, на котором запущен eDirectory с использованием порта NCP по умолчанию (524). Если для eDirectory используется другой порт (например 1524), строка должна иметь следующий вид:

```
SERVER test-server:1524
```

6.7.2 . Ошибки при запуске субагента NDS

В субагенте может произойти ошибка со следующим сообщением:

```
Unable to load library: libnetsnmp.so
```

Чтобы решить эту проблему, экспортируйте переменную окружения SNMP_MAJOR_VERSION с номером основной версии библиотеки net-snmp (`libnetsnmp.so`). Например, можно использовать следующую команду:

```
экспортируйте переменную SNMP_MAJOR_VERSION=10
```

6.7.3 Перезапуск ndssnmpsa

При перезапуске главного агента в ОС Linux необходимо перезапустить ndssnmpsa.

Для перезапуска ndssnmpsa остановите ndssnmpsa и запустите его вновь.

Чтобы остановить ndssnmpsa, введите следующую команду:

```
/etc/init.d/ndssnmpsa stop
```

Для запуска ndssnmpsa введите следующую команду:

```
/etc/init.d/ndssnmpsa start
```

6.7.4 . Ошибки при запуске ndssnmpsa

При запуске ndssnmpsa в Linux могут появиться следующие ошибки:

```
Error: eDirectory SNMP Initialization component. Error code: -168
```

```
Error: eDirectory SNMP Initialization component. Error code: 9
```

Чтобы устранить эти ошибки, выгрузите и загрузите ndssnmp при помощи следующих команд:

```
/opt/novell/eDirectory/bin/ndssnmp -u
```

```
/opt/novell/eDirectory/bin/ndssnmp -l
```

6.7.5 . Ошибки при остановке ndssnmpsa

При остановке ndssnmpsa в ОС SLES 9 отображается сообщение об ошибке, похожее на следующее: «`*** Обнаружена glibc *** повреждение или удвоенный объем свободной (!prev): 0x0819cdd0 ***`».

Можно не обращать внимания на эти сообщения.

6.7.6 Компиляция edir.mib

MIB-файл eDirectory (*<Корневой_каталог_установки_eDirectory>*`\snmp\edir.mib`) в Windows компилируется с некоторыми ошибками и предупреждениями для HP OpenView. Можно не обращать на них внимания.

6.7.7 Изменение файла конфигурации SNMP

Если протокол LDAP не настроен для запуска в режиме открытого текста, в конфигурационном файле SNMP (например, SSLKEY `C:\Novell\nds\trust.der`) необходимо указать имя файла доверенного корневого сертификата, прежде чем запускать субагент eDirectory SNMP.

В Windows файл ndssnmp.cfg находится в каталоге `C:\novell\nds\snmp`.

6.7.8 Использование SNMP после установки нового дерева

Если при первой установке eDirectory 8.8 с пакетом обновления 8 (когда создается новое дерево) на сервере установлен сервис Windows SNMP, который имеет один или несколько зависимых сервисов, eDirectory не может завершить этот сервис. В таких случаях протокол SNMP не готов к использованию сразу после установки eDirectory.

Чтобы перезапустить сервис SNMP, выполните действия, которые указаны далее

1. Последовательно выберите пункты *"Пуск"* > *"Настройка"* > *"Панель управления"* > *"Администрирование"* > *"Службы"*.
2. Щелкните правой кнопкой мыши пункт *Сервис SNMP* в списке *Имя*, затем щелкните пункт *Остановить*.
3. Выберите пункт *Да, для всех*.
4. Щелкните правой кнопкой мыши пункт *SNMP Service* в списке *Имя*, затем щелкните пункт *Запустить*.

6.7.9 Ошибка создания объекта SNMP в Windows Server

При установке eDirectory на любой поддерживаемой серверной платформе Windows может возникнуть ошибка создания объекта "Группа SNMP". В этом случае нужно создать данный объект вручную. Дополнительную информацию о действиях по созданию объекта SNMP вручную см. в разделе eDirectory and SNMP (eDirectory и SNMP) (http://www.netiq.com/documentation/edir88/edir88/data/ag7hr1h.html) документа *Novell eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию Novell eDirectory 8.8 SP8)*.

6.7.10 Удаление SNMP при удалении eDirectory

Если на сервере установлен сервис Windows SNMP, который имеет один или несколько зависимых сервисов, удаление eDirectory не приводит к удалению всех файлов SNMP из папки `C:\novell\nds`. Однако в остальном удаление завершается успешно, включая удаление ключей SNMP из реестра и процесс деконфигурации DS и сервиса SNMP, выполняемые агентом NetIQ SNMP.

Для завершения удаления выполните описанные ниже действия.

1. Последовательно выберите пункты *"Пуск"* > *"Настройка"* > *"Панель управления"* > *"Администрирование"* > *"Службы"*.
2. Щелкните правой кнопкой мыши пункт *Сервис SNMP* в списке *Имя*, затем щелкните пункт *"Остановить"*.
3. Выберите пункт *Да, для всех*.
4. Щелкните правой кнопкой мыши пункт *SNMP Service* в списке *Имя*, затем щелкните пункт *Запустить*.
5. Вручную удалите оставшиеся файлы SNMP в каталоге `C:\novell\nds`.

7 iMonitor

7.1 Просмотр в iMonitor объектов, содержащих двухбайтовые символы

При использовании iMonitor для поиска объектов в дереве eDirectory объекты, в имени которых содержатся двухбайтовые символы, могут неправильно ссылаться на свойства объекта.

7.2 Проверка состояния агентов в дереве с одиночным сервером

Если функция проверки состояния агентов в iMonitor выполняется в дереве с одним сервером, в столбце результатов отображается значок предупреждения вследствие статуса данных с ограниченным временем существования. Это не означает, что дерево не работает или что проверка состояния агентов не выполняется надлежащим образом. Данные с ограниченным временем существования – это количество данных, которые еще не были синхронизированы, как минимум, для одной реплики. Использование дерева с одним сервером по своей природе предполагает, что для данных всегда есть угроза катастрофического сбоя из-за отсутствия другого местоположения для тиражирования данных. В случае повреждения жесткого диска данные будут утрачены.

Если не требуется получать предупреждения функции проверки состояния о данных с ограниченным временем существования или о количестве реплик с возможностью чтения в дереве с одним сервером, можно отключить эти функции проверки состояния. Для этого в файле `ndsimonhealth.ini` измените следующие записи:

```
perishable_data-active: OFF
```

и

`ring_readable-Min_Marginal: 1` или `ring_readable-active: OFF`

В результате предупреждения о количестве реплик с возможностью чтения и о данных с ограниченным временем существования будут отключены.

7.3 В отчете iMonitor не сохраняются записи для каждого часа

Функция настраиваемых отчетов в iMonitor позволяет при создании настраиваемого отчета помещать в сохраняемый отчет (сохраняемый HTML-файл) URL-адрес, указанный пользователем. Это значит, что при открытии сохраненного настраиваемого отчета отображаются текущие данные, а не данные, полученные URL во время создания этого отчета. Эта проблема будет решена в следующей версии iMonitor.

7.4 Создание и изменение отметок времени.

В связи с тем, что на платформах Linux время создания файла не сохраняется, iMonitor всегда показывает одинаковое время создания и изменения файла.

7.5 Проблемы с iMonitor в старых версиях Mozilla

При доступе к iMonitor с использованием более ранних версий Mozilla, чем 1.5, в iMonitor могут возникнуть проблемы при выборе флага DSTrace. Mozilla может не поддерживать все действия.

7.6 В iMonitor не выравнивается экран запуска отчета.

В Linux рамка навигации и помощника отображается дважды.

Чтобы решить эту проблему, обновите страницу.

7.7 В iMonitor отображается ошибка -672

Если одновременно с iMonitor выполняется какое-либо средство отладки, не удается выполнить некоторые операции. Возвращается ошибка -672.

На платформе Linux

Если инструмент dsdump выполняется одновременно с iMonitor, то в iMonitor выводится ошибка -672.

Чтобы разрешить эту проблему, завершите работу инструмента dsdump перед запуском iMonitor.

На компьютерах с Windows

Если инструмент dsbrowse или dsedit выполняется одновременно с iMonitor, то в iMonitor выводится ошибка -672.

Чтобы разрешить эту проблему, завершите работу инструментов dsbrowse и dsedit перед запуском iMonitor.

7.8 Метки времени отображаются в шестнадцатеричном формате

Если атрибуту синтаксиса времени задать значение, предшествующее 1 января 1970 года, то в iMonitor метка времени для данного атрибута будет отображаться в шестнадцатеричном формате вместо стандартного формата дата/время. Все атрибуты со значениями после 1 января 1970 года отображаются в iMonitor в формате дата/время.

7.9 Проблема с конфигурацией трассировки iMonitor в Internet Explorer 10

Трассировка в iMonitor не настраивается в Internet Explorer 10.

Чтобы разрешить эту проблему, запустите Internet Explorer 10 в режиме совместимости, добавьте адрес iMonitor в список доверенных сайтов и перезапустите браузер.

8 iManager

8.1 Ошибка операций с LDAP после создания новой группы LDAP с помощью функции быстрого создания.

При быстром создании создается только объект "Группа LDAP" с фиктивными атрибутами, которые впоследствии можно изменить. Будет создан объект "Группа LDAP" с версией 11, а не 12. Таким образом, все операции LDAP будут завершаться с ошибкой из-за невозможности ассоциировать сервер LDAP вследствие несовместимости версий.

Чтобы разрешить эту проблему, после создания группы LDAP с помощью функции быстрого создания измените номер версии объекта "Группа LDAP" на 12.

9 Значения устаревшего состояния

Значения устаревшего состояния служат операционными атрибутами, которые eDirectory помещает в объекты, чтобы обеспечить ссылочную целостность при выполнении операций удаления, перемещения, переименования и восстановления. Например, если в группе A есть участник (Пользователь B), который удаляется, то каталог автоматически удалит ссылку на Пользователя B из группы A. В eDirectory 8.8 SP8 значения устаревшего состояния, сформированные операциями удаления, перемещения и переименования оптимизированы по умолчанию.

ПРИМЕЧАНИЕ. Объекты со значениями устаревшего состояния рассматриваются при каждой исходящей синхронизации агента, а также процессом обработки значений устаревших состояний, выполнение которого запланировано в конце цикла входящей синхронизации.

Существуют три основных вида значений устаревшего состояния:

- Первичные значения устаревшего состояния включают значения следующих типов: "Dead" (Мертвый, 0001), "Restored" (Восстановлен, 0000), "Moved" (Перемещен, 0002), "New RDN" (Новое имя RDN, 0005) и "Tree New RDN" (Новое имя RDN дерева, 0008).
- Вторичные значения устаревшего состояния в основном ассоциированы с первичными значениями и являются агентами и разделами, требующими оповещения об операции, указанной в первичном значении устаревшего состояния. В них входят следующие типы: "Back Link" (Обратная ссылка, 0006), "Used By" (Используется объектом, 000C) и "Move Tree" (Перемещение дерева, 000a).
- Отслеживающие значения устаревшего состояния включают следующие типы: "Inhibit Move (0003)" (Запрещение переноса), "Old RDN" (Старое имя RDN, 0004) и "Tree Old RDN" (Старое имя RDN дерева, 0007).

Значения устаревшего состояния, за исключением отслеживающих, должны пройти ряд состояний синхронизации:

- Начальное состояние или установлено (0)
- Оповещено (1)
- Готово к очистке (2)
- Очищаемый (4)

Состояния регистрируются в поле "Флаги" атрибута значения устаревшего состояния. До того, как значение устаревшего состояния сможет перейти в следующее состояние, текущее состояние должно быть синхронизировано со всеми репликами реального объекта. Чтобы определить, все ли реплики кольца были оповещены о данном состоянии значения устаревшего состояния, вычисляется переходный вектор. В eDirectory 8.6 и более поздних версий используется несохраняемый вектор значений устаревшего состояния. В предыдущих версиях eDirectory использовался вектор очистки. Если дата отметки времени модификации

(Modification Timestamp - MTS) значения устаревшего состояния окажется более ранней, чем дата поврежденного вектора, сервер, ответственный за данное значение устаревшего состояния, может перевести его в следующее состояние.

Агент, хранящий главную реплику объекта со вторичным значением устаревшего состояния типа "Обратная ссылка", несет ответственность за изменение его состояний. Ответственность за изменение состояний вторичного значения устаревшего состояния типа "Используется" несет создавший его агент реплики на протяжении всего времени существования этой реплики. Если эта реплика больше не существует, ответственность за изменение состояний вторичного значения устаревшего состояния типа "Используется" несет главная реплика данного раздела. Ответственность за изменение состояний значения устаревшего состояния типа "Перенос дерева" несет главная реплика корневого раздела.

Изменение состояния первичных значений устаревшего состояния может происходить только после того, как все вторичные значения устаревшего состояния последовательно прошли все свои состояния. После того, как первичное значение устаревшего состояния достигает своего конечного состояния, а также после синхронизации этого состояния со всеми серверами кольца, остается объект без атрибутов, который впоследствии может быть удален из системы в процессе очистки. Отслеживающие значения устаревшего состояния удаляются тогда, когда первичное значение устаревшего состояния готово к удалению, а устаревшие отслеживающие значения устаревшего состояния с `запретом переноса (Inhibit_move)` удаляются после того, как первичное значение устаревшего состояния перейдет в состояние `OBF_NOTIFIED` в главной реплике.

Реплика, ответственная за обработку значений устаревшего состояния, выполняет это в виде фонового процесса (процесса обработки значений устаревшего состояния), планируемого для каждого раздела, после того как в данном разделе будет завершен цикл входящей синхронизации. Если в разделе других реплик нет, процесс исходящего тиражирования планируется с интервалом Heartbeat. Затем процесс исходящего тиражирования запускает процесс обработки значений устаревшего состояния. Процесс обработки значений устаревшего состояния не может и не должен планироваться вручную. По мере выполнения синхронизации обновляются переходные векторы, изменяется состояние векторов очистки и векторов значений устаревшего состояния. Вместе с ними изменяются и состояния значений устаревшего состояния. Совместно с автоматическим планированием при входящей синхронизации это приводит к завершению цикла обработки значений устаревшего состояния. Таким образом, движущей силой процесса обработки значений устаревшего состояния является синхронизация объектов.

Для удаляемого объекта: после того, как все значения устаревшего состояния, которые ассоциированы с первичным значением устаревшего состояния "Dead" (Мертвое), перешли в последнее состояние "Purgable" (Очищаемое) и информация об этом была синхронизирована во всех репликах, запускается другой процесс, ответственный за удаление остатков объекта из базы данных. Процесс очистки автоматически удаляет остаточные элементы. Процесс очистки можно запланировать вручную. Можно также изменить интервал его автоматического планирования с помощью страницы iMonitor Конфигурация агента.

9.1 Примеры

Этот раздел включает следующие примеры:

- "Удаление объекта" на стр. 65
- "Перемещение объекта" на стр. 66

9.1.1 Удаление объекта

1 Добавление первичного значения устаревшего состояния OBT_DEAD.

Атрибут "Обратная ссылка" содержит список серверов, которые ассоциированы с данным объектом и которые должны быть оповещены об изменениях этого элемента. Для каждого имени DN, перечисленного в атрибуте "Обратная ссылка", и для всех серверов, перечисленных в атрибуте реплики раздела элемента, eDirectory добавляет значение устаревшего состояния "Обратная ссылка". Время создания первичного значения устаревшего состояния OBT_DEAD хранится во вторичном значении устаревшего состояния.

Атрибут "Используется" содержит список разделов, которые ассоциированы с данным объектом и которые должны быть оповещены об изменениях этого элемента. Для каждого имени DN, перечисленного в атрибуте "Используется", eDirectory добавляет значение устаревшего состояния "Используется". Время создания первичного значения устаревшего состояния OBT_DEAD хранится во вторичном значении устаревшего состояния.

2 Удаление всех атрибутов, кроме значений устаревшего состояния.

Затем процесс исходящего тиражирования синхронизирует это изменение со всеми серверами кольца реплик.

При следующей входящей синхронизации данного раздела запускается процесс обработки значений устаревших состояний, выполняющий следующее:

- Вычисление вектора времени, который является минимальным переходным вектором и называется вектором очистки. В более поздних версиях eDirectory вычисляется второй минимальный вектор, который называется вектором значения устаревшего состояния. При этом не принимаются во внимание реплики, которые являются ссылками на подчиненный раздел.
- В данном разделе проверяются все значения устаревшего состояния.

  Если значение устаревшего состояния является первичным, а вторичных значений нет и при этом атрибут был изменен раньше создания вектора очистки, то о данном изменении были оповещены все серверы. Данное значение устаревшего состояния удаляется.

  Если типом значения устаревшего состояния является "Обратная ссылка" и данный сервер является главным, он отвечает за обработку данного значения устаревшего состояния.

  ЗАМЕЧАНИЕ. Выполнение операций, требуемых для данного состояния, если они не были выполнены ранее. Чаще всего это выполняется посредством оповещения внешней ссылки.

  Если значение устаревшего состояния имеет тип "Used By (Используется)", а данный сервер - это сервер, на котором выполняется удаление (что проверяется сравнением номера реплики в MTS значения устаревшего состояния с номером текущей реплики), то этот сервер отвечает за обработку этого значения устаревшего состояния.
- Если определенный сервер отвечает за обработку типа вторичного значения устаревшего состояния ("Обратная ссылка" или "Используется"), все вторичные значения устаревшего состояния данного типа для элемента находятся в одном и том же состоянии, и требуемая для данного состояния операция выполнена для всех значений устаревшего состояния (например, серверы оповещены), и данные MTS для

данного типа значений устаревшего состояния старше, чем вектор значений устаревшего состояния, то все вторичные значения устаревшего состояния этого типа могут перейти в следующее состояние.

9.1.2 Перемещение объекта

Операция переноса аналогична операции удаления, за исключением следующего:

- Перед тем, как первичное значение устаревшего состояния помещается в источник переноса, в целевом контейнере создается частичный элемент, в который помещается отслеживающее значение устаревшего состояния (OBT_INHIBIT_MOVE). Размещение отслеживающего значения устаревшего состояния обусловлено необходимостью предотвращения переноса элемента или его участия в функционировании раздела до того, как весь элемент будет перенесен из источника.
- Первичным значением устаревшего состояния исходного элемента является OBT_MOVED.
- После того, как первичное значение устаревшего состояния OBT_MOVED переходит в состояние "Оповещено" (т. е. все реплики источника оповещены о переносе элемента), и после оповещения всех внешних ссылок отслеживающее значение устаревшего состояния (OBT_INHIBIT_MOVE) удаляется из целевого элемента.

9.2 Меры предосторожности

Регулярно формируйте отчет iMonitor "Информация о сервере". При создании этого отчета выполняется обход всего дерева, обращение ко всем NCP-серверам, которые были найдены, а также сообщается обо всех найденных ошибках. Этот отчет можно использовать для диагностики проблем синхронизации времени и процесса Limber, а также для выяснения способности взаимодействия текущего сервера с другими серверами с точки зрения данного сервера. Если данный сервер выбран на странице конфигурации, он также сможет формировать информацию о состоянии агента NDS для любого сервера в дереве. Дополнительную информацию о выполнении отчета информации о сервере см. в разделе "Configuring and Viewing Reports (настройка и просмотр отчетов)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

При использовании iMonitor 2.0 или более поздней версии убедитесь в том, что включены параметры вложенного отчета о состоянии и ошибках. Необходимо проверить перечисленные ниже элементы. Следует просмотреть отчет и убедиться в отсутствии ошибок.

- В зависимости от информации в конфигурационном файле `ndsimonhealth`, который хранится с iMonitor (см. раздел "Configuration Files (Конфигурационные файлы)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*), при выполнении этого отчета будет проверена версия агента eDirectory, что позволит убедиться в выполнении правильных исправлений каталога во всем дереве.
- Все серверы работают в пределах допусков Timesync.
- Данный сервер может взаимодействовать со всеми остальными серверами.
- Отсутствуют серверы, неправильно или неполностью удаленные из дерева.
- Если какие-либо разделы работают с нарушением допусков для времени синхронизации тиражирования, это будет указано во вложенном отчете состояния.

Если используется iMonitor 1.5, выберите параметр отчета "Ошибки". Необходимо проверить перечисленные ниже элементы. Следует просмотреть отчет и убедиться в отсутствии ошибок.

- Отображается версия агента. Убедитесь в наличии на серверах всего дерева самого последнего пакета обновления eDirectory, доступного на веб-сайте поддержки NetIQ (http://support.novell.com).
- Все серверы работают в пределах допусков Timesync.
- Данный сервер может взаимодействовать со всеми остальными серверами.
- Отсутствуют серверы, неправильно или неполностью удаленные из дерева.

Любые значения устаревшего состояния в системе можно обнаружить с помощью отчета iMonitor "Список устаревших состояний" или "Статистика объектов". При выявлении каких-либо значений устаревшего состояния, которые не должны обрабатываться, см. раздел Раздел 9.3, "Советы по устранению проблем" на стр. 67.

9.3 Советы по устранению проблем

Есть две общие причины, по которым значения устаревшего состояния не обрабатываются: нарушены ассоциации значения устаревшего состояния (т. е. оно существует на некоторых, но не на всех серверах) или значение устаревшего состояния не может быть обработано (т. е. оно существует на всех серверах, но его состояния по какой-то причине не изменяются).

Для решения проблем со значениями устаревшего состояния, которые не могут быть обработаны, и со значениями устаревшего состояния с нарушенными ассоциациями воспользуйтесь следующими рекомендациями.

- ❒ Не паникуйте.
- ❒ Если это значение устаревшего состояния объекта, не хранящегося на данном сервере (т. е. объект является внешней ссылкой):
  - Проверьте, нет ли у действительного объекта соответствующего значения устаревшего состояния. Если нет, то значение устаревшего состояния не синхронизировано. См. "Исправление значений устаревшего состояния с нарушенными ассоциациями с внешними ссылками" на стр. 69 для получения дополнительной информации.
  - Если у действительного объекта есть соответствующее значение устаревшего состояния, устраните проблемы и исправьте значение устаревшего состояния действительного объекта перед попыткой решения проблем со значением устаревшего состояния в разделе `внешних ссылок`.
- ❒ Убедитесь в том, что значения устаревшего состояния правильно синхронизированы.
  - Для проверки и исправления ошибок синхронизации используйте страницу iMonitor Синхронизация агента.
  - Состояния значений устаревшего состояния могут меняться только тогда, когда все агенты, на которых хранится копия кольца реплик, распознают изменение состояния. Существует несколько способов проверки получения данных всеми серверами:

    При просмотре элемента со значениями устаревшего состояния щелкните ссылку "Синхронизация элемента". На этой странице будут отображены все атрибуты, которые не были синхронизированы на всех репликах.

Найдите самую раннюю отметку времени любых значений атрибута устаревшего состояния. Разница меду этим и текущим временем не должна превышать интервал времени, отображаемого в поле "Макс. дельта кольца" на странице "Синхронизация раздела".

Оцените переходный вектор.

- ❒ Выполните Отчет по информации сервера iMonitor, чтобы проверить работоспособность связи с сервером.
- ❒ Проверьте раздел Статус процесса агента: значения устаревшего состояния на наличие любых ошибок.
  - Распространенные в разделе "Статус процесса агента: значения устаревшего состояния":

    -625, -622, -634, и -635 (проблемы с обменом данными). Дополнительную информацию см. в отчете Информация о сервере.

    Ошибки -601 и -603, в которых указываются неправильно удаленные серверы или серверы, объект "Сервер" которых, возможно, имеет базовый класс "Неизвестный".
  - Ошибки, указанные на данной странице, не являются критическими. Попытка выполнения данной операции будет повторно предпринята при следующем выполнении процесса обработки значений устаревших состояний для данного раздела. Устраните все проблемы, отображаемые на данной странице, и дождитесь повторной попытки.
- ❒ Просматривая объекты значений устаревшего состояния, сравните значения устаревшего состояния по всему кольцу реплик.
  - Если копии значений устаревшего состояния существуют не во всех репликах и все значения атрибутов не являются очищаемыми, значит, данный объект не согласован с кольцом реплик. Это случай значения устаревшего состояния с нарушенными ассоциациями. См. "Исправление значений устаревшего состояния с нарушенными ассоциациями" на стр. 69 для получения дополнительной информации.
  - Если объект существует на всех репликах и согласован, его состояния могут не изменяться из-за ошибок синхронизации или ошибок процесса обработки значений устаревших состояний.
- ❒ При необходимости можно использовать трассировку со включенным параметром "Значения устаревшего состояния" для детальной проверки процесса обработки значений устаревших состояний.
- ❒ Для предотвращения проблем со значениями устаревшего состояния в дальнейшем воспользуйтесь последней версией пакета обновления (для серверов eDirectory 8.6). В последний пакет обновления включены исправления всех известных ошибок, возникающих при работе со значениями устаревшего состояния.

9.3.1 Решения

Используйте правильное решение, на которое присутствует ссылка в разделе Раздел 9.3, "Советы по устранению проблем" на стр. 67.

Перед использованием любых из этих решений убедитесь в безопасности данных. Возможно, потребуется резервное копирование файлов базы данных Каталога, конфигурации сервера и опекунов. Для повышения вероятности успеха и снижения возможности появления проблем в будущем воспользуйтесь последними пакетами обновления eDirectory.

Исправление значений устаревшего состояния с нарушенными ассоциациями

- **Предпочитаемый способ.** Если eDirectory 8.6 или более поздней версии установлен на любом из серверов кольца реплик, найдите объект в iMonitor, затем выберите "Send Single Entry" (Отправить один элемент). При этом произойдет недостоверная отправка всем остальным репликам.
- **Нежелательный способ.** Если на всех серверах кольца реплик, имеющих копию значения устаревшего состояния с нарушенными ассоциациями, используется версия eDirectory, предшествующая 8.6, загрузите приложение DSBrowse с параметром "–a", найдите объект, затем установите отметки времени элемента. При этом объект в том виде, в котором он существует на данном сервере, станет достоверной копией. Не рекомендуется систематически прибегать к преобразованию объектов в достоверные.

Исправление значений устаревшего состояния с нарушенными ассоциациями с внешними ссылками

- **Менее предпочитаемый способ.** Запустите DSRepair с выбранным параметром отметки времени.
- **Менее предпочитаемый способ.** Перенесите действительную реплику на сервер, дождитесь ее включения и обработки значения устаревшего состояния. Если значение устаревшего состояния не обрабатывается, для устранения проблемы воспользуйтесь информацией, приведенной в разделе Раздел 9.3, "Советы по устранению проблем" на стр. 67, после того как объект будет перенесен в действительную реплику. После обработки значения устаревшего состояния реплику можно при необходимости удалить.

9.3.2 Способы, использовавшиеся ранее

В прошлом для решения проблемы значений устаревшего состояния, которые не могут быть обработаны, использовались разные стратегии. Некоторые из них включают в себя дорогостоящие операции разбиения на разделы, а также использование недокументированных функций, что могло привести к появлению новых проблем.

Первая стратегия заключалась в переключении главных реплик. Иногда это помогало, поскольку главная реплика является агентом, отвечающим за смену состояний значений устаревшего состояния типа "Обратная ссылка". Если реплика оказывалась несогласованной, а главная реплика не хранила удаленный объект, то переключение главной реплики на агент, содержащий удаленный объект со всеми значениями устаревшего состояния, позволяло новому агенту изменять состояния значения устаревшего состояния и, наконец, очистить его. Функция "Send Single Entry" (Отправить один элемент) является намного более аккуратным и безопасным способом устранения проблем значений устаревшего состояния, которые не могут быть обработаны, и возникли из-за несогласованности реплик.

Следующая стратегия заключалась в использовании утилиты DSRepair с определенными параметрами для удаления всех значений устаревшего состояния. (Есть стороннее приложение, которое позволяет разрешить значения устаревшего состояния, которые не могут быть обработаны путем запуска DSRepair). Мы не рекомендуем использовать эту стратегию. Использование таких параметров приведет к удалению всех значений устаревшего состояния данного агента, в том числе и нормально обрабатываемых, что приведет к росту несогласованности реплик и увеличению числа значений устаревшего состояния, которые не могут быть обработаны. Поскольку это нераспределенная операция, утилиту DSRepair потребуется запускать на всех серверах, содержащих значения устаревшего состояния, которые не могут быть обработаны. При этом увеличится вероятность того, что на одном из

этих серверов будут существовать значения устаревшего состояния для другого раздела, которые будут удалены раньше времени. Преждевременное удаление значений устаревшего состояния может привести к появлению дополнительных значений устаревшего состояния с нарушенными ассоциациями, и, в свою очередь, привести к проблемам, о которых станет известно лишь через несколько лет при изменении типов реплик, добавлении новых реплик или выполнения других операций по разбиению на разделы.

Третья использовавшаяся стратегия заключалась в преобразовании объектов в достоверные или с помощью режима эксперта в утилите DSBrowse, устанавливающей отметки времени элементов, или с помощью запуска утилиты DSRepair с параметром "-0T". При этом элемент становится достоверным и выполняет исходящую синхронизацию со всеми остальными репликами. Это следует делать с большой осторожностью, поскольку можно утратить данные, измененные на других серверах. Не рекомендуем использовать этот метод часто для очистки значений устаревшего состояния.

10 Миграция в NetIQ eDirectory

В этом разделе описан процесс миграции в NetIQ eDirectory с:

10.1 Миграция схемы Sun ONE в NetIQ eDirectory

Порядок выполнения миграции схемы Sun ONE в NetIQ eDirectory.

10.1.1 Этап 1. Выполните операцию обновления кэша схемы

Можно записать ошибки, возникшие при сравнении схемы с файлом ошибок. Для этого выполните следующую команду:

```
ice -e LDIF error file name -C -a -SLDAP -s Sun ONE server -p Sun ONE port -DLDAP -
s eDirectory server -p eDirectory port
```

Например:

```
ice -e err.ldf -C -a -SLDAP -s sun_srv1 -p sun_port1 -DLDAP -s edir_srv2 -p
edir_port2
```

Все ошибки, возникшие при сравнении схемы записываются в файл ошибок (в данном примере — `err.ldf`). Для выполнения этой операции необязательно входить в систему. Исключение составляют те случаи, когда серверы требуют аутентификации для чтения Root DSE. Microsoft Active Directory требует аутентификации для чтения Root DSE.

10.1.2 Этап 2. Исправьте файл ошибок LDIF для устранения ошибок

- В Sun ONE некоторые схемы определены публично, чего нет в eDirectory. Это справедливо для атрибутов, таких как `objectClasses`, `attributeTypes`, `ldapSyntaxes` и `subschemSubentry`. Эти определения существуют внутри и очень важны для схемы, поэтому их невозможно изменить. Операции, направленные на изменение этих определений, приводят к следующей ошибке:

  ```
  LDAP error : 53 (DSA is unwilling to perform)
  ```

  Любые записи, содержащие ссылки на эти определения, приводят к следующей ошибке:

  ```
  LDAP error : 16 : ( No such attribute )
  ```

Поэтому записи, которые содержат любую ссылку на эти объекты или пытаются изменить эти определения, необходимо закомментировать в файле ошибок LDIF (в данном примере это файл `err.ldf`).

- Некоторые определения классов объекта не имеют атрибутов наименования. Добавление этих классов объекта приведет к возврату следующей ошибки в eDirectory:

  ```
  LDAP error : 80 (NDS error: ambiguous naming (-651)
  ```

  Эта ошибка происходит, поскольку в Sun ONE и eDirectory используются разные методы определения правил наименования.

  Для разрешения этой проблемы можно использовать *любую* из трех указанных ниже возможностей.

  Вариант 1.

  Просмотрите все нарушенные классы объекта и добавьте действительный атрибут наименования в каждый из них.

  Например:

  Чтобы добавить атрибут наименования `[ cn ]` в класс объекта `netscapeMachineData`, измените запись (которая *выделена* в примере ниже) в файле `err.ldf` для включения флага `X-NDS_NAMING` как показано ниже:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
      DESC 'iPlanet defined objectclass' SUP top STRUCTURAL MAY 'cn'     X-
  NDS_NAMING 'cn' )-
  ```

  Вариант 2.

  Просмотрите все нарушенные классы объекта и измените их определение на AUXILIARY или ABSTRACT.

  Например:

  Чтобы изменить определение класса объекта `netscapeMachineData` с STRUCTURAL на AUXILIARY, измените запись файла `err.ldf` (которая *выделена* в примере ниже) как показано ниже:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
     DESC 'iPlanet defined objectclass' SUP top AUXILIARY )-
  ```

  Чтобы изменить определение класса объекта `netscapeMachineData` с STRUCTURAL на ABSTRACT, измените запись файла `err.ldf` (которая *выделена* в примере ниже) как показано ниже:

  ```
  dn: cn=schemachangetype: modifyadd: objectClassesobjectClasses: (
  2.16.840.1.113730.3.2.32 NAME 'netscapeMachineData'
     DESC 'iPlanet defined objectclass' SUP top ABSTRACT )-
  ```

  Вариант 3.

  Добавьте `cn` в определение `Top` в eDirectory, в результате чего потенциальные атрибуты наименования будут добавлены во все классы объекта.

  Есть два способа добавить `cn` в `Top`.

  - **Метод 1:**

    Создайте файл, как показано ниже, и назовите его `topsch.ldf`.

    ```
    version : 1

    dn:cn=schema

    changetype :modify
    ```

```
delete : objectclasses

objectclasses : ( 2.5.6.0 NAME 'top' STRUCTURAL )

-

add:objectclasses

objectclasses : (2.5.6.0 NAME 'top' STRUCTURAL MAY cn)
```

Выполните следующую команду NetIQ Import Conversion Export:

```
ice -SLDIF -f LDIF_file_name -DLDAP -s eDirectory_server -p eDirectory_port
-d eDirectory_Admin_DN -w eDirectory_password
```

Например:

```
ice -SLDIF -f topsch.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

- **Метод 2:**

  1. В NetIQ iManager нажмите кнопку *Функции и задачи*  .
  2. Последовательно выберите пункты *Схема* > *Добавить атрибут*.
  3. В списке *Доступные классы* выберите *Top* и нажмите кнопку *OK*.
  4. В списке *Доступные необязательные атрибуты* дважды щелкните *CN*.
  5. Нажмите кнопку *OK*.

- В некоторых определениях класса объекта имеется атрибут `userPassword`, который входит в список обязательных атрибутов. Добавление таких классов объекта в eDirectory приведет к возврату следующей ошибки:

  ```
  LDAP error : 16 (No such attribute)
  ```

  Чтобы устранить эту ошибку, измените определение класса объекта таким образом, чтобы он наследовал новый класс объекта из `ndsLoginProperties`, и удалите атрибут `userPassword` из списка обязательных атрибутов.

  Например:

  Класс объекта, содержащий атрибут `userPassword` из списка обязательных атрибутов:

  ```
  version : 1
  dn: cn=schemaz
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP top STRUCTURAL MUST userPassword )
  ```

  Необходимо внести указанные ниже изменения (обратите внимание на изменения в последней строке):

  ```
  version : 1
  dn: cn=schema
  changetype: modify
  add: objectClasses
  objectClasses: ( 0.9.2342.19200300.100.4.19 NAME 'simpleSecurityObject' DESC '
   Standard LDAP objectClass' SUP (ndsLoginProperties $ top) STRUCTURAL )
  ```

10.1.3 Этап 3. Импорт файла LDIF

Воспользуйтесь следующей командой NetIQ Import Conversion Export для импорта измененного файла сравнения схемы LDIF (`err.ldf` в данном примере):

```
ice -e error_file -SLDIF -f modified_LDIF_file -DLDAP -s eDirectory_server -p
eDirectory_port -d eDirectory_Admin_DN -w eDirectory_password
```

Например:

```
ice -e errors.ldf -SLDIF -f err.ldf -DLDAP -s edir_srv2 -p edir_port2 -d
cn=admin,o=org -w pwd1
```

10.2 Миграция Active Directory Schema в NetIQ eDirectory с использованием ICE

При выполнении миграции схемы из Active Directory в NetIQ eDirectory с использованием ICE для класса объекта `Computer` возвращается ошибка `ambiguous naming error (-651)`.

Чтобы решить эту проблему, выполните описанные ниже действия.

"Этап 1. Выполните операцию обновления кэша схемы" на стр. 71
"Этап 2. Исправьте файл ошибок LDIF для устранения ошибок" на стр. 71
"Этап 3. Импорт файла LDIF" на стр. 73

10.2.1 Этап 1. Выполните операцию обновления кэша схемы

При миграции схемы из Active Directory в NetIQ eDirectory с использованием ICE, убедитесь в том, что указан параметр (`-e`) журнала ошибок ICE, как указано ниже:

```
ice -e error_file -S ldap -s Active_Directory_server -p Active_Directory_port -d
Active_Directory_full_admin_context -w Active_Directory_password -D ldap -s
eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w
eDirectory_password
```

Например:

```
ice -e err.ldf -S ldap -s activesrv1 -p activeport1 -d cn=admin,o=company -w
activepwd -D ldap -s edirsrv2 -p edirport2 -d cn=admin,o=company -w edirpwd
```

10.2.2 Этап 2. Исправьте файл ошибок LDIF для устранения ошибок

Запись, вызвавшая сбой, присутствует в файле `err.ldf` как показано ниже:

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP (device $
 user ) STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $
 local PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netboot MirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )
```

```
-
```

Измените эту запись в файле ошибок (в данном примере это файл `err.ldf`), чтобы удалить класс объекта `user` из списка вышестоящих классов объекта в определении класса объекта `Computer`, как показано ниже.

```
dn: cn=schema

changetype: modify

delete: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' )

-

add: objectclasses

objectclasses: ( 2.16.840.1.113719.1.1.6.1.4 NAME 'computer' SUP device
 STRUCTURAL MAY (operator $ server $ status $ cn $ networkAddress $ local
 PolicyFlags $ defaultLocalPolicyObject $ machineRole $ location $
 netbootInitialization $ netbootGUID $ netbootMachineFilePath $ siteGUID $
 operatingSystem $ operatingSystemVersion $ operatingSystemServicePack $
 operatingSystemHotfix $ volumeCount $ physicalLocationObject $ dNSHostName
 $ policyReplicationFlags $ managedBy $ rIDSetReferences $ catalogs $
 netbootSIFFile $ netbootMirrorDataFile ) X-NDS_NOT_CONTAINER '1' X
 -NDS_NONREMOVABLE '1' X-NDS_NAME 'Computer' )

-
```

10.2.3 Этап 3. Импорт файла LDIF

После этого импортируйте измененную запись, используя следующую команду ICE:

```
ice -S ldif -f LDIF_file -D ldap -s Novell_eDirectory_server -p port_number -d
full_admin_context -w password
```

Например:

```
ice -S ldif -f err.ldf -D ldap -s edirsrv1 -p edirport1 -d cn=admin,o=company -w
pwd1
```

10.3 Миграция из OpenLDAP в NetIQ eDirectory

10.3.1 Необходимые условия

Данные, которые мигрировали с сервера OpenLDAP, могут иметь пароли MD5, а это может привести к сбою приложений, если соответствующие методы NetIQ Modular Authentication Service (NMAS) не установлены. Для NetIQ eDirectory необходимо установить метод NMAS SimplePassword при помощи следующей команды:

```
nmasinst -addmethod контекст_администратора имя_дерева файл_конфигурации -h
имя_хоста:порт-w пароль
```

Например: `nmasinst -addmethod admin.novell eDir-Tree /Linux/eDirectory/nmas/NmasMethods/Novell/SimplePassword/config.txt -h eDir_srv:524 -w secret`

10.3.2 Миграция схемы OpenLDAP в eDirectory

Порядок выполнения миграции схемы OpenLDAP в eDirectory.

- "Этап 1. Выполните операцию обновления кэша схемы" на стр. 76
- "Этап 2. Исправьте файл ошибок LDIF для устранения ошибок" на стр. 76

Этап 1. Выполните операцию обновления кэша схемы

Можно записать ошибки, возникшие при сравнении схемы с файлом ошибок. Для этого выполните следующую команду:

```
ice -e error_file -C -a -S ldap -s OpenLDAP_server -p Open_LDAP_port - D ldap -s eDirectory_server -p eDirectory_port -d eDirectory_full_admin_context -w eDirectory_password
```

Например:

```
ice -e err.ldf -C -a -SLDAP -s open_srv1 -p open_port1 -DLDAP -s edir_srv2 -p edir_port2 -d cn=admin,o=novell -w secret
```

Все ошибки, возникшие при сравнении схемы записываются в файл ошибок (в данном примере — `err.ldf`).

Этап 2. Исправьте файл ошибок LDIF для устранения ошибок

Open LDAP определяет некоторые определения схемы общедоступно. Это относится к таким атрибутам, как `objectClasses`, `attributeTypes`, `ldapSyntaxes` и `subschemSubentry`. Эти определения существуют внутри и очень важны для схемы, поэтому их невозможно изменить. Операции, направленные на изменение этих определений, приводят к следующей ошибке:

```
LDAP error : 53 (DSA is unwilling to perform)
```

Любые записи, содержащие ссылки на эти определения, приводят к следующей ошибке:

```
LDAP error : 16 ( No such attribute )
```

Поэтому записи, которые содержат любую ссылку на эти объекты или пытаются изменить эти определения, необходимо закомментировать в файле ошибок LDIF (в данном примере это файл `err.ldf`).

10.3.3 Миграция данных Open LDAP в NetIQ eDirectory

Чтобы выполнить миграцию данных, воспользуйтесь следующей командой:

```
ice -e error_data.ldif -SLDAP -s OpenLDAP_server -p OpenLDAP_port  -d admin_context -w password -t -b dc=blr,dc=novell,dc=com -F objectclass=* -DLDAP -d  admin_context -w password  -l  -F
```

Например:

```
ice -e err_data.ldif -SLDAP -s open_srv1 -p open_port1  -d cn=administrator,dc=blr,dc=novell,dc=com -w secret1 -t -b dc=blr,dc=novell,dc=com -F objectclass=* -DLDAP -d cn=admin,o=novell -w secret2 -l -F
```

Миграция некоторых объектов может быть не выполнена из-за опережающих ссылок и внутренних зависимостей объектов, которые могут не нарушать работу ни одного приложения.

10.3.4 Обеспечение работы PAM с NetIQ eDirectory после миграции

После миграции из OpenLDAP в eDirectory необходимо внести некоторые изменения, которые требуются для работы PAM с eDirectory.

Изменения в файле /etc/ldap.conf File

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
  binddn cn=admin,o=acme
  ...
# The credentials to bind with.
# Optional: default is no credential.
  bindpw secret
  ...
# The search scope.
  scope sub
  ...
# Filter to AND with uid=%s
  pam_filter objectclass=inetorgperson
  ...
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
  pam_password nds
  ...
  ssl off
  ...
```

Изменения данных в каталоге

Это изменение относится только к тому сценарию, в котором пользовательские объекты в OpenLDAP имеют алгоритм хэширования паролей CRYPT.

Используя iManager, добавьте в контейнер со всеми объектами "Пользователь" следующий атрибут с указанным значением:

Атрибут: `sasDefaultLoginSequence`

Значение: Simple Password

11 Схема

В этом разделе содержится информация о поиске и устранении проблем схемы.

Поиск и устранение проблем схема

При отделении вспомогательного класса от объекта, данное значение не удаляется немедленно, а отмечается как неприсутствующее. Этот вспомогательный класс остается связанным с этой записью до тех пор, пока процесс DRL не очистит эти значения при фактической проверке объекта.

Поскольку DRL — это ресурсоемкий фоновый процесс, то при выполнении очистки другие операции замедляются. Продолжительность процесса очистки зависит от количества объектов и внешних ссылок в системе. Не запускайте часто этот процесс, поскольку он существенно загружает ЦП и память. По умолчанию фоновый процесс Backlinker выполняется в течение 50 минут после запуска ndsd, а затем последовательно выполняется каждые 13 часов.

Очистка вспомогательного класса из записи может занять от 0 до 13 часов; сюда прибавляется время, необходимое для обработки этой записи в системе.

Чтобы разрешить эту проблему, удалите запись вспомогательного класса, вызвав процесс Backlinker через DSTrace или iMonitor.

ПРИМЕЧАНИЕ. При удалении объекта эти значения немедленно удаляются, поскольку это удаление обрабатывается другими фоновыми процессами.

---

12 DSRepair.

12.1 Запуск DSRepair в DIB, смонтированном в файловой системе NFS в Linux

При попытке выполнения операций ndsrepair (DSRepair) в DIB, смонтированном в файловой системе NFS в Linux, могут возникать ошибки -732 или -6009.

12.2 При выполнении команды DSRepair с параметром -R она зависает

После включения шифрования проиндексированных атрибутов команда ndsrepair (DSRepair) с параметром `-R` зависает.

12.3 Выполнение DSRepair после обновления или миграции

При выполнении автоматического процесса DSRepair после обновления или миграции с сервера 8.7.3.x появится сообщение об ошибке `Invalid Ancestor ID list for the entry (Недопустимый список ИД предков для данного элемента).`

Это сообщение можно проигнорировать, поскольку обновление ИД предка выполняется как часть фонового процесса после завершения обновления или миграции DIB.

13 Тиражирование

eDirectory предлагает надежный сервис каталога NetIQ и высокую отказоустойчивость при тиражировании реплик. Тиражирование позволяет хранить копии базы данных eDirectory или ее части одновременно на нескольких серверах.

13.1 Проблемы с зашифрованным тиражированием

13.1.1 Настройка зашифрованного тиражирования с помощью iManager

Настройка зашифрованного тиражирования при помощи iManager невозможна, если в кольце тиражирования отключен какой-либо сервер.

13.1.2 Ошибка слияния деревьев при использовании зашифрованного тиражирования

Если включено зашифрованное тиражирование, объединение деревьев завершается ошибкой. Отключите зашифрованное тиражирование для каждого дерева до начала слияния.

13.2 Восстановление после проблем реплики eDirectory

Вы должны всегда поддерживать несколько реплик разделов eDirectory. В этом случае, если произойдет повреждение одной реплики или ее потеря в результате сбоя жесткого диска, Вы можете удалить эту реплику с помощью ConsoleOne или NetIQ iManager и заменить ее новой неповрежденной репликой.

Дополнительную информацию об удалении реплик см. в разделе "Administering Replicas (Администрирование реплик)" (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html) документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

14 Проблемы при клонировании базы данных Каталога (DIB)

14.1 . Клонирование базы данных Каталога завершается с ошибками -601 и -603

Если на уровне дерева разрешены зашифрованные атрибуты и зашифрованное тиражирование, клонирование DIB завершается со следующими ошибками:

- Клонирование DIB на целевом сервере завершается с ошибкой -601 во время настройки SAS
- После клонирования DIB созданный объект клонирования завершает работу с ошибкой -603

Чтобы обойти эту проблему, запретите зашифрованные атрибуты и зашифрованное тиражирование.

14.2 При клонировании базы данных Каталога (DIB) может произойти сбой сразу после автономной пакетной загрузки

При попытке клонирования сервера сразу после автономной пакетной загрузки может произойти сбой, если пакетная загрузка выполнялась с параметром, отключающим индексы.

Тем не менее, если инициализировать dibclone через несколько часов после завершения пакетной загрузки, то сбоя не будет.

14.3 Проблемы при клонировании с включенной функцией зашифрованного тиражирования

Если клонирование выполняется при включенном шифровании тиражирования на сервере-источнике, настройте политику шифрования тиражирования на временное исключение клонируемого сервера. Это изменение можно отменить по завершении настройки клонируемого сервера.

15 Сервисы инфраструктуры открытых ключей NetIQ

15.1 Операции PKI не работают

Если операции PKI в ConsoleOne или iManager не работают, это может свидетельствовать о том, что NetIQ PKI Services не запущены в Linux. Запустите службы PKI при помощи команды `npki -1`.

Если Вы не можете создать сертификаты, проверьте, правильно ли инсталлирован модуль NICI. См. раздел "Initializing the NICI Module on the Server (Инициализация модуля NICI на сервере)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*. Информацию о том, как проверить инициализацию NICI, см. в разделе "Verifying Whether NICI Is Installed and Initialized on the Server (Проверка установки и инициализации NICI на сервере)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

15.2 Невозможно удалить конфигурацию сервера eDirectory, который работает в качестве сервера ключа дерева в дереве с несколькими серверами, после перемещения существующих объектов eDirectory на другой сервера. Возвращается ошибка для критической реплики.

Чтобы выполнить эту операцию, измените атрибут Key Server DN в объекте W0 ("Security Container (Контейнер защиты)" > "KAP") другим сервером в данном дереве, для которого ключ дерева загружен с этого сервера.

1. В NetIQ iManager нажмите кнопку *Функции и задачи*  .
2. Последовательно выберите пункты *eDirectory Administration (Администрирование eDirectory)* > *Изменить объект*.

3 Укажите имя и контекст объекта W0 (как правило, это W0.KAP.Security) и нажмите кнопку *OK*.

4 В столбце *Атрибуты со значениями* выберите *NDSPKI:SD Key Server DN* и нажмите кнопку *Изменить*.

5 Измените имя и контекст другого сервера в поле *Security Domain Key Server's DN (Характерное имя ключевого сервера домена безопасности)* и нажмите кнопку *OK*.

6 Щелкните *Применить*, затем щелкните *OK*.

15.3 При удалении сервера eDirectory, на котором хранятся центры сертификации, ключевые материальные объекты, созданные на данном сервере, будут перемещены на другой сервер в дереве и станут недействительными.

Для этого дерева нудно повторно создать центр авторизации и ключевые материальные объекты. Дополнительную информацию см. в разделах "Creating an Organizational Certificate Authority Object (Создание объекта центра сертификации организации)" и "Creating a Server Certificate Object (Создание объекта сертификата сервера)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.

Не рекомендуется удалять сервер eDirectory, на котором был создан центр сертификации для данного дерева.

16 Утилиты поиска и устранения проблем в Linux

16.1 Утилита NetIQ Import Convert Export

Если сервер LDAP обновлен или загружен при выполнении операции NetIQ Import Conversion Export на экране появляется сообщение `LBURP operation is timed out (Время ожидания операции LBURP истекло)`. Сервер восстанавливается позже, после истечения времени ожидания операции LBURP.

16.2 Утилита ndsconfig

Содержание этого раздела.

16.2.1 Настройка ndsconfig для запуска из расположения, которое не является расположением по умолчанию

Если при выполнении утилиты ndsconfig из каталога, отличного от каталога по умолчанию (`/opt/novell/eDirectory/bin`) возвращается ошибка, то перед запуском ndsconfig убедитесь в том, что выполнен экспорт ndspath. Используйте команду:

```
source /opt/novell/eDirectory/bin/ndspath
```

После экспорта данной команды введите`ndsconfig` для запуска утилиты ndsconfig вместо `./ndsconfig`.

16.2.2 . Команда ndsconfig не выполняет проверку правильности пути к конфигурационному файлу

Для создания требуемого конфигурационного файла с помощью ndsconfig необходимо указать полный путь к файлу и его имя. Если для конфигурационного файла и каталога экземпляра указан один и тот же путь, то ndsconfig не удается создать файл, и операция прерывается.

16.2.3 . Неправильное отображение неанглийских символов в выходных данных команды ndsconfig get

Команда `ndsconfig get` выводит нежелательные символы в Linux для некоторых параметров, содержащих символы, не входящие в латинский алфавит.

Чтобы решить эту проблему, вводите имена требуемых параметров следующим образом:

`ndsconfig get <параметр_для_вывода>`

Список параметров см. в руководстве по `nds.conf` (файлы man).

16.3 Утилита ndsmerge

Серверы PKI не активны после выполнения операции слияния. Их необходимо перезапустить при помощи команды `npki -l`.

Операции слияния продуктов разных версий могут быть не выполнены. Если на вашем сервере выполняется более старая версия NDS или eDirectory, выполните обновление до последней версии eDirectory, затем продолжите выполнять операции слияния.

Слияние двух деревьев не будет успешным, если контейнеры с одним именем, подчиняющиеся дереву, будут присутствовать как в исходном, так и в целевом деревьях. Переименуйте один из контейнеров и продолжите операцию слияния.

При выполнении операции пересадки может появиться сообщение об ошибке `-611 Illegal Containment`. Измените схему, выполнив `ndsrepair`. Затем запустите `ndsrepair -S` и выберите *Необязательные расширения схемы*.

16.4 Утилита DSTrace

При включении экрана DSTrace может отображаться сообщение об ошибке, указывающее на то, что основной объект недействителен для данной справочной ссылки. Если eDirectory работает правильно, это сообщение можно игнорировать.

16.5 Утилита ndsbackup

При резервном копировании eDirectory может появляться сообщение об ошибке `NDS Error: Connect to NDS server failed (Ошибка NDS: сбой подключения к серверу NDS)`. Эта проблема может быть вызвана тем, что eDirectory принимает информацию на порту,

отличном от порта по умолчанию (524). В командной строке введите номер порта, на котором настроен eDirectory. Например, если eDirectory настроен на порту 1524, введите следующую команду:

```
ndsbackup sR 164.99.148.82:1524
```

В eDirectory 8.8 и более поздней версии при резервном копировании данных может выводится ошибка "NDS Error: Requires a Password (Ошибка NDS: требуется пароль)". Это происходит, поскольку сервер может иметь атрибуты, отмеченные для шифрования, и при этом параметр -E не был использован для шифрования или дешифрования данных резервного копирования.

16.6 Использование DSRepair

Содержание этого раздела.

Используйте утилиту DSRepair в консоли сервера, чтобы выполнять указанные ниже действия.

- Исправлять проблемы eDirectory (например, плохие записи, несоответствия схемы, неверные адреса сервера и внешние ссылки).
- Выполнять дополнительные изменения схемы eDirectory.
- Выполнять указанные ниже операции с базой данных eDirectory.
  - Автоматически проверять структуры базы данных без закрытия базы данных и без вмешательства пользователя.
  - Проверять индексы базы данных.
  - Исправлять базу данных без закрытия базы и блокирования пользователей.
  - Использование свободного пространства за счет удаления пустых записей.

16.6.1 Синтаксис

Для запуска DSRepair используйте следующий синтаксис:

```
ndsrepair {-U| -P| -S| -C| -E| -N| -T| -J entry_id}
[-A yes|no] [-O yes|no] [-F filename] [-Ad]
```

или

```
ndsrepair -R [-l yes|no [-u yes|no] [-m yes|no] [-i yes|no] [-f yes|no] [-d yes|no]
[-t yes|no] [-o yes|no] [-r yes|no] [-v yes|no] [-c yes|no] [-A yes|no] [-O yes|no]
[-F filename]
```

ЗАМЕЧАНИЕ. Опция `-Ad` не должна использоваться без получения предварительного указания от персонала службы поддержки NetIQ.

Параметры DSRepair

Параметр	Описание
-R	Производится исправление локальной базы данных eDirectory. Используйте эту операцию исправления для устранения несоответствий в локальной базе данных, чтобы ее можно было открыть и обратиться к ней из eDirectory. Данный параметр имеет подпараметры, которые облегчают операции исправления базы данных. Он имеет модификаторы функций, которые описаны в разделе "Модификаторы функций, используемые с опцией -R" на стр. 93. Этот параметр без дополнительных вложенных параметров является средством исправления базы данных, если службой поддержки NetIQ не указано выполнить определенные операции вручную.
-P	Операции с репликами и разделами. Отображается список разделов, которые имеют реплики, хранящиеся в файлах базы данных eDirectory текущего сервера. Меню "Параметры реплики" содержит параметры для исправления реплик, отмены операции с разделом, расписания синхронизации и назначения локальной реплики в качестве главной реплики. Дополнительные сведения см. в разделе "Опция "Операции с репликами и разделами"" на стр. 94.
-S	Операции с глобальной Схемой. Данная опция включает несколько операций со схемой, которые могут потребоваться для приведения схемы сервера в соответствие с главной репликой объекта Tree. Однако эти операции следует использовать только тогда, когда это действительно необходимо. Схема уже проверена в ходе выполнения локальных и автоматических операций исправления.
-C	Проверка внешних ссылок. Проверяется каждая внешняя ссылка объекта на возможность определения местоположения реплики, содержащей этот объект. Если все серверы, содержащие реплику раздела, в котором находится данный объект, недоступны, этот объект не будет найден. Если объект невозможно найти, выдается предупреждение.
-E	Отчет о синхронизации реплик. Выдается отчет о статусе синхронизации реплики для каждого раздела, имеющего реплику на текущем сервере. При выполнении этой операции осуществляется чтение атрибута статуса синхронизации из реплики объекта Tree на каждом сервере, содержащем реплики разделов. Отображается время последней успешной синхронизации всех серверов, а также ошибки, возникшие после ее выполнения. Если синхронизация не завершена в течение 12 часов, то выдается предупреждающее сообщение.
-N	Серверы, известные этой базе данных. Отображается список всех серверов, известных этой локальной базе данных eDirectory. Если текущий сервер содержит реплику раздела Tree, сервер отображает список всех серверов в данном дереве eDirectory. Выберите сервер, на котором будут выполнены опции сервера.
-J	Исправление одного объекта на локальном сервере. Вам необходимо будет предоставить ИД элемента (в шестнадцатеричном формате) для объекта, исправление которого будет выполняться. Вы можете использовать этот параметр вместо параметра автоматического исправления (-U) для исправления одного конкретного объекта, который был поврежден. Выполнение опции автоматического исправления может занять несколько часов, в зависимости от размера базы данных. Этот параметр позволяет сэкономить время.

Параметр	Описание
-T	Синхронизации времени. Устанавливается связь с каждым сервером, содержащимся в локальной базе данных eDirectory, и запрашивается информацию о статусе синхронизации времени каждого сервера. Если сервер содержит реплику раздела "Дерево", то будет опрошен каждый сервер в данном дереве eDirectory. Также показывается версия eDirectory, запущенная на каждом сервере.
-A	Добавление данных в существующий файл журнала. Информация добавляется к существующему файлу журнала. По умолчанию этот параметр включен.
-O	Запись выходных данных в файл. По умолчанию этот параметр включен.
-F *имя_файла*	Запись выходных данных в указанный файл.
-U	Автоматическое полное исправление. Указывает утилите DSRepair запустить операцию и выйти без дальнейшего вмешательства со стороны пользователя. Этот параметр блокирует базу данных и обновляет адреса сервера. Вы можете просмотреть файл журнала по завершении процедуры исправления, чтобы определить, какие изменения выполнила утилита DSRepair.

Модификаторы функций, используемые с опцией -R

Изменявший	Описание
-l	Блокирование базы данных eDirectory в процессе операции исправления.
-u	Использование временной базы данных eDirectory в процессе операции исправления.
-m	Сохранение оригинальной неисправленной базы данных.
-i	Проверка структуры и индексов базы данных eDirectory.
-f	Восстановление свободного пространства в базе данных.
-d	Восстановление всей базы данных.
-t	Выполнение проверки структуры дерева. Установите для этой опции значение "Yes" для проверки всех структурных ссылок дерева на предмет их правильного взаимодействия в базе данных. Установите "No", чтобы пропустить проверку. По умолчанию=Yes
-o	Перестройка действующей Схемы.
-r	Исправление всех локальных реплик.
-v	Проверка правильности интерпретируемых пакетных файлов.
-c	Проверка локальных ссылок.

Операции с глобальной Схемой

Чтобы показать список со всеми операциями схемы, которые вы можете выполнить, можно воспользоваться утилитой `ndsrepair -S ([-Ad] дополнительный параметр)`. В следующей таблице представлены доступные параметры.

Параметр	Описание
Request Schema From Master Server (Запросить схему с основного сервера)	Запрашивает главную реплику корня дерева для синхронизации его Схемы с данным сервером. Все изменения в Схеме будут передаваться на этот сервер из главной реплики раздела "Дерево" в течение следующих 24 часов. Если все серверы запросят Схему из главной реплики, может произойти увеличение сетевого трафика.
Переустановка локальной Схемы	Эта параметр вызывает переустановку схемы, которая очищает отметки времени в локальной схеме и запрашивает входящую синхронизацию схемы. Эта опция недоступна для использования из главной реплики раздела "Дерево". Он используется для того, чтобы избежать ситуаций одновременного перезапуска всех серверов в дереве.
Дополнительные изменения Схемы	С помощью этого параметра осуществляется расширение и изменение содержимого Схемы, а также выполняются некоторые другие изменения. Для использования этой опции необходимо, чтобы данный сервер содержал реплику раздела Tree, причем состояние реплики должно быть "Вкл".
Импорт удаленной Схемы (дополнительный ключ)	Выберите дерево eDirectory, содержащее схему, которую Вы хотите добавить к схеме текущего дерева. При выборе дерева происходит обращение к серверу, содержащему главную реплику раздела Tree. Схема этого сервера будет использована для расширения Схемы текущего дерева.
Объявление новой эпохи (дополнительный ключ)	При объявлении новой эпохи Схемы осуществляется взаимодействие с главной репликой раздела "Дерево" и исправление недействительных отметок времени, объявленных на этом сервере. Все другие серверы получат новую копию данной схемы, включая исправленные отметки времени. Если сервер-получатель содержит схему, которая не входила в новую эпоху, объекты и атрибуты, использующие старую схему, станут объектами и атрибутами класса "Неизвестный".

Опция "Операции с репликами и разделами"

Для отображения информации о каждой реплике, хранящейся на сервере, введите следующую команду:

```
ndsrepair -P
```

Выберите нужную реплику. Отобразятся параметры, которые перечислены ниже.

- Исправление всех реплик

Производится исправление всех реплик, показанных в таблице реплик.

- Исправление выбранной реплики

  Производится исправление только выбранной реплики из таблицы реплик.

ЗАМЕЧАНИЕ. Исправление реплики состоит в проверке каждого объекта реплики на совместимость со Схемой и данными в соответствии с синтаксисом этого атрибута. Также проверяются другие внутренние структуры данных, ассоциированные с репликой. Если операция исправления локальной базы данных eDirectory не выполнена в течение последних 30 минут, это следует сделать до исправления любых реплик.

- Планирование немедленной синхронизации

  Выполняется планирование немедленной синхронизации всех реплик. Эта опция полезна, если вы, например, наблюдаете экран DSTrace и хотите просмотреть информацию о процессе синхронизации eDirectory, не дожидаясь ее обычного запланированного запуска.

- Отмена операции с разделом

  Производится отмена операции с выбранным разделом. Эта опция может быть полезной, когда не удалось завершить операцию из-за проблем в дереве DSTrace, например, из-за отсутствия сервера или плохих коммуникаций. Некоторые операции невозможно отменить, если их выполнение находится в финальной стадии.

- Назначение данного сервера новой главной репликой

  Локальная реплика выбранного раздела назначается в качестве новой главной реплики. Используйте эту операцию для назначения новой главной реплики, если исходная потеряна.

- Отчет о статусе синхронизации всех серверов

  Сообщается о статусе синхронизации реплик всех разделов на текущем сервере. Отображается время последней успешной синхронизации всех серверов, а также ошибки, возникшие после ее выполнения.

- Синхронизация реплики на всех серверах

  Определяется статус полной синхронизации на каждом сервере, содержащем реплику выбранного раздела. Это помогает определить состояние раздела. Если все серверы, имеющие реплику этого раздела, синхронизированы правильно, то раздел находится в нормальном состоянии. Каждый сервер выполняет немедленную синхронизацию со всеми другими серверами в кольце реплик. Серверы не синхронизируются сами с собой. Поэтому статус собственных реплик текущего сервера отображается как "Хост".

- Исправление кольца, все реплики

  Производится исправление колец реплик, в которые входят все реплики, отображенные в таблице реплик.

- Исправление кольца, выбранная реплика

  Производится исправление кольца реплик, в которое входит выбранная реплика, отображенная в таблице реплик.

ЗАМЕЧАНИЕ. Процедура исправления кольца реплик состоит из проверки информации кольца реплик на каждом сервере, содержащем реплику данного раздела, и проверки информации удаленного ИД. Если операция исправления локальной базы данных eDirectory не выполнена в течение последних 30 минут, это следует сделать до исправления всех или только выбранных колец. Исправить локальную базу можно с помощью опции `-R`. Дополнительные сведения см. в разделе "-R" на стр. 92.

- Просмотр кольца реплик

Отображается список всех серверов, содержащих реплику выбранного раздела. Этот набор серверов называется кольцом реплик. Список кольца реплик предоставляет информацию о типе реплики и ее текущем статусе для каждого отдельного сервера кольца. Для возможности просмотра параметров сервера необходимо из кольца реплик выбрать сервер.

Опции сервера

- Отчет о статусе синхронизации выбранного сервера

  Выдается отчет о статусе синхронизации реплики для выбранного раздела, имеющего реплику на выбранном сервере. При выполнении этой операции осуществляется чтение атрибута статуса синхронизации из реплик объекта "Дерево" на каждом сервере, содержащем реплики разделов. Отображается время последней успешной синхронизации всех серверов, а также ошибки, возникшие после ее выполнения. Эта опция выдает предупреждающее сообщение, если синхронизация не завершена в течение 12 часов.

- Синхронизация реплики на выбранном сервере

  Определяется статус полной синхронизации на выбранном сервере, содержащем реплику выбранного раздела. Это помогает определить состояние раздела. Если сервер, содержащий реплику этого раздела, синхронизирован правильно, то раздел находится в нормальном состоянии. Выполняется немедленная синхронизация данного сервера с каждым сервером кольца реплик. Сервер не может синхронизироваться сам с собой. Поэтому статус собственной реплики текущего сервера отображается как "Хост".

- Передать все объекты каждой реплике в кольце

  Осуществляется передача всех объектов из выбранного сервера в кольце реплик на все другие серверы, содержащие реплику этого раздела. При выполнении этой операции может произойти значительное увеличение сетевого трафика. Используйте эту опцию, чтобы проверить, синхронизирована ли реплика выбранного раздела на выбранном сервере кольца реплик со всеми другими серверами в кольце реплик. Эту операцию нельзя выполнить на сервере, который содержит только реплику подчиненной ссылки данного раздела.

- Получить все объекты из главной реплики в данную реплику

  Обеспечивается получение всех объектов от главной реплики в реплику, находящуюся на выбранных серверах. При выполнении этой операции может произойти значительное увеличение сетевого трафика. Используйте эту опцию, чтобы проверить, синхронизирована ли с главной репликой реплика выбранного раздела на выбранном сервере в кольце реплик. Эту операцию нельзя выполнить на сервере, содержащем главную реплику.

- Просмотр полного имени сервера

  Используется для просмотра полного имени сервера, если его имя слишком длинное и не умещается в таблице серверов.

- Удаление данного сервера из кольца реплик

  (Дополнительная опция). Выполняется удаление выбранного сервера из указанной реплики, хранящейся на текущем сервере. Если в кольце реплик появился сервер, который больше не является частью дерева eDirectory или больше не содержит реплику данного раздела, с помощью утилиты iManager удалите соответствующий ему объект "Сервер". Как только объект "Сервер" будет удален, соответствующий ему объект будет исключен из кольца реплик.

ПРЕДУПРЕЖДЕНИЕ. Некорректное использование этой операции может явиться причиной неисправимого повреждения базы данных eDirectory. Используйте этот параметр только после инструктажа со стороны персонала технической поддержки NetIQ.

- Просмотр полного имени раздела

  Используется для определения полного характерного имени раздела, если его имя слишком длинное и не умещается в таблице реплик.

- Исправление отметок времени и объявление новой эпохи

  (Дополнительная опция). Обеспечивается новая точка отсчета для главной реплики таким образом, что все обновления реплик выбранного раздела становятся текущими. Данная операция выполняется над главной репликой раздела. Главная реплика необязательно должна быть локальной репликой данного сервера. Отметки времени, устанавливаемые на объекты, определяют, когда объекты были созданы или изменены, эти отметки должны быть уникальными. Проверяются все отметки времени в главной реплике. Если какие-либо отметки времени датированы более поздним числом по отношению к текущему времени сети, они заменяются на новые.

- Уничтожение выбранной реплики на данном сервере

  (Дополнительная опция). Удаляется выбранная реплика на данном сервере. Использвоание этого параметра не рекомендуется. Эту опцию рекомендуется использовать только в том случае, если все другие утилиты не могут удалить реплику.

- Удаление конечных объектов "Неизвестный"

  (Параметр дополнительного ключа). Удаляются все объекты локальной базы данных eDirectory, относящиеся к классу "Неизвестный" и не содержащие в себе других объектов. Этот параметр отмечает объекты "Неизвестный" для удаления. Позднее это удаление будет синхронизировано с другими репликами в данном дереве eDirectory.

ПРЕДУПРЕЖДЕНИЕ. Используйте эту опцию только в том случае, если объекты нельзя изменить или удалить с помощью ConsoleOne или iManager.

Опции для серверов, известных этой базе данных

Для серверов имеются следующие опции исправления:

- Исправление всех сетевых адресов

  Проверка сетевого адреса каждого сервера в локальной базе данных eDirectory. В зависимости от используемого транспортного протокола этот параметр выполняет поиск агента каталога SLP для каждого имени сервера. Затем каждый адрес сравнивается со свойством "Сетевой адрес" объекта "Сервер" и записью адреса в каждом свойстве "Реплика" каждого объекта раздела "Дерево". Если адреса различаются, то они изменяются для полного соответствия друг другу.

- Исправление сетевого адреса выбранного сервера

  Осуществляет проверку сетевого адреса указанного сервера в файлах локальной базы данных eDirectory. В зависимости от используемых в данный момент транспортных протоколов, этот параметр выполняет поиск агента каталога SLP для данного имени сервера.

- Просмотр полного имени сервера

  Отображается полное имя сервера в том случае, когда это имя слишком длинное и не умещается в таблице серверов. Эта опция аналогична опции "-P". Дополнительные сведения см. в разделе "-P" на стр. 92.

Примеры

Для выполнения автоматического исправления и записи событий в файл `/root/ndsrepair.log` или для добавления событий в существующий файл журнала введите следующую команду:

```
ndsrepair -U  -A no -F /root/ndsrepair.log
```

Для отображения списка всех операций с глобальной Схемой вместе с дополнительными опциями введите следующую команду:

```
ndsrepair -S -Ad
```

Для исправления локальной базы данных посредством принудительной блокировки базы данных введите следующую команду:

```
ndsrepair -R -l yes
```

ПРИМЕЧАНИЕ. Ввод утилиты `ndsrepair` можно переназначить на файл параметров. Этот файл параметров — это текстовый файл, который содержит параметры, в отношении операций с репликами и разделами, а также вложенные параметры, для которых не требуется аутентификация сервера. Все параметры или вложенные параметры разделены новой строкой. Удостоверьтесь, что содержимое файла приведено в правильном порядке. Если порядок будет нарушен, результаты могут быть непредсказуемыми.

16.6.2 Поиск и устранение проблем DSRepair

Error -786 While Running DSRepair

При использовании DSRepair необходимо иметь пространство в три раза большее, чем размер DIB, на определенном разделе вашего компьютера, в котором будет выполняться DSRepair.

16.7 Использование DSTrace

Чтобы использовать утилиту DSTrace в среде Linux выполните следующую команду из командной строки сервера:

```
/opt/novell/eDirectory/bin/ndstrace
```

Полный синтаксис команды ndstrace:

```
ndstrace [-l|-u|-c "command1;....."|--version] [-h <local_interface:port>] [--
config-file <configuration_file_path>] [thrd <thread ID>] [svty <severity_level>]
[conn <connection_ID>]
```

Утилита DSTrace состоит из трех главных частей.

- "Основные функции" на стр. 99
- "Отладочные сообщения" на стр. 100
- "Фоновые процессы" на стр. 102

16.7.1 Основные функции

К основным относятся указанные ниже функции DSTrace.

- Просмотр действий eDirectory и сообщений отладки в Linux.
- Инициализация процессов ограниченной синхронизации.

Можно использовать утилиту DSTrace в режиме интерфейса пользователя или в режиме командной строки. По умолчанию DSTrace выполняется в режиме интерфейса пользователя. Чтобы запустить DSTrace в режиме интерфейса пользователя, в командной строке сервера введите следующую команду:

```
/opt/novell/eDirectory/bin/ndstrace
```

Чтобы запустить DSTrace в режиме командной строки, в командной строке сервера введите следующую команду:

```
/opt/novell/eDirectory/bin/ndstrace -l
```

Для инициализации основных функций DSTrace введите команды с консоли сервера, используя следующий синтаксис:

```
ndstrace command_option
```

В следующей таблице перечислены параметры команды, доступные для использования.

Параметр	Описание
ON	Запуск экрана трассировки eDirectory с отображением основных сообщений трассировки.
OFF	Запрещение отображения экрана трассировки.
ALL	Запуск экрана трассировки eDirectory и отображение всех сообщений трассировки.
AGENT	Запуск экрана трассировки eDirectory с отображением сообщений трассировки, эквивалентных флагам ON, BACKLINK, DSAGENT, JANITOR, RESNAME и VCLIENT.
DEBUG	Включение предопределенного набора сообщений трассировки, обычно используемых для отладки. Устанавливаются следующие флаги: ON, BACKLINK, ERRORS, EMU, FRAGGER, INIT, INSPECTOR, JANITOR, LIMBER, MISC, PART, RECMAN, REPAIR, SCHEMA, SKULKER, STREAMS и VCLIENT.
NODEBUG	Оставляет включенным экран трассировки, но выключает все предустановленные сообщения отладки. Эта параметр также позволяет оставить сообщения, установленные командной опцией ON.

16.7.2 Отладочные сообщения

Когда экран DSTrace включен, отображаемая информация базируется на установленном по умолчанию наборе фильтров. Если Вы хотите просматривать больше или меньше, чем это установлено по умолчанию, можно настроить фильтры с помощью установки флагов сообщений отладки. Сообщения отладки полезны при определении статуса eDirectory и проверке правильности функционирования системы.

У каждого процесса eDirectory есть набор сообщений отладки. Для просмотра сообщений отладки конкретного процесса используйте знак плюс (+) и имя процесса или опцию. Для запрещения отображения процесса используйте знак минус (-) и имя процесса или опцию. Далее приводятся некоторые примеры.

Сообщение	Описание
`set ndstrace = +SYNC`	Разрешение отображения сообщений синхронизации.
`set ndstrace = -SYNC`	Запрещение отображения сообщений синхронизации.
`set ndstrace = +SCHEMA`	Разрешение отображения сообщений Схемы.

Вы можете также комбинировать флаги сообщений отладки с помощью логических операторов & (логическое "И" - "AND") и (логическое "ИЛИ" - "OR"). Далее приводятся примеры синтаксиса, с помощью которого с консоли сервера можно контролировать сообщения отладки.

`set ndstrace = <trace_flag> [parameter]`

В приведенной ниже таблице описываются флаги трассировки сообщений отладки. Допускается вводить аббревиатуры для каждого из флагов трассировки.

Флаг трассировки	Описание
ABUF	Сообщения и информация, относящиеся к буферам входящих и исходящих пакетов, которые содержат данные, получаемые в запросах к каталогу eDirectory или в ответах от него.
ALOC	Сообщения, в которых показано распределение памяти.
AREQ	Сообщения, связанные со входящими запросами от других серверов или клиентов.
AUTH	Сообщение и отчеты об ошибках, относящиеся к аутентификации.
BASE	Отладочные сообщения об ошибках на минимальном отладочном уровне.
BLNK	Сообщение об обратных ссылках и входящих значениях устаревшего состояния, а также отчеты об ошибках.
CBUF	Сообщения, относящиеся к исходящим запросам клиента DS.
CHNG	Сообщения изменения кэша.
COLL	Отчеты о статусе и ошибках, относящиеся к информации обновления объектов, когда это обновление уже было получено ранее.

Флаг трассировки	Описание
CONN	Сообщения, в которых показана информация о серверах, к которым пытается подключиться ваш сервер, а также об ошибках и истечении времени ожидания, что может служить причиной проблем с подключением сервера.
DNS	Сообщения о процессах интегрированного с eDirectory сервера DNS.
DRLK	Сообщения, которые относятся к распределенным справочным ссылкам.
DVRS	Сообщения, в которых отображаются области драйвера DirXML®, на которых может работать eDirectory.
DXML	Сообщения, в которых отображается подробная информация о событиях DirXML.
FRAG	Сообщения от модуля NCP™ fragger, который разбивает сообщения eDirectory на сообщения с размером, пригодным для NCP.
IN	Сообщения, которые относятся к входящим запросам и процессам.
INIT	Сообщения, которые относятся к инициализации eDirectory.
INSP	Сообщения, которые относятся к целостности объектов в локальной базе данных исходного сервера. При использовании этого флага возрастают требования к дисковой подсистеме, памяти и процессору исходного сервера. Включайте этот флаг только в случае, если начали появляться поврежденные объекты.
JNTR	Сообщения, которые относятся к следующим фоновым процессам: janitor, replica synchronization и flat cleaner.
LDAP	Сообщения, которые относятся к серверу LDAP.
LMBR	Сообщения, которые относятся к процессу Limber.
LOCK	Сообщения, которые относятся к использованию и изменению блокировок локальной базы данных исходного сервера.
LOST	Сообщения, которые относятся к записям журнала.
MISC	Сообщения из разных источников в eDirectory.
MOVE	Сообщения от операций по перемещению раздела или перемещению поддерева.
NCPE	Сообщения, в которых показан сервер, получающий запросы на уровне NCP.
NMON	Сообщения, которые относятся к iMonitor.
OBIT	Сообщения от процесса устаревших состояний.
PART	Сообщения, которые относятся к операциям с разделом от фоновых процессов или от обработки запросов.
PURG	Сообщение о процессе очистки.
RECM	Сообщения, которые относятся к изменению базы данных исходного сервера.
RSLV	Отчеты, которые относятся к обработке разрешения запросов имени.

Флаг трассировки	Описание
SADV	Сообщения, которые относятся к регистрации имен и разделов дерева с использованием Service Location Protocol (SLP).
SCMA	Сообщения, которые относятся к процессу синхронизации схемы.
SCMD	Сообщения, в которых показана подробная информация об операциях, относящихся к схеме. Предоставляется подробная информация как о входящей, так и исходящей синхронизации.
SKLK	Сообщения, которые относятся к процессу синхронизации реплики.
SPKT	Сообщения, которые относятся к информации уровня сервера eDirectory NCP.
STRM	Сообщения, которые относятся к обработке атрибутов с синтаксисом потока.
SYDL	Сообщения, в которых показан более подробная информация во время процесса репликации.
SYNC	Сообщения о входящем трафике синхронизации (полученные сервером данные).
TAG	Показывает строку тега, которая определяет параметр трассировки, вызвавший событие в каждой строке, отображенной процессом трассировки.
THRD	Сообщения, в которых отображается время начала или завершения любых фоновых процессов (потоков).
TIME	Сообщения о транзитивных векторах, используемых в процессе синхронизации.
TVEC	Сообщения, которые относятся к следующим атрибутам: Synchronize Up To, Replica Up To, и Transitive Vector.
VCLN	Сообщения, которые относятся к установке или удалению подключений к другим серверам.

Работая с сообщениями отладки в DSTrace, вы убедитесь, что некоторые флаги трассировки более полезны, нежели другие. Одним из любимых настроек DSTrace группы техподдержки NetIQ является ярлык:

```
set ndstrace = A81164B91
```

Эта настройка включает группу отладочных сообщений.

16.7.3 Фоновые процессы

Кроме отладочных сообщений, помогающих Вам проверить состояние eDirectory, существует набор команд, которые выполняют принудительный запуск фоновых процессов eDirectory. Для принудительного запуска фонового процесса поместите перед командой звездочку (*). Например:

```
set ndstrace = *H
```

Кроме того, Вы можете изменить состояние, синхронизацию нескольких фоновых процессов и управление ими. Для изменения этих параметров поместите восклицательный знак (!) перед командой и введите новый параметр или значение. Например:

```
set ndstrace = !H 15 (parameter_value_in_minutes)
```

Ниже представлен синтаксис каждого оператора, управляющего фоновыми процессами eDirectory.

```
set ndstrace = <trace_flag> [parameter]
```

В следующей таблице перечислены флаги трассировки для фоновых процессов и требуемые для них параметры, а также приведены описания происходящих при этом процессов.

Флаг трассировки	Параметры	Описание
*A	Нет	Сброс кэша адресов на исходном сервере.
*AD	Нет	Отключение кэша адресов на исходном сервере.
*AE	Нет	Включение кэша адресов на исходном сервере.
*B	Нет	Планирует запуск на исходном сервере процесса обратной ссылки (backlink) через одну секунду.
!B	Время	Устанавливает интервал (в минутах) для процесса backlink. По умолчанию=1500 минут (25 часов) Диапазон=2 до 10080 минут (168 часов)
*CT	Нет	Отображает таблицу исходящих соединений исходного сервера и текущую статистическую информацию для этой таблицы. Эта статистика не дает какой-либо информации о входящих соединениях, поступающих на сервер от других серверов или клиентов.
*CTD	Нет	Отображает таблицу (с использованием запятой в качестве разделителя) исходящих соединений исходного севера и текущую статистическую информацию для этой таблицы. Эта статистика не дает какой-либо информации о входящих соединениях, поступающих на сервер от других серверов или клиентов.
*D	ИД корневого элемента (rootEntry) реплики	Удаляет указанный ИД локального элемента из списка объекта "Отправить всем" исходного сервера. ИД элемента должен указывать объект корня раздела, относящийся к локальной базе данных сервера. Данная команда обычно используется только в случае, когда процесс "Send All Updates (Отправить обновления всем)" не прекращает попытки показать обновления, которые не удается выполнить из-за недоступности сервера.
!D	Время	Устанавливает значение интервала входящей и исходящей синхронизации в соответствии с указанным количеством минут. По умолчанию=24 минуты. Диапазон=от2 до 10080 минут (168 часов)
!DI	Время	Устанавливает значение интервала входящей синхронизации в соответствии с указанным количеством минут. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)

Флаг трассировки	Параметры	Описание
!DO	Время	Устанавливает значение интервала исходящей синхронизации в соответствии с указанным количеством минут. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)
*E	Нет	Повторная инициализация кэша элементов исходного сервера.
!E	Нет	Планирует начало запуска процессов входящей и исходящей синхронизации.
!EI	Нет	Планирует начало запуска процесса входящей синхронизации.
!EO	Нет	Планирует начало запуска процесса исходящей синхронизации.
*F	Нет	Планирует запуск на исходном сервере процесса Flat Cleaner, который является частью процесса janitor, через 5 секунд.
!F	Время	Устанавливает интервал (в минутах) для процесса Flat Cleaner. По умолчанию=240 минут (4 часа) Диапазон=2 до 10080 минут (168 часов)
*FL	1-10	Задает количество последовательных файлов журнала, которые используются процессом DSTrace. Если задать этому параметру любое значение больше 1, то после того как размер файла `ndstrace.log` на исходном сервере достигнет настроенного максимального предела, DSTrace переименует файл `ndstrace1.log` и создать новый файл `ndstrace.log`. Когда размер файла достигнет максимального, предыдущий файл `ndstrace1.log` переименовывается в `ndstrace2.log`, а более новый файл `ndstrace.log` переименовывается в `ndstrace1.log`. Этот процесс продолжается до тех пор, пока DSTrace не достигнет максимального количества последовательных файлов журнала, которые задаются этим параметром. После достижения указанного лимита, самые старые файлы журнала будут удалены. Будет поддерживаться только максимальное количество последовательных файлов. Можно настроить не более 10 последовательных файлов журнала. По умолчанию в DSTrace должен использоваться хотя бы 1 последовательный файл журнала. Если задать этому параметру значение 0, DSTrace использует значение 1 в качестве значения параметра.
*G	ИД корневого элемента (rootEntry) реплики	Заново создает кэш изменений указанного ИД корневого раздела.

Флаг трассировки	Параметры	Описание
*H	Нет	Планирует немедленный запуск процесса синхронизации реплик на исходном сервере.
!H	Время	Устанавливает интервал (в минутах) для процесса синхронизации "heartbeat". По умолчанию=30 минут Диапазон=от 2 до 1440 минут (24 часа)
*HR	Нет	Удаляет из памяти последний отправленный вектор.
*I	ИД корневого элемента (rootEntry) реплики	Добавляет указанный ИД локальной записи в список объекта "Отправить всем" исходного сервера. ИД элемента должен указывать объект корня раздела, относящийся к локальной базе данных сервера. В процессе синхронизации реплик происходит проверка списка объекта "Отправить всем". Если ИД элемента объекта корневого раздела имеется в списке, eDirectory синхронизирует все объекты и атрибуты в разделе, независимо от значения атрибута синхронизации реплики.
!I	Время	Устанавливает интервал (в минутах) для процесса синхронизации "heartbeat". По умолчанию=30 минут Диапазон=от 2 до 1440 минут (24 часа)
*J	Нет	Планирует запуск на исходном сервере процесса очистки, который является частью процесса синхронизации реплик.
!J	Время	Устанавливает интервал (в минутах) для процесса janitor. По умолчанию=2 минуты Диапазон=от 1 до 10080 минут (168 часов)
*L	Нет	Планирует выполнение на исходном сервере процесса limber через 5 секунд.
*M	Байты	Изменяет максимальный размер файла, используемый файлом журнала `ndstrace.log` исходного сервера. Эту команду можно использовать независимо от состояния файла отладки. Для данного параметра нужно указать значение между 10000 байтами и 100 МБ. Если указанное значение находится за пределами интервала, изменение не выполняется.
!M	Нет	Создает отчет о максимальной памяти, используемой eDirectory.
!N	0|1	Устанавливает формат имени. 0=только шестнадцатиричный формат 1=форма полной точки
*P	Нет	Отображение настраиваемых параметров и их значений по умолчанию.

Флаг трассировки	Параметры	Описание
*R	Нет	Сбрасывает размер файла `ndstrace.log` в нуль байт. Данная команда аналогична параметру SET "NDS Trace File Length Set to Zero".
*S	Нет	Планирование процесса Skulker, который проверяет, нужно ли синхронизировать какие-либо реплики на сервере.
!SI	Время	Устанавливает интервал (в минутах) для процесса входящей синхронизации схемы. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)
!SO	Время	Устанавливает интервал (в минутах) для процесса исходящей синхронизации схемы. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)
!SIO	Время	Запрещает процесс входящей синхронизации в течение указанного количества минут. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)
!SO0	Время	Запрещает процесс входящей синхронизации в течение указанного количества минут. По умолчанию=24 минуты Диапазон=от 2 до 10080 минут (168 часов)
*SS	Нет	Принудительная немедленная синхронизация Схемы.
*SSA	Нет	Планирует немедленный запуск процесса синхронизации Схемы и вызывает синхронизацию Схемы на всех целевых серверах, даже если они были синхронизированы в течение последних 24 часов.
*SSD	Нет	Сбрасывает список целей синхронизации схемы исходного сервера. Этот список определяет, с какими серверами должен синхронизироваться исходный сервер во время выполнения процесса синхронизации Схемы. Сервер, не содержащий ни одной реплики, отправляет запрос на включение его в целевой список серверов, содержащих реплики с его объектом "Сервер".
*SSL	Нет	Отображает список синхронизации Схемы целевых серверов.
*ST	Нет	Отображает информацию о статусе фоновых процессов на исходном сервере.
*STX	Нет	Отображает информацию о статусе процесса обратной ссылки backlink (внешние ссылки) на исходном сервере.
*STS	Нет	Отображает информацию о статусе процесса синхронизации схемы на исходном сервере.

Флаг трассировки	Параметры	Описание
*STO	Нет	Отображает информацию о статусе процесса обратной ссылки backlink (значения устаревшего состояния) на исходном сервере.
*STL	Нет	Отображает информацию о статусе процесса limber на исходном сервере.
!T	Время	Устанавливает интервал (в минутах) для проверки состояния работоспособности севера. По умолчанию=30 минут Диапазон=от 1 до 720 минут (12 часов)
*U	Дополнительный ИД сервера	Если команда не содержит ИД элемента, она изменяет статус любого ранее отмеченного сервера с **закрытого (down)** на открытый **(up)**. Если команда содержит ИД локального элемента, она изменяет статус указанного сервера с **выключен** на **включен**. ИД элементов являются специфическими для базы данных исходного сервера и должны указывать на объект, представляющий сервер.
!V	Список	Выводит список версий eDirectory, ограниченных для использования. Если ни одна версия не выведена, это означает, что ограничений на использование нет. Каждая версия отделяется запятой.
*Z	Нет	Отображает текущие запланированные задачи.

17 NMAS в Linux

17.1 Не удается войти, используя любой метод

После установки и настройки NMAS перезапустите сервер eDirectory.

После переустановки метода с предшествовавшим удалением предыдущего экземпляра этого метода, перезапустите сервер eDirectory.

17.2 Пользователь, добавленный с использованием утилиты ICE, не может войти, используя простой пароль

При добавлении пользователей с простыми паролями при помощи утилиты NetIQ Import Conversion Export используйте параметр `-l`.

18 Поиск и устранение проблем в Windows

18.1 Сервер eDirectory for Windows не запускается

Если в процессе загрузки сервера Windows произойдет сбой при запуске сервера eDirectory, будет выдано сообщение о том, что произошел сбой при запуске службы.

При отсутствии других реплик базы данных eDirectory пользователи не могут войти.

Если существуют другие реплики, то регистрация может быть медленной и возможны коммуникационные ошибки, а также ошибки синхронизации на серверах, хранящих эти реплики.

- Могли быть изменены элементы сервера eDirectory в реестре Windows, или может быть поврежден реестр Windows.
- Файлы базы данных eDirectory могут быть повреждены или удалены.
- Если сервер eDirectory не запускается из-за того, что не запущена какая-либо служба, дополнительную информацию можно получить, последовательно выбрав пункты *Пуск* > *Программы* > *Администрирование (Общее)* > *Просмотр событий*.

  Вам придется устранить проблему, связанную с этой службой, перед запуском сервера eDirectory.
- Исполнимые файлы реестра или eDirectory повреждены или потеряны. Запустите утилиту SAMMIG в системном каталоге. Выберите *Uninstall NDS on Windows NT (Удалить NDS в Windows NT)* и включить новую информацию о eDirectory в домен NT. Продолжите процесс удаления до его завершения. После этого перезапустите `sammig.exe` и продолжите установку eDirectory.

- Файлы базы данных повреждены или удалены. Если сервер eDirectory загружается на сервере NT, однако при этом данный сервис не может открыть файлы базы данных eDirectory, см.Раздел 18.2, "Сервер Windows не может открыть файлы базы данных eDirectory" на стр. 112.
- Сервер eDirectory не подключен напрямую к концентратору или коммутатору либо к рабочей станции (с использованием перекрестного кабеля). Соедините сервер с концентратором или коммутатором.

18.2 Сервер Windows не может открыть файлы базы данных eDirectory

Если сервер eDirectory не может открыть файлы базы данных, будет выдано сообщение об этом на сервере Windows.

При отсутствии других реплик базы данных пользователи не могут войти.

Если существуют другие реплики, то регистрация может быть медленной и возможны коммуникационные ошибки, а также ошибки синхронизации на серверах, хранящих эти реплики.

- Файлы базы данных могут быть повреждены из-за дисковых ошибок на сервере NT/2000.
- Кто-то мог удалить один или несколько файлов базы данных.

Если существуют другие реплики базы данных eDirectory, выполните указанные ниже действия.

1. Запустите NetIQ iManager с административной рабочей станции.
2. Удалите поврежденную реплику из кольца реплик.

   Дополнительную информацию см. в разделе "Deleting a Replica (Удаление реплики)" документа *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)*.
3. Запустите утилиту `sammig.exe` в системном каталоге, который на сервере NT имеет путь `c:\winnt\system32` или воспользуйтесь меню *Пуск*.
4. Выберите параметр для создания новой реплики на сервере eDirectory.

Если сервер eDirectory содержит единственную реплику раздела, выполните указанные ниже действия.

1. Запустите утилиту `sammig.exe` в системном каталоге, который на сервере NT имеет путь `c:\winnt\system32` или воспользуйтесь меню *Пуск*.
2. Выберите *Uninstall NDS (Удалить NDS)* для возвращения домена Windows в прежнее состояние.
3. Продолжите процесс удаления до его завершения.
4. Перезапустите инструмент миграции и продолжите установку в Windows.
5. Перенесите объекты `Пользователь` из домена NT в дерево eDirectory.

18.3 SLP_NETWORK_ERROR(-23) происходит на компьютерах Windows

Запрос протокола обнаружения сервисов SLP возвращает -23 SLP_NETWORK_ERROR на виртуальном компьютере с адресом DHCP или на физическом либо виртуальном компьютере, на котором широковещательная передача SLP не выполняется.

Чтобы избежать ошибки SLP, настройте Directory Agent в своей сети одним из указанных ниже способов.

1. Скопируйте файл `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` в каталог `c:\Windows\`.
2. Откройте файл `slp.conf`, используя текстовый редактор, и измените следующую строку:

   ```
   ;net.slp.DAAddresses = myDay1,myDa2,myDa3
   ```

   на

   ```
   net.slp.DAAddresses = <Give your DA Address>
   ```

3. Сохраните изменения, затем закройте файл.

ИЛИ

1. Скопируйте файл `C:\Windows\System32\Novell\eDir\OpenSLP\slp.conf` в каталог `c:\Windows\`.
2. Откройте файл `slp.conf`, используя текстовый редактор, и измените следующую строку:

   ```
   ;net.slp.isDA = true
   ```

   на

   ```
   net.slp.isDA = true
   ```

3. Сохраните изменения, затем закройте файл.

18.4 При установке eDirectory на странице обзора отображается неправильный путь установки

Укажите нужный путь вручную.

18.5 Если SLP не настроен правильно в Windows, то при добавлении сервера происходит сбой

Не удается выполнить установку eDirectory при добавлении сервера в дерево (в котором нужно выполнить обзор текущего дерева), если SLPD уже установлен и запущен. В Windows отображается сообщение *launch.exe died*.

Чтобы успешно установить eDirectory, выполните указанные ниже действия без перезагрузки системы.

1. Остановите сервис протокола обнаружения сервисов.
2. Удалите файл `C:\Windows\slp.conf`.

3 Удалите папку `C:\Windows\System32\Novell\eDir\OpenSLP`.

4 Удалите ключи реестра для сервиса SLPD из `Registry HKLM\SYSTEM\CurrentControlSet\Services\slpd`.

5 Выполните программу настройки заново с ролью администратора.

19 Доступ к HTTPSTK, если DS не загружен

Можно настроить предварительно сконфигурированного пользователя-администратора, которые разрешит доступ к стеку протоколов HTTP (HTTPSTK), если DS не загружен. Предварительно настроенный административный пользователь sadmin имеет права, которые эквиваленты объекту "Административный пользователь eDirectory". Если данный сервер находится в таком состоянии, которое обусловливает неправильную работу eDirectory, вы можете войти на сервер от имени этого пользователя и выполнить все необходимые задания диагностики и отладки, для которых не требуется eDirectory.

19.1 Установка пароля пользователя sadmin в Windows

Воспользуйтесь страницей удаленного менеджера DHost (доступна по URL-адресу `/dhost` или с корневой страницы), чтобы задать пароль sadmin. Чтобы можно было установить или изменить пароль пользователя sadmin, на сервере eDirectory должен выполняться файл`dhost.exe`.

1. Откройте веб-навигатор.
2. В поле адреса (URL) введите следующее:

   `http://`*`server.name`*`:`*`port`*`/dhost`

   Например:

   `http://MyServer:80/dhost`

   Для доступа к DHost iConsole можно также использовать IP-адрес сервера. Например:

   `http://137.65.135.150:80/dhost`
3. Укажите имя пользователя, контекст и пароль.
4. Щелкните *HTTP Server (Сервер HTTP)*, затем укажите пароль sadmin.
5. Проверьте указанный пароль и нажмите кнопку *Отправить*.

19.2 Установка пароля пользователя sadmin в Linux

Можно использовать страницу удаленного управления DHost или утилиту ndsconfig.

Страница удаленного управления DHost

Воспользуйтесь страницей удаленного менеджера DHost (доступна по URL-адресу `/dhost` или с корневой страницы), чтобы задать пароль sadmin. Чтобы можно было установить или изменить пароль пользователя sadmin, на сервере eDirectory должен выполняться сервер NetIQ eDirectory.

1. Откройте веб-навигатор.
2. В поле адреса (URL) введите следующее:

   `http://server.name:port/dhost`

   Например:

   `http://MyServer:80/dhost`

   Для доступа к DHost iConsole можно также использовать IP-адрес сервера. Например:

   `http://137.65.135.150:80/dhost`
3. Укажите имя пользователя, контекст и пароль.
4. Щелкните *HTTP Server (Сервер HTTP)*, затем укажите пароль sadmin.
5. Проверьте указанный пароль и нажмите кнопку *Отправить*.

ndsconfig

Чтобы задать пароль sadmin, воспользуйтесь утилитой ndsconfig. Чтобы можно было установить или изменить пароль пользователя sadmin, на сервере eDirectory должен выполняться ndsd.

С консоли сервера введите следующую команду

`ndsconfig set http.server.sadmin-pwd=пароль`

где *пароль* — это новый пароль sadmin.

Дополнительную информацию об использовании утилиты ndsconfig, см. в разделе "ndsconfig Utility Parameters (Параметры утилиты ndsconfig)" документа *NetIQ eDirectory 8.8 SP8 Installation Guide (Руководство по установке NetIQ eDirectory 8.8 SP8)*.

20 Шифрование данных в eDirectory

В NetIQ eDirectory 8.8 и более поздних версий можно зашифровать определенные конфиденциальные данные в то время как они хранятся на диске и к ним получает доступ клиент. В этом разделе представлена информация об ошибках, которые могут произойти при использовании зашифрованных атрибутов и функций репликации в eDirectory 8.8 и более поздних версий. Дополнительную информацию о зашифрованных атрибутах и репликации см. в документе *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html).

Информацию о других сообщениях об ошибках в eDirectory см. Веб-сайт кодов ошибок NetIQ (http://www.novell.com/documentation/nwec/)

20.1 Сообщения об ошибке

В этом разделе содержится информация об указанных ниже ошибках.

20.1.1 -6090 0xFFFFE836 ERR_ER_DISABLED

В процессе синхронизации реплики eDirectory предпринята попытка запустить зашифрованную репликацию с целевым сервером. Однако для целевого сервера eDirectory зашифрованный процесс синхронизации реплики отключен

Возможная причина

Зашифрованная репликация отключена на целевом сервере eDirectory.

Действие

Включите зашифрованную репликацию на сервере eDirectory.

20.1.2 -6089 0xFFFFE837 ERR_REQUIRE_SECURE_ACCESS

Со стороны приложения (доступ клиента) предприняты попытки получить доступ к зашифрованному атрибуту по каналу открытого текста.

Источник

eDirectory или NDS

Возможная причина

Зашифрованные атрибуты настроены таким образом, что получить к ним доступ можно только по безопасному каналу. Попытка доступа приложения к зашифрованным атрибутам по каналу открытого текста.

Действие

Приложение должно получать доступ к зашифрованным атрибутам по безопасному каналу, например безопасному каналу LDAP или HTTP.

Возможная причина

Если эта ошибка возвращается при репликации, то на одном сервере или нескольких серверах в кольце реплик есть несколько атрибутов, отмеченных для шифрования; кроме того, в конфигурации указано, что доступ к ним возможен только по безопасным каналам.

Действие

Измените конфигурацию политики зашифрованных атрибутов, чтобы к ним можно было получить доступ по каналам, которые не являются безопасными. Дополнительную информацию см. в документе *NetIQ eDirectory 8.8 SP8 Administration Guide (Руководство по администрированию NetIQ eDirectory 8.8 SP8)* (http://www.netiq.com/documentation/edir88/edir88/data/a2iii88.html).

Возможная причина

Если эта ошибка возвращается, когда зашифрованная репликация сконфигурирована на уровне раздела или между репликами раздела, то в кольце реплик есть серверы, на которых установлен eDirectory более ранней версии, чем 8.8.

Действие

Обновите eDirectory на всех серверы в кольце реплик до версии, совместимой с 8.8.

20.1.3 -666 FFFFFD66 INCOMPATIBLE NDS VERSION

Здесь будет текст справки

Возможная причина

Если при включенной на уровне раздела зашифрованной репликации вы пытаетесь добавить реплику этого раздела на сервер eDirectory, то версия eDirectory этого сервера несовместима с версией исходного сервера.

Действие

Обновите eDirectory на сервере до совместимой версии.

Возможная причина

Если в родительском разделе есть серверы, на которых установлен eDirectory более ранней версии, чем 8.8 (кольцо со смешанными версиями) и на дочернем разделе включен ER, то операции объединения и (или) присоединения разделов не будут разрешены. В этом случае возвращается ошибка ERR_INCOMPATIBLE_DS_VERSION.

Причина этой ошибки заключается в том, что дочерний раздел содержит конфиденциальные данные с включенным ER на уровне раздела, а в родительском разделе установлен сервер eDirectory более ранней версии, чем 8.8. Поскольку ER включен только между серверами eDirectory 8.8, то при объединении конфиденциальные данные становятся доступными при репликации на серверы eDirectory более ранней версии, чем 8.8.

Действие

1. Обновите eDirectory на сервере до совместимой версии.

   ИЛИ

2. Отключите ER в родительском или дочернем разделе.

   ПРИМЕЧАНИЕ. После отключения ER репликация будет выполняться в режиме открытого текста.

20.2 Проблема с назначением двух алгоритмов шифрования

Добавляя с помощью LDIF атрибут для шифрования, не связывайте два алгоритма с одним атрибутом.

Например, если отметить *title* как зашифрованный атрибут с алгоритмами шифрования AES и DES, то в конечном итоге не будет ясно, какой из этих алгоритмов нужно использовать. При каждом выполнении процесса Limber для атрибута "title" будут попеременно представляться атрибуты AES и DES. Поэтому это будет воспринято таким образом, как будто в конфигурацию внесены изменения.

Во избежание подобных сценариев рекомендуем не назначать два алгоритма шифрования одному атрибуту.

Этого не происходит, если атрибут отмечается для шифрования в iManager.

20.3 Шифрование атрибутов потока

Атрибуты потока могут быть представлены как данные в режиме открытого текста. Это происходит потому, что атрибуты потока в eDirectory 8.8 не шифруются.

20.4 Настройка зашифрованного тиражирования с помощью iManager

Настройка зашифрованного тиражирования при помощи iManager невозможна, если в кольце тиражирования отключен какой-либо сервер.

20.5 Просмотр и изменение зашифрованных атрибутов с помощью iManager

Если атрибут объекта зашифрован, то с помощью iManager 2.5 нельзя посмотреть или изменить объект.

Чтобы решить эту проблему, просматривайте и изменяйте зашифрованный атрибут по защищенному каналу одним из следующих способов.

- LDAP: необходимо послать LDAP-запрос по защищенному каналу. Это требует использования доверенного корневого сертификата сервера.
- ICE: для изменения объекта можно использовать сценарии LDIF. При этом ICE должен использовать защищенный канал.
- Используйте iManager версии 2.5 FP2, iManager 2.6 или более поздней.

ПРИМЕЧАНИЕ. Для просмотра и изменения зашифрованных атрибутов рекомендуется использовать iManager 2.6 или более поздней версии.

Также можно выключить параметр, требующий использования защищенного канала для просмотра и изменения зашифрованных атрибутов, отключив атрибут `requireSecure` политики EA. В результате объект и зашифрованные атрибуты станут доступны любому клиенту по каналу передачи обычных текстовых сообщений. Таким образом, доступ к объекту получит и iManager.

20.6 Ошибка слияния деревьев при использовании зашифрованного тиражирования

Если включено зашифрованное тиражирование, объединение деревьев завершается ошибкой. Отключите зашифрованное тиражирование для каждого дерева до начала слияния.

20.7 . Процесс limber отображает ошибку -603

Процесс Limber отображает ошибку -603 в том случае, если на сервере имеется только реплика sub-ref раздела политики зашифрованных атрибутов.

Эту проблему можно обойти одним из следующих способов.

- Разрешите доступ на чтение объекта "NCP-сервер". Эту операцию можно выполнить при помощи iManager с помощью добавления опекуна в корень дерева и разрешения доступа на чтение объекта «NCP-сервер». В атрибутах укажите `attrEncryptionDefinition` и `attrEncryptionRequiresSecure`.
- Разрешите открытый доступ на чтение следующих атрибутов при помощи LDAP или ndssch:
  - `attrEncryptionDefinition`
  - `attrEncryptionRequiresSecure`

21 Набор утилит управления eDirectory

NetIQ eDirectory Management Toolbox (eMBox) позволяет получить доступ ко всем внутренним утилитам eDirectory удаленно, а также на сервере.

Совместная работа eMBox и NetIQ iManager обеспечивает веб-доступ к утилитам eDirectory, таким как DSRepair, DSMerge, Backup and Restore и Service Manager.

ЗАМЕЧАНИЕ. Сервисы административных функций необходимо настроить посредством iManager. При настройке необходимо указать то дерево, которое должно администрироваться, чтобы можно было запустить задачи eMBox.

Все функции доступны либо на локальном сервере, либо удаленно через клиент командной строки. С помощью клиента eMBox можно с одного сервера или рабочей станции выполнять задачи для нескольких серверов. Чтобы запустить все eDirectory Management Tools (eMTools), включая Backup, DSRepair, DSMerge, Schema Operations и eDirectory Service Manager, eMBox необходимо загрузить и запустить на сервере eDirectory.

21.1 Не удается остановить сервисы eMTool

При выполнении команды `serviceStop -n{сервис}`, где *{сервис}* это один из сервисов (`libsasl.so`, `libncpengine.so`, `libhttpstk.so` или `libdsloader.so`), возвращается следующая ошибка:

```
Service {service} could not be stopped, Error : -660
```

Это не ошибка. Эти процессы (`libsasl.so`, `libncpengine.so`, `libhttpstk.so` и `libdsloader.so`) невозможно остановить, поскольку другие модули зависят от них.

21.2 Восстановление возвращает ошибку -6020

При прокрутке вперед журналов в расположении по умолчанию с одновременным выполнением операции восстановления при помощи DSBK или eMBox Client возвращается ошибка -6020. Чтобы избежать появления этой ошибки, необходимо выполнять команду `restore` с ключом `-s`.

21.3 Проблемы с менеджером сервисов eDirectory

Если остановка eDirectory в iManager осуществляется с помощью менеджера сервисов eDirectory, перезапуск eDirectory с помощью менеджера сервисов невозможен. Для перезапуска eDirectory воспользуйтесь утилитой eDirectory Services, доступной на сервере eDirectory (`C:\novell\NDS\NDSCons.exe`).

21.3.1 Удаление перемещенного объекта

Удаление перемещенного объекта может привести к ошибке 637 в дереве с двумя или более серверами.

21.3.2 Проблема с перемещением динамической группы

Перемещение объекта динамической группы с атрибутом `dynamicgroup` в атрибуте `Класс объекта` в другой контейнер приводит к нарушению функциональности динамической группы. После перемещения не работают поиск и запросы динамических членов.

21.3.3 Ошибка восстановления сетевого адреса через eMBox

При восстановлении сетевых адресов через eMBox будут возвращены следующие ошибки, поскольку eMBox не обновлен последними исправлениями для восстановления:

```
ОШИБКА: невозможно найти сетевой адрес для этого сервера - Ошибка : 11004
```

```
Ошибка: невозможно установить соединение. Ошибка : 11004
```

21.3.4 Просмотр файлов man page на французском языке

Для просмотра в ОС Red Hat Linux файлов man на французском языке выполните следующую команду:

```
export MANPATH=/opt/novell/man/frutf8:/opt/novell/eDirectory/man/frutf8
```

21.3.5 Удаление перемещенного объекта

Удаление перемещенного объекта может привести к ошибке 637 в дереве с двумя или более серверами.

21.3.6 eDirectory не создает событие выхода из системы из-за ограничения на количество клиентов eDirectory.

eDirectory не создает событие выхода из системы при выходе из iManager. Это объясняется техническими ограничениями в клиентской части eDirectory.

Приложения аудита могут использовать интерфейс NWDS API для получения событий выхода из системы. Приложения, использующие LDAP, могут отслеживать выход из системы с помощью событий отмены привязки (unbind).

21.3.7 Проблемы в работе TERM при выполнении DSTrace

Теги TIME и TAGS отображаются как активные (подчеркнуты), хотя по умолчанию таковыми не являются. Если тегу TERM назначено значение VT100 или xterm из терминала Linux, эти теги отображатся как активные (подчеркнуты). Эта проблема не возникает с каким-либо иным терминалом, например dtterm.

21.3.8 eMBox не обрабатывает двухбайтовые символы

eMBox не обрабатывает двухбайтовые символы для установки каталога прокрутки вперед посредством клиента eMBox и iManager. Это можно сделать при помощи DSBK.

22 SASL-GSSAPI

В этом разделе описаны сообщения об ошибках, которые протоколируются механизмом аутентификации SASL-GSSAPI.

22.1 Проблемы с SASL-GSSAPI

22.1.1 Проблема с несколькими объектами "Пользователь"

Если тот же участник системы защиты Kerberos связан с несколькими объектами "Пользователь" eDirectory, происходит сбой привязки LDAP с SASL GSSAPI.

22.1.2 . ИД авторизации

В RFC2222 объявлена поддержка *ИД* авторизации, отправляемого пользователем и клиентом. Эта технология не поддерживается методом SASL-GSSAPI.

22.2 Файл журнала

На платформах Linux сообщения об ошибке заносятся в файл журнала `ndsd.log`.

22.3 Сообщения об ошибке

SASL-GSSAPI: Reading Object *user_FDN* FAILED *код ошибки eDirectory*

Причина: Эта ошибка генерируется в eDirectory. Объект `user_FDN` не существует.

SASL-GSSAPI: Reading principal names for *user_FDN* failed *код ошибки eDirectory*

Причина: Эта ошибка генерируется в eDirectory. Имя участника системы защиты Kerberos не прикрепляется к объекту "Пользователь" (`userdn`).

SASL-GSSAPI: Reading Object *Realm_FDN* FAILED *код ошибки eDirectory*

Причина: Эта ошибка генерируется в eDirectory. Объект `realm` не существует.

SASL-GSSAPI: Not enough memory

Причина: Недостаточно памяти для выполнения данной операции.

SASL-GSSAPI: Invalid Input Token

Причина: Маркер от клиента поврежден или не является допустимым

SASL-GSSAPI: NMAS error *код ошибка NMAS*

Причина: Эта ошибка генерируется в NMAS и является внутренней ошибкой.

SASL-GSS: Invalid LDAP service principal name *имя_участника_сервиса_LDAP*

Причина: Недействительное имя участника сервиса LDAP.

SASL-GSS: Reading LDAP service principal key from eDirectory failed

Причина: Объект участника сервиса LDAP не создан.

Причина: Главный ключ объекта realm изменен.

Причина: Объект участника сервиса LDAP не найден в поддереве области аутентификации, к которой он принадлежит.

SASL-GSS: Creating GSS context failed

Причина: Время не синхронизировано между клиентом, KDC и серверами eDirectory.

Причина: Ключ участника сервиса LDAP изменен в базе данных Kerberos, однако не обновлен в eDirectory.

Причина: Тип шифрования не поддерживается.

SASL GSSAPI: Invalid user FDN = *полное_характерное_имя_пользователя*

Причина: Предоставленное клиентом полное характерное имя пользователя недействительно.

SASL GSSAPI: No user DN is associated with principal *имя_участника_системы_защиты_клиента*

Причина: К объекту `Пользователь` не прикреплено имя участника системы защиты Kerberos.

SASL GSSAPI: More than one user DN is associated with principal *имя_участника_системы_защиты_клиента*

Причина: Несколько объектов `Пользователь` в поддереве связаны с одним участником системы защиты.

ldap_simple_bind_s: Invalid credentials major = 1, minor =0

Причина: Причиной может стать несоответствие версий между участником сервиса LDAP на сервере KDC и участником сервиса LDAP на сервере eDirectory. Это происходит, поскольку при каждом извлечении ключа участника сервиса LDAP в файл keytab, номер версии увеличивается на единицу.

Действие:

Выполните описанную ниже процедуру.

1. Обновите ключ на сервере eDirectory, чтобы номера версии были синхронизированы.
2. Уничтожьте билеты на клиентах.
3. Заново получите TGT для участника системы защиты.
4. Выполните операцию привязки LDAP `sasl`.

23 Разное

23.1 Резервное копирование контейнера

При использовании ndsbackup для резервного копирования контейнера, который имеет множество объектов (например, миллион), некоторое время может понадобиться для получения списка объекта в контейнере и начала запуска их копирования по отдельности.

23.2 Повторяющиеся входы eDirectory

Повторяющиеся входы eDirectory могут занять всю доступную память. Чтобы разрешить эту проблему, отключите атрибут "Login Update (Обновление входа)", используя iMonitor.

23.3 Включение системной статистики сообщений

Статистика времени поддерживается для каждого события, возникшего и прошедшего в eDirectory. Эта информация полезна для поиска и устранения проблем, относящихся к потребителю события. Эта статистика не требуется для нормальной работы каталога, поэтому она отключена из соображений безопасности. Статистика событий может быть включена во время выполнения. Для этого необходимо воспользоваться расширенными параметрами конфигурации iMonitor.

Чтобы просмотреть статистику событий, задайте параметр `ENABLE_EVENT_STATISTICS` и перезапустите сервер. Это постоянный параметр конфигурации.

23.4 Отслеживание проблем сбоя памяти в Linux

На платформах Linux eDirectory использует Google malloc (`libtcmalloc`) в качестве распределителя памяти по умолчанию.

Для отслеживания проблем сбоя памяти установите переменную среды `MALLOC_CHECK_` в сценарии запуска ndsd. Сценарий запуска проверит эту переменную. Если переменная задана, используется malloc, установленный в системе по умолчанию. В противном случае загружается `libtcmalloc`.

Настройки MALLOC_CHECK в ndsd

- Если переменной `MALLOC_CHECK_` задано значение 0, то любое обнаруженное повреждение кучи игнорируется без каких-либо сообщений.
- Если переменной `MALLOC_CHECK_` задано значение 2, немедленно вызывается прерывание.

  Это помогает на ранних стадиях определить реальную причину сбоя, которую может быть сложно выявить позже.

23.5 Соединение TCP не прерывается после аварийного выхода

Иногда серверу OES Linux не удается определить хост клиента, который неожиданно выключился из-за сбоя рабочей станции или отключения питания. Однако подключение еще остается активным в течение времени ожидания по умолчанию (приблизительно от 12 до 15 минут). Если задать количество параллельных подключений равным 1, то до повторного входа рекомендуется прервать подключение вручную или подождать, пока истечет время ожидания по умолчанию. Эта ситуация происходит, когда процессу watchdog не удается штатно закрыть подключение. Поэтому если для количества параллельных подключений задано значение 1, и подключение не закрыто процессом watchdog, пользователи не могут войти в систему. Ядро Linux предоставляет три параметры для изменения способа, которым `keepalive` проверяет работу с серверной стороны. Воспользуйтесь этими параметрами, чтобы практически разрешить эту проблему на уровне TCP.

Эти параметры доступны в каталоге `/proc/sys/net/ipv4/` .

- `tcp_keepalive_time`: определяет частоту отправки пакетов `keepalive` протокола TCP для сохранения работы соединения, если оно не используется в данный момент. Это значение используется только в том случае, если параметр `keepalive` включен.

  `tcp_keepalive_time` принимает значение типа integer, которое указывает количество секунд. По умолчанию установлено значение 7200 секунд или 2 часа. Это значение хорошо подходит для большинства хостов. Оно не требует существенных сетевых ресурсов. Если задать это значение низким, ваши сетевые ресурсы будут перегружены бесполезным трафиком.

- `tcp_keepalive_probes`: определяет частоту отправки проверочных пакетов `keepalive` протокола TCP перед тем как будет установлено, что подключение утрачено.

  Параметр `tcp_keepalive_probes` принимает значение типа integer. Рекомендуется задать значение меньше 50 в зависимости от значений `tcp_keepalive_time` и `tcp_keepalive_interval`. По умолчанию задано значение на уровне 9 попыток. После этого в приложение отправляется информация о том, что соединение утрачено.

- `tcp_keepalive_intvl`: определение продолжительности ответа для каждой попытки `keepalive`. Это значение важно для расчета времени, по истечение которого отправленный пакет `keepalive` считается утраченным.

  Параметр `tcp_keepalive_intvl` принимает значение типа integer. По умолчанию задано значение 75 секунд. Итак, 9 попыток по 75 секунд продляться 11 минут. Значение переменных `tcp_keepalive_probes` и `tcp_keepalive_intvl` по умолчанию можно использовать для расчета времени ожидания по умолчанию, в течение которого ожидается ответ на пакеты `keepalive`.

Измените эти три параметры таким образом, чтобы разрешить проблему, не создавая при этом чрезмерный сетевой трафик. Ниже приведен пример такого изменения (время определения составляет 3 минуты):

- `tcp_keepalive_time set -120`
- `tcp_keepalive_probes - 3`
- `tcp_keepalive_intvl - 20`

ПРИМЕЧАНИЕ. Настройки параметров следует изменять осмотрительно. Рекомендуется не настраивать параметры для тех подключений, которые действуют.

Эти настройки вступают в силу немедленно после изменения файлов. Нет необходимости перезапускать какие-либо сервисы. Однако настройки действительны только для текущего сеанса. После перезагрузки сервера настройкам возвращаются значения по умолчанию.

Чтобы окончательно изменить настройку параметра (без изменений при перезапуске), выполните указанную ниже процедуру.

В файл `/etc/sysctl.conf`. добавьте указанные ниже записи

- net.ipv4.tcp_keepalive_time=120
- net.ipv4.tcp_keepalive_probes=3
- net.ipv4.tcp_keepalive_intvl=20

Мы рекомендуем использовать эти настройки только в том случае, если все клиенты и серверы подключены через локальную сеть.

23.6 Ошибка NDS, системный сбой (-632) при выполнении ldapsearch для объекта "Пользователь"

Импортируйте объекты "Пользователь" с простым паролем, а затем включите универсальный пароль для контейнера, в который импортируются объекты "Пользователь". Остановите сервер DS и задайте переменную среды как `NDSD_TRY_NMASLOGIN_FIRST=true`, затем перезапустите сервер DS. При выполнении ldapsearch для объектов "Пользователь", которые были импортированы с использованием простого пароля, возвращается следующая ошибка:

```
ldap_bind: Unknown error,  additional info: NDS error: system failure (-632)
```

Чтобы разрешить эту проблему, до выполнения операции ldapsearch для этих объектов "Пользователь", задайте последовательность входа в систему по умолчанию как простой пароль для контейнера, в который импортируются объекты "Пользователь".

Когда LDAP запрашивает NMAS выполнить вход пользователя, в NMAS используется последовательность входа в систему по умолчанию. Если не указать последовательности входа в систему по умолчанию для этих пользователей, то будет использована последовательность NDS. Если этим пользователям не предоставлялся пароль NDS при их импорте, то последовательность NDS не будет работать. Если включить универсальный пароль, то при входе пользователя в систему с простым паролем последний будет синхронизирован с паролем NDS и универсальным паролем.

23.7 Отключение SecretStore

Администратор eDirectory может отключить SecretStore с помощью следующего процесса:

23.7.1 На платформе Linux

1. Перейдите в каталог `nds-modules` и переименуйте или переместите следующие модули SecretStore:

   ```
   libsss.so
   libssncp.so
   libssldp.so
   ```

2. Перезагрузите сервер.

В качестве альтернативного варианта можно в файле /etc/opt/novell/eDirectory/conf/ndsmodules.conf закомментировать строку, которая загружает ssncp.

23.7.2 На компьютерах с Windows

1 Перейдите в каталог novell\nds и переименуйте или переместите следующие модули SecretStore:

```
lsss.dll
sss.dlm
ssncp.dlm
ssldp.dlm
```

2 Перезагрузите сервер.

23.8 . Просмотр файлов man page протокола SLP

Для просмотра файлов manpage по SLP необходимо указать пути к руководству. Например, в ОС AIX для manpath вместо /usr/share/man необходимо установить /opt/novell/man.

23.9 . Расположение конфигурационного файла DSBK

Файл DSBK.CONF расположен в каталоге /etc, а не в соответствующем каталоге конкретного экземпляра eDirectory.

23.10 . Проблемы совместимости с протоколом SLP в OES Linux

OpenSLP реализует протокол SLPv2, в то время как NetIQ SLP (NDSslp) на платформах Linux и Windows реализует протокол SLPv1.

UA SLPv1 не получает ответов от SA SLPv2, а UA SLPv2 не получает ответов от SA SLPv1. Таким образом, клиенты OpenSLP не могут видеть деревья NDSslp. Аналогично клиенты NDSslp не могут видеть деревья OpenSLP. Чтобы обеспечить совместимость протоколов SLPv1 и SLPv2, необходимо настроить DA, который работает по протоколу SLPv2. OpenSLP входит в комплект поставки OES Linux. Однако при установке eDirectory на другие платформы Linux, такие как Red Hat Linux, необходимо использовать NDSslp, поставляемый с eDirectory. Из-за проблем совместимости двух версий SLP дерево, объявленное через OpenSLP в режиме многоадресной передачи, может быть невидимо для NDSslp, и наоборот. Чтобы решить эту проблему, необходимо настроить DA, который работает по протоколу OpenSLP.

23.11 . Ldif2dib не удается открыть файл журнала ошибок, если каталог DIB установлен не в путь по умолчанию

Ldif2dib не может открыть файл журнала, используемый по умолчанию (LDIF2DIB.LOG), если директория базы dib данных Каталога перемещена в другое место.

Чтобы решить эту проблему, явным образом укажите расположение файла журнала с помощью ключа -b.

23.12 Сервер eDirectory не загружается автоматически в виртуальной ОС SLES 10

Если после добавления пакетов не производится настройка eDirectory с использованием YaST, необходимо выполнить следующую команду из командной строки:

```
chkconfig -a ndsd
```

23.13 . Ndsd не запускается автоматически после аварийного отказа системы

В некоторых случаях сервисы eDirectory (`Ndsd`) не запускаются после аварийного отказа системы или отключения питания. Для перезапуска eDirectory выполните следующие действия.

1. Удалите файл `/var/opt/novell/eDirectory/data/ndsd.pid`.
2. Введите команду `/etc/init.d/ndsd start`.

23.14 Не выполняйте DSTrace со всеми тегами, включенными на компьютерах Linux

При включении всех тегов запрещено запускать DSTrace в следующих случаях:

- **Загруженная система в режиме журнала:** имеется тенденция к использованию существенного объема памяти.
- **Серверы во встроенном режиме:** сбой выполнения ndsd.

23.15 . LDAP не соответствует требованиям RFC при анонимных запросах на поиск

Если незарегистрированный клиент выполняет поиск при отключенных анонимных подключениях, LDAP-сервер вместо результатов поиска выводит результат подключения ненадлежащей аутентификации, `operationsError`.

23.16 . Поиск и устранение проблем с портами при использовании пользовательских экземпляров eDirectory 8.8

Если настройка нового экземпляра eDirectory 8.8 осуществляется не в расположение по умолчанию, а сервер экземпляра по умолчанию остановлен, то новый экземпляр будет использовать порты экземпляра по умолчанию. Экземпляр по умолчанию не восстановится автоматически, так как его порты выделены новому экземпляру, установленному в пользовательское расположение.

Перед перезагрузкой хоста следует выполнить действия, описанные в разделе "«Устранение проблем с портами при использовании пользовательских экземпляров eDirectory 8.8»" (http://www.novell.com/coolsolutions/feature/17933.html).

23.17 . Перезагрузка хоста

После перезагрузки запускается только экземпляр по умолчанию, созданный с помощью двоичных файлов экземпляра по умолчанию.

Для запуска других экземпляров задайте пути к ним и используйте ndsmanage.

23.18 . Команда ndsd не выполняет прослушку кольцевого адреса на заданном порту NCP

При наличии нескольких экземпляров eDirectory второй и последующие экземпляры всегда пытаются прослушать порт 524 (по умолчанию) вместо заданного порта NCP на петлевом адресе.

Чтобы решить эту проблему, установите для второго экземпляра значение параметра n4u.server.tcp-port равное номеру требуемого порта. Параметр n4u.server.tcp-port находится в файле `NDS.CONF`.

ЗАМЕЧАНИЕ. Перед обновлением до eDirectory 8.8 SP8 необходимо запустить все экземпляры eDirectory.

23.19 . ИД объектов для транзакций LDAP

Для поддержки транзакций LDAP идентификатор объекта `supportedGroupingTypes` совпадает с идентификатором объекта `transactionGroupingType` (`2.16.840.1.113719.1.27.103.7`).

23.20 Ошибки -5871 и -5875 при трассировке LDAP

Ошибки -5871 и -5875 при трассировке LDAP обычно происходят, когда клиент LDAP принудительно закрывается без отмены привязки. Поэтому эти ошибки не свидетельствуют о проблемах; их можно игнорировать. Дополнительную информацию об этих ошибках см. на веб-сайте кодов ошибок NetIQ (http://www.novell.com/documentation/nwec/).

23.21 При переименовании дерева NDSCons возвращает ошибку -625

Если переименовать дерево на основном сервере и выключить DHost на вторичном сервере, утилита NDSCons возвратит сообщение о транспортной ошибке -625 со вторичным сервером в то время как DHost продолжает выполняться как на основном, так и на вторичном сервере. Эта ошибка происходит, поскольку NDSCons был запущен на вторичном сервере, когда дерево было переименовано на основном сервере. NDSCons работает нормально, если закрыть и перезапустить ее.

23.22 Прием данных на нескольких сетевых картах замедляет работу ldapsearch в eDirectory

Для решения проблемы сделайте следующее,

Отключите те сетевые карты в конфигурационном файле, которые замедляют работу ldapsearch.

или

Включите Advanced Referral Costing (ARC) с помощью команды `set NDSTRACE =!ARC1` в DSTrace.

23.23 Не удается ограничить количество параллельных пользователей на платформах Linux

В eDirectory 8.8 SP8 невозможно ограничить количество параллельных подключений на платформах Linux. *Для восстановления прежнего поведения (на основе строгой проверки порта) установите следующий параметр в файле*`nds.conf`.

```
n4u.server.mask-port-number=0
```

23.24 ndsd не удается завершить работу из-за SLP

Если в вашей сети на настроен SLP Directory Agent (DA), то поиск сервисов, которые используют SLP, может занять продолжительное время. При выключении eDirectory ndsd пытается выполнить операции, используя SLP. Это может занять более время, чем позволяет сценарий init, поэтому выключение выполняется принудительно.

Для решения этой проблемы выполните описанные ниже действия.

1. В каталоге конфигурации создайте пустой файл с именем `hosts.nds`. Каталог конфигурации сервера можно получить, выполнив команду `ndsconfig get n4u.server.confdir`
2. Задайте переменную среды NDS_USESLP равной 0, указав экспорт NDS_USESLP=0 в каталоге `/opt/novell/eDirectory/sbin/pre_ndsd_start`
3. Перезапустите eDirectory.

23.25 Перезапуск NLDAP в Windows

После остановки NLDAP необходимо перезапустить сервер, чтобы загрузить NLDAP.

23.26 Работа хранилища секретов по протоколу LDAP

Функциональность SecretStore не работает по протоколу LDAP. Чтобы решить эту проблему, нужно обновить LDAP через iManager.

23.27 Проблемы совместимости

23.27.1 Не удается изменить ключевую фразу после разблокировки SecretStore

Если пользователь пытается получить забытый пароль, войдя в систему с пользовательской учетной записью и неверной фразой-паролем, хранилище секретов блокируется. Открыть заблокированное SecretStore можно, воспользовавшись правами администратора. Кроме того, клиент NetIQ SecureLogin позволяет войти в систему без ключевой фразы. При попытке изменить фразу-пароль вход в систему заканчивается ошибкой.

23.27.2 Учетные данные пользователей, измененные с помощью хранилища секретов, сбрасываются

При попытке сохранить новые учетные данные в SecretStore при помощи подключаемого модуля iManager появляется пустой столбец учетных данных, потому что iManager не удалось сохранить изменения.

Изменить учетные данные с помощью подключаемого модуля SecretStore iManager можно только с учетной записью пользователя. Не используйте для этого учетную запись администратора.

23.27.3 При создании новых учетных данных прежние учетные данные перезаписываются.

При сохранении альтернативного набора учетных данных SecretStore не может хранить первый набор, при этом виден только последний.

Изменить учетные данные с помощью подключаемого модуля SecretStore iManager можно только с учетной записью пользователя. Не используйте для этого учетную запись администратора.

24 IPV6

В данном разделе содержится информация о поиске и устранении проблем IPv6 на всех платформах.

24.1 Безопасный поиск LDAP работает либо с IPv4, либо с IPv6, но не одновременно с обоими.

Безопасный поиск LDAP не выполняется, если клиент имеет адрес в обоих форматах IPv4 и IPv6.

24.2 Подключаемый модуль ICE не работает для адресов IPV6

Модуль не подключается к запрошенному серверу, если iManager принимает данные только по адресу в формате IPv4. Возвращается следующая ошибка:

```
Unable to connect to the requested server. Verify the name/address and port.
```

Чтобы настроить IPv6 в iManager для работы с eDirectory необходимо включить IPv6 согласно описанной ниже процедуре.

1. Задайте перечисленные ниже свойства в файле `catalina.properties` и перезапустите Tomcat.

   ```
   java.net.preferIPv4Stack=false
   ```

   ```
   java.net.preferIPv4Addresses=true
   ```

   Обратите внимание, что `java.net.preferIPv4Stack` применяется для работы iManager с eDirectory, а `java.net.preferIPv4Addresses` — для работы браузеров с iManager.

2. Последовательно выберите пункты *Параметры LDAP* > *Просмотр серверов LDAP* > *Соединения* > *Сервер LDAP*, затем добавьте интерфейсы LDAP для адресов IPv6 с номерами портов.

   ```
   ldap://[xx::xx]:389
   ldaps://[xx::xx]:636
   ```

3. Настройте сервис административных функций при выходе из сеанса и войдите снова.

24.3 Прослушиватель для неопределенных адресов IPv6 в Linux и Windows

Прослушиватель для неопределенных адресов IPv6 принимает подключения как IPv4, так и IPv6 в Linux. Из-за этого поведения в Linux не разрешено одновременно запускать прослушиватели для неопределенных адресов IPv4 и IPv6 на одном порту. Поэтому если прослушиватель уже настроен для неопределенного адреса IPv6, то при запуске прослушивателя на неопределенном адресе IPv4 происходит сбой. В Linux неопределенные адреса используются для прослушивателей LDAP.

ПРИМЕЧАНИЕ. Если на компьютере SLES 10 присутствует прослушиватель для неопределенного адреса IPv4, то прослушиватели для IP-адресов в формате IPv6 для того же порта не запускаются. Эта проблема известна в SLES 10. Однако в SLES 11 такой проблемы нет.

В Windows прослушиватель неопределенных адресов IPv6 принимает только подключения IPv6. Поэтому для приема соединений IPv4 вместе с соединениями IPv6 необходимо настроить отдельный прослушиватель IPv4.

По умолчанию оба прослушивателя IPv4 и IPv6 настроены для ldapInterfaces. В зависимости ldapInterfaces запускает требуемых прослушивателей.