

IBM

@server

iSeries

Технология преобразования идентификаторов в
рамках предприятия





@server

iSeries

Технология преобразования идентификаторов в
рамках предприятия

Содержание

Преобразование идентификаторов предприятия (EIM)	1
Как напечатать этот раздел	2
Преобразование идентификаторов предприятия	2
Общие сведения о EIM	4
Контроллер домена EIM	6
Домен EIM	6
Идентификатор EIM	7
Определения реестров EIM	10
Определения реестров систем и приложений	12
Связи EIM	13
Операции поиска в EIM	16
Права доступа EIM	17
Общие сведения о LDAP в рамках EIM	21
Отличительное имя LDAP	21
Родительское отличительное имя LDAP	21
Создание единого входа в сеть с помощью EIM	22
Планирование работы с EIM	24
Установка необходимых компонентов Навигатора	25
Настройка службы сетевой идентификации	25
Настройка EIM	26
Создание нового домена и присоединение к нему	27
Настройка защищенного соединения с контроллером домена EIM	30
Присоединение к существующему домену	30
Управление EIM	33
Управление доменами EIM	33
Добавление домена в папку Управление доменами	34
Подключение к домену	34
Удаление домена	34
Удаление домена из папки Управление доменами	34
Управление связями	34
Создание связи	35
Удаление связи	35
Управление идентификаторами EIM	36
Создание идентификатора EIM	36
Добавление псевдонима для идентификатора EIM	37
Удаление идентификатора EIM	37
Управление правами доступа пользователей EIM	37
Управление пользовательскими реестрами	38
Добавление пользовательского реестра	38
Добавление псевдонима в пользовательский реестр	39
Определение частного типа пользовательского реестра в EIM	39
Удаление пользовательского реестра	40
Удаление псевдонима из пользовательского реестра	41
API EIM	41
Устранение неполадок EIM	42
Невозможно подключиться к контроллеру домена	42
Вывод списка идентификаторов EIM занимает много времени	43
"Зависание" мастера настройки EIM во время завершающего этапа обработки	43
Описатель EIM более не действителен	43
Идентификационные и диагностические сообщения Kerberos	43
Информация, связанная с EIM	44

Преобразование идентификаторов предприятия (EIM)

Зачастую на предприятиях одновременно применяется несколько реестров пользователей, и из-за этого возникает необходимость создавать по несколько идентификаторов для одного сотрудника. Работа с несколькими реестрами пользователей быстро превращается в серьезную проблему, влияющую и на самих пользователей, и на администраторов, и на разработчиков приложений. Технология преобразования идентификаторов в рамках предприятия (EIM) позволяет сократить затраты на обслуживание реестров и идентификаторов пользователей на предприятии.

Технология EIM позволяет установить соответствие между каждым физическим лицом или объектом и всеми его идентификаторами в различных реестрах. В EIM предусмотрены API для создания таких соответствий и работы с ними. В операционной системе OS/400^(R) реализована единая среда входа в систему, в которой применяются технология EIM и протоколы Kerberos.

Для работы с EIM разработаны специальные мастера графического интерфейса Навигатора iSeries. С помощью Навигатора iSeries можно выполнять любые операции с EIM.

На серверах iSeries^(TM) могут применяться средства сетевой идентификации, основанные на EIM. Приложения и операционная система OS/400 могут получать паспорта Kerberos и определять, каким пользовательским профайлам они соответствуют, с помощью EIM.

Дополнительная информация о технологии EIM приведена в следующих разделах:

“Как напечатать этот раздел” на стр. 2

Сведения о том, как можно напечатать этот и другие разделы справки по EIM в формате PDF.

“Преобразование идентификаторов предприятия” на стр. 2

Сведения о том, какие задачи можно решить с помощью EIM, и в чем заключаются достоинства технологии EIM при решении этих задач.

“Общие сведения о EIM” на стр. 4

Общие сведения, необходимые для работы с EIM.

“Общие сведения о LDAP в рамках EIM” на стр. 21

Общие сведения о протоколе LDAP, необходимые для работы с EIM.

“Создание единого входа в сеть с помощью EIM” на стр. 22

Достоинства технологии EIM, позволяющие упростить среду входа пользователей в систему.

“Планирование работы с EIM” на стр. 24

Сведения о том, какие службы и приложения должны быть настроены для работы с EIM.

“Настройка EIM” на стр. 26

Описание мастера настройки EIM, упрощающего начало работы с этой технологией.

“Управление EIM” на стр. 33

Инструкции по работе со свойствами EIM, доменами EIM, реестрами пользователей, правами доступа пользователей EIM и прочими объектами.

“API EIM” на стр. 41


Инструкции по применению API EIM в пользовательских приложениях и в сети.

“Устранение неполадок EIM” на стр. 42

Описание типичных проблем и распространенных ошибок, возникающих при работе с EIM.

Как напечатать этот раздел

Для просмотра или загрузки документа в формате PDF щелкните на ссылке Enterprise Identity

Mapping  (около 390 Кб или 50 страниц).

Дополнительная информация

Вы можете просмотреть или загрузить следующие связанные документы:


- Документ Службы сетевой идентификации (около 199 Кб или 60 страниц) содержит инструкции по настройке службы сетевой идентификации вместе с EIM для создания среды единого входа в систему.
- Документ Службы каталогов (LDAP) (около 323 Кб или 66 страниц) содержит инструкции по настройке сервера LDAP, который может применяться в качестве контроллера домена EIM, а также сведения о расширенных опциях конфигурации LDAP.

Сохранение файлов PDF

Для сохранения PDF-версии на рабочей станции (для дальнейшего просмотра или печати) выполните следующие действия:

1. Откройте файл PDF в браузере (щелкнув по указанной выше ссылке).
2. Выберите в меню браузера пункт **Файл**.
3. Выберите опцию **Сохранить как...**
4. Выберите каталог, в котором вы хотите сохранить PDF-версию документа.
5. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Acrobat Reader

Программу Adobe Acrobat Reader, необходимую для просмотра и печати файлов PDF можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Преобразование идентификаторов предприятия

Современные сети состоят из сложных групп систем и приложений, требующих поддержания нескольких реестров пользователей. Работа с несколькими реестрами пользователей быстро превращается в серьезную проблему, влияющую и на самих пользователей, и на администраторов, и на разработчиков приложений. Для многих компаний организация надежной идентификации и упорядочения доступа к системам и приложениям становится одной из первоочередных задач.

Функция преобразования идентификаторов предприятия (EIM) фирмы IBM  **server** позволяет администраторам и разработчикам приложений быстро решать эту проблему.

В данной главе рассказано о возможных проблемах, кратко описаны наиболее широко применяемые способы их решения, а также рассказано о достоинствах системы EIM.

Проблемы, связанные с отсутствием централизованного реестра

Многим администраторам приходится управлять сетями, включающими самые разные системы, каждая из которых применяет свой собственный реестр пользователей и собственные процедуры управления этим реестром. В таких сложных сетях администраторам приходится обеспечивать обслуживание идентификационных данных пользователей сразу в нескольких системах.

Администраторам часто приходится обеспечивать синхронизацию имен, паролей и прав доступа пользователей, а пользователям приходится держать в голове множество имен и паролей, а также заботиться об их синхронизации. Пользователям и администраторам в такой среде приходится затрачивать слишком много усилий, администраторы часто тратят свое высокооплачиваемое рабочее время не на управление предприятием, а на разрешение проблем, связанных с забытыми паролями неудачными попытками входа в систему.

Проблема обслуживания нескольких реестров пользователей мешает жить и разработчикам приложений, создающих многоуровневые или неоднородные приложения. Разработчики с вниманием относятся к тому, что важные данные заказчиков хранятся в самых разных системах, каждая из которых поддерживает только свой собственный реестр пользователей. В результате разработчикам приходится создавать для своих приложений собственный реестр пользователей и разрабатывать связанную с ним семантику защиты. Такой подход решает проблему разработчиков, но несколько не облегчает жизнь пользователей и администраторов.

Текущие подходы к решению проблемы

В настоящее время существует несколько подходов к решению проблемы управления несколькими реестрами пользователей, но ни один из них не обеспечивает полного решения этой проблемы. Например, простой протокол доступа к каталогам (LDAP) обеспечивает решение, в котором реализуется распределенный реестр пользователей. Однако, для применения решений, основанных на LDAP (и других аналогичных решениях, например, Microsoft Passport), администраторам придется обеспечить управление еще одним реестром пользователей и набором семантики защиты, либо заменить существующие приложения, обеспечив применение нового способа идентификации.

При использовании подобных решений администраторы вынуждены обслуживать несколько механизмов защиты различных ресурсов, что существенно повышает нагрузку на администраторов и увеличивает вероятность возникновения ошибок, приводящих к возникновению брешей в защите. Когда защита одного ресурса обеспечивается несколькими механизмами, всегда существует очень значительная вероятность того, что администратор изменит права доступа с помощью одного механизма и забудет сделать это для одного или нескольких других механизмов. Например, ситуация, когда доступ пользователя к ресурсу запрещен через один интерфейс, но разрешен через один или несколько других, является потенциальной угрозой защите.

Тем не менее, после выполнения всего объема работы администраторы обнаружат, что проблема решена не полностью. Как правило, предприятия инвестируют довольно большой объем денег в свои реестры пользователей и связанную с ними семантику защиты, что делает реализацию подобного подхода неэффективной. Создание еще одного реестра пользователей со связанной семантикой решает проблему поставщика приложений, но не проблему пользователей и администраторов.

Один из других возможных подходов заключается в применении механизма однократного входа в систему. Существует несколько продуктов, позволяющих администраторам управлять файлами, содержащими все идентификационные данные и пароли пользователя. Однако и у такого подхода есть свои недостатки:

- Проблема решается только с точки зрения пользователей. Несмотря на то, что для входа в несколько систем пользователь должен указать только одно имя и пароль, идентификационные данные должны храниться и обслуживаться во всех системах.
- Возникает потенциальная угроза безопасности, поскольку пароли в применяемых файлах обычно хранятся в текстовом или в легко расшифровываемом формате. Пароли всегда должны храниться в зашифрованном виде и не должны быть доступны другим пользователям, включая администраторов.
- Не решается проблема независимых поставщиков приложений, создающих неоднородные многоуровневые приложения. Они по-прежнему должны поддерживать в своих приложениях независимые реестры пользователей.

Несмотря на перечисленные недостатки, некоторые предприятия применяют такой подход, поскольку он несколько упрощает проблемы, связанные с наличием нескольких реестров пользователей.

Подход, основанный на EIM

Архитектура EIM предлагает новый подход к организации децентрализованных реестров пользователей, позволяющий сэкономить значительные средства. Архитектура EIM описывает соотношения между отдельными объектами предприятия (например, файловыми серверами или серверами печати) и идентификаторами, соответствующими им в сети предприятия. Кроме того, EIM содержит набор API, позволяющих приложениям запрашивать информацию о таких взаимосвязях.

Например, если вам известно имя пользователя в одном из реестров, то вы можете определить, какая запись другого реестра соответствует этому пользователю. Если пользователь успешно прошел идентификацию с помощью одного реестра и вы можете установить соответствие между записью этого реестра и записью другого реестра пользователей, то пользователю не придется еще раз вводить свои данные для повторной идентификации. Вам известен пользователь и достаточно сведений о его идентификаторе в другом реестре. Таким образом, EIM обеспечивает общую функцию преобразования идентификаторов для всей сети предприятия.

Возможность установления соответствия между записями различных реестров пользователей обеспечивает множество преимуществ. Прежде всего, обеспечивается высокая гибкость - приложения могут применять для идентификации один реестр, а для проверки прав доступа - другой. Например, администратор может применять запись SAP (точнее, SAP может делать это самостоятельно) для доступа к ресурсам SAP.


Функция преобразования идентификаторов требует от администраторов выполнения следующих задач:

1. Создать идентификаторы EIM, соответствующие сотрудникам и объектам предприятия.
2. Создать определения реестров EIM, описывающие существующие реестры пользователей предприятия.
3. Определить взаимосвязь между идентификаторами пользователей в этих реестрах и созданными идентификаторами EIM.

Изменять программы обслуживания существующих реестров не требуется. Администратору не требуется обеспечивать преобразование всех идентификаторов из реестров пользователей. EIM обеспечивает преобразование один-несколько (другими словами, одному пользователю в реестре может соответствовать несколько идентификаторов). EIM также обеспечивает преобразование много-один (т.е. несколько пользователей могут применять общий идентификатор из реестра), хотя применять такую конфигурацию и не рекомендуется. Администратор может указать в EIM любой реестр пользователей любого типа.

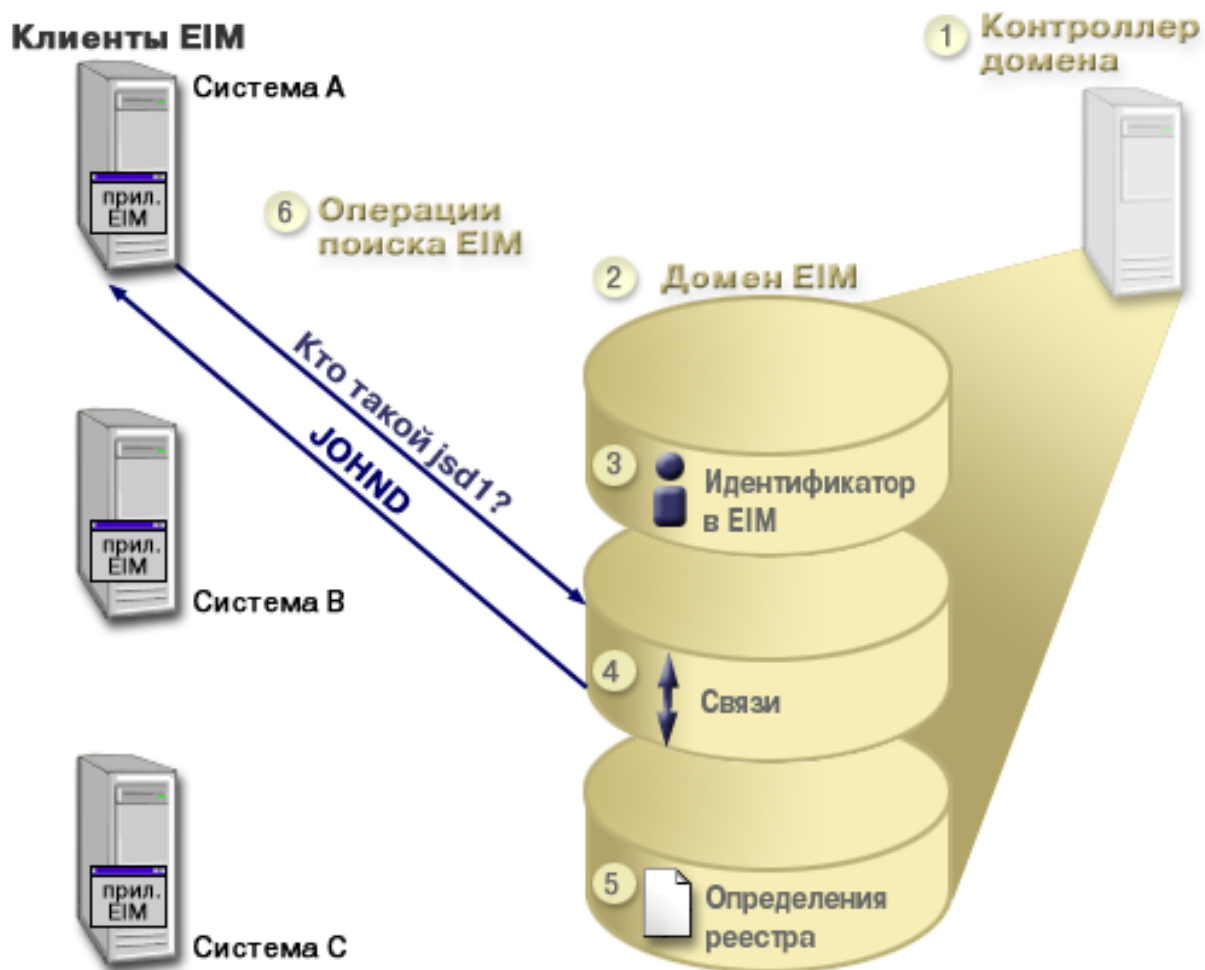
EIM - это открытая архитектура, позволяющая создавать связи между определениями пользователей в различных реестрах. Она не требует копирования существующих данных в новое хранилище и обеспечения синхронизации обеих копий. Единственный набор новых данных, необходимых для EIM, - это информация о взаимосвязи. Администраторы хранят эти сведения в каталоге LDAP, который обеспечивает необходимую гибкость, позволяя управлять данными в одном расположении, и создавать копии этих данных в тех местах, где информация применяется. EIM сокращает нагрузку на разработчиков и администраторов и расширяет возможности по совмещению различных компьютерных сред в масштабах предприятия.

Общие сведения о EIM

Для успешной реализации EIM на предприятии рекомендуем вам ознакомиться с общими принципами работы этой системы. Хотя настройка и реализация API EIM зависят от конкретной платформы IBM , общие принципы работы одни и те же на всех платформах.

На рис. 1 показан пример реализации EIM на предприятии. Три сервера выступают в роли клиентов EIM и используют приложения, получающие данные EIM с помощью операций поиска в EIM **6**. Контроллер домена **1** содержит данные о домене EIM **2**. В состав этих данных входят идентификатор EIM **3**, связи **4** между этими идентификаторами и определения из реестра EIM **5**.

Рисунок 1: Пример реализации EIM




Дополнительные сведения о EIM приведены в следующих разделах:

- “Контроллер домена EIM” на стр. 6
- “Домен EIM” на стр. 6
- “Идентификатор EIM” на стр. 7
- “Определения реестров EIM” на стр. 10
- “Связи EIM” на стр. 13
- “Операции поиска в EIM” на стр. 16
- “Права доступа EIM” на стр. 17

Контроллер домена EIM

Контроллер домена EIM - это сервер LDAP, в котором настроен по крайней мере один домен EIM. *Домен EIM* - это каталог LDAP, в котором содержатся все идентификаторы, связи EIM и реестры пользователей домена. Системы (клиенты EIM) используют данные домена в операциях поиска в EIM. На предприятии должен быть по крайней мере один контроллер домена EIM.

В настоящее время функция домена EIM поддерживается на нескольких платформах компьютеров  фирмы IBM. Клиентами могут быть любые системы, поддерживающие API EIM. Клиенты выполняются "Операции поиска в EIM" на стр. 16 с помощью API EIM.

В зависимости от расположения клиента EIM, контроллер домена может быть либо локальным, либо удаленным. Контроллер домена называется *локальным*, если клиент EIM работает в той же системе, что и контроллер домена. Контроллер домена называется *удаленным* по отношению к клиенту, если клиент и контроллер работают в разных системах.

Домен EIM

Домен EIM - это каталог сервера LDAP, в котором хранятся данные EIM. Домен EIM содержит все идентификаторы, связи и реестры пользователей EIM. Системы (клиенты EIM) используют данные домена в операциях поиска в EIM.

Домен EIM и реестр пользователей - это разные вещи. Реестр содержит идентификаторы пользователей, известные конкретным операционной системе или приложению. Кроме этого, в реестрах пользователей хранятся идентификационные данные пользователей, необходимые для входа в систему. Зачастую реестры также содержат сведения о ролях пользователей, личные данные и т.п.

Домен EIM содержит *ссылки* на идентификаторы пользователей в реестрах. Домен EIM фактически задает *соответствие* между идентификаторами пользователей в разных реестрах и реальными людьми, которым эти идентификаторы предназначены. Поскольку EIM отслеживает только соответствие между идентификаторами, синхронизация реестров пользователей и EIM не требуется.

На рис. 2 показаны данные, которые хранятся в домене EIM. В число этих данных входят идентификаторы EIM, определения из реестра EIM и связи EIM. Данные EIM задают связь между идентификаторами пользователей и реальными людьми, которым предоставлены эти идентификаторы.

Рисунок 2: Домен EIM и данные, которые в нем хранятся



В EIM хранятся следующие данные:

- **Идентификаторы EIM.** Каждый идентификатор EIM соответствует физическому лицу или объекту предприятия. Дополнительная информация приведена в разделе “Идентификатор EIM”.
- **Определения реестров EIM.** Каждое определение реестра EIM соответствует фактическому реестру пользователей, применяемому конкретной системой или группой систем предприятия. Для того чтобы реестр пользователей мог участвовать в домене EIM, нужно создать его определение в домене. Дополнительная информация приведена в разделе “Определения реестров EIM” на стр. 10.
- **Связи EIM.** Связь EIM - это сочетание идентификатора EIM и идентификатором пользователя в одном из реестров предприятия. Связи должны существовать для всех пользователей, работающих в домене EIM. Связи содержат информацию, необходимую для сопоставления идентификаторов EIM и идентификаторов пользователей в отдельных реестрах. Связи нужны для выполнения операций поиска в EIM. Операции поиска заключаются в определении идентификаторов пользователей в конкретных реестрах по их идентификаторам в EIM или идентификаторам в других реестрах. Дополнительная информация приведена в разделе “Операции поиска в EIM” на стр. 16.

Для начала работы с EIM достаточно создать идентификаторы EIM, определения реестров и связи.

Идентификатор EIM

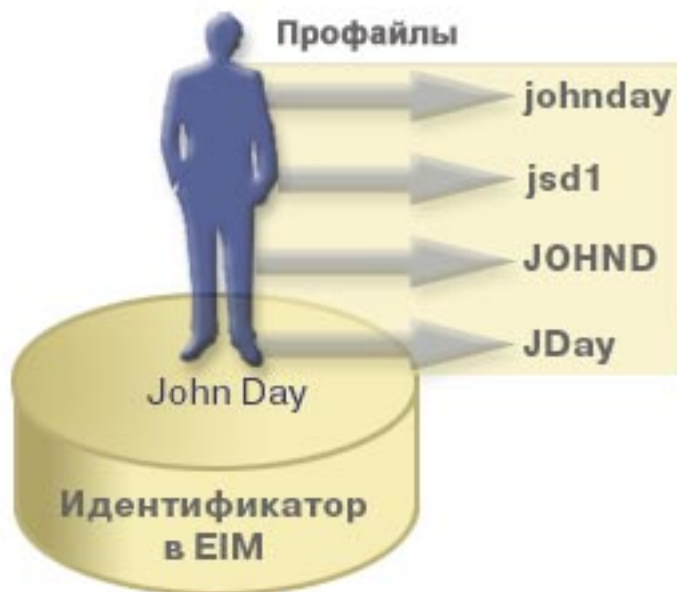
Идентификатор EIM - это уникальный идентификатор сотрудника или объекта на предприятии. Довольно часто сеть предприятия состоит из разнообразного аппаратного и программного обеспечения с несколькими независимыми реестрами пользователей. Часто это обусловлено требованиями различных платформ или реестров. Каждый реестр содержит идентификационные данные, относящиеся к пользователям его серверов и приложений.

Если для каждого пользователя или объекта будет создан единый идентификатор EIM, который будет связан со всеми идентификаторами этого пользователя или объекта в разных реестрах, это значительно упростит администрирование сети и позволит создать единую среду идентификации. Администратору будет проще разрабатывать средства управления доступом пользователей и работать с этими средствами.

Идентификатор EIM для пользователя

На рисунке 3 показан пример идентификатора EIM для пользователя *John Day*. У пользователя *John Day* есть четыре идентификатора в разных реестрах: johnday, jsd1, JOHND и JDay.

Рисунок 3: Связь между идентификатором EIM пользователя *John Day* и его прочими идентификаторами.

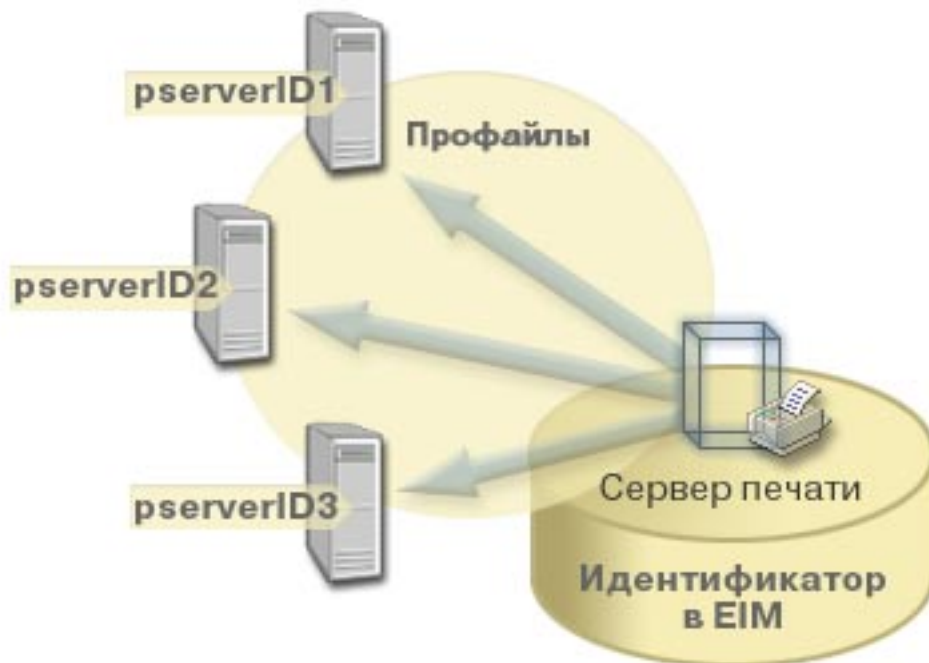


В EIM создаются связи между идентификатором пользователя John Day в EIM и его прочими идентификаторами в разных реестрах. После этого все приложения смогут пользоваться единым идентификатором пользователя, хранящимся в EIM.

Идентификатор EIM для объекта

Помимо идентификаторов пользователей, в EIM могут создаваться идентификаторы объектов (см. рис. 4). Например, сервер печати предприятия может работать в нескольких системах. На рис. 4 сервер печати работает в трех системах, и в каждой системе ему присвоен собственный идентификатор: pserverID1, pserverID2 и pserverID3.

Рисунок 4: Связь между идентификатором EIM сервера печати и его идентификаторами в отдельных системах.



В EIM можно создать единый идентификатор для сервера печати, который будет применяться в масштабах предприятия. В данном примере идентификатор функции сервера печати используется для идентификации сервера печати во всех системах предприятия. Идентификатор сервера в EIM (функция сервера печати) привязывается ко всем отдельным идентификаторам этого сервера (pserverID1, pserverID2 и pserverID3). Это устранил необходимость обращаться к серверу по разным именам из разных систем. Разработчики программ могут использовать в своих приложениях единое имя сервера независимо от того, в каких отделах предприятия будут использоваться эти приложения.

Идентификаторы и псевдонимы EIM

Для идентификаторов EIM можно создавать псевдонимы. Псевдонимы упрощают поиск идентификаторов EIM при выполнении операций поиска. Например, псевдонимы могут быть полезны в случаях, когда идентификатор пользователя в организации не совпадает с его реальным именем.

Все идентификаторы EIM должны быть уникальны в пределах домена EIM. Псевдонимы упрощают работу в случаях, когда идентификаторы трудны для запоминания. Например, в организации могут работать несколько человек с одинаковыми именами.

На рис. 5 показана ситуация, когда в организации работают два сотрудника с именем *John S. Day*. Администратор EIM создал для них два идентификатора EIM: *John S. Day1* и *John S. Day2*. Однако по этим идентификаторам не очевидно, какому из пользователей *John S. Day* соответствует каждый из них.

Рисунок 5: Примеры идентификаторов EIM для двух пользователей *John S. Day*



С помощью псевдонимов администратор EIM может задавать дополнительную информацию об идентификаторах EIM. Эта информация используется в операциях поиска EIM. Например, для пользователя John S. Day1 можно создать псевдоним John Samuel Day, а для пользователя John S. Day2 - псевдоним John Steven Day.

Для любого идентификатора EIM можно создать произвольное число псевдонимов. Это удобно в случаях, когда различать пользователей можно по нескольким признакам. Например, в дополнительных псевдонимах можно указывать номера пользователей, номера отделов, должности и т.п.

Определения реестров EIM

Определение реестра EIM содержит данные об отдельном реестре пользователей предприятия. Реестр пользователей - это каталог, в котором содержатся идентификаторы пользователей отдельной системы или приложения. Как правило, в реестре хранятся идентификаторы и пароли пользователей. Типичным примером может служить реестр z/OS Security Server Resource Access Control Facility (RACF^(R)). Реестры пользователей могут содержать и прочие данные. Например, в каталогах LDAP хранятся DN связывания, пароли и параметры управления доступом к данным каталога LDAP. Другими примерами реестров пользователей могут служить центры рассылки ключей Kerberos (KDC) и реестры пользовательских профайлов OS/400.

В определениях реестров EIM хранятся сведения об отдельных реестрах пользователей предприятия. Администратор указывает следующие данные о реестрах пользователей в EIM:

- Уникальное имя реестра в EIM
- Тип реестра

Для каждого реестра пользователей создается отдельное определение в EIM. Для удобства рекомендуем присваивать определениям реестров в EIM простые и понятные идентификаторы. Например, в качестве идентификаторов можно использовать имена хостов (возможно, в сочетании с именем приложения, использующего реестр). Именами реестров в EIM могут быть любые алфавитно-цифровые строки. В именах могут содержаться пробелы.

На рис. 6 администратор создал в EIM определения пользовательских реестров систем System A, System B и System C. По сценарию в системе System A содержится реестр WebSphere Lightweight Third-Party Authentication (LTPA). Имя, присвоенное определению реестра администратором, позволяет без труда идентифицировать этот реестр. Как правило, для идентификации реестров

удобно применять IP-адреса или имена хостов. В данном примере администратор присвоил реестру имя System_A_WAS. В качестве типа реестра указано значение WebSphere LTPA.

Рисунок 6: Определения трех реестров пользователей в EIM



Допускается определение вложенных реестров пользователей. Например, реестр z/OS Security Server (RACF) может содержать внутренние реестры, распространяющиеся на отдельные подмножества пользователей общего реестра RACF. Подробная информация об этом приведена в разделе “Определения реестров систем и приложений” на стр. 12.

Псевдонимы определений реестров в EIM

В EIM предусмотрена возможность создания псевдонимов для определения реестров. Можно воспользоваться одним из predefined типов псевдонимов, а также создавать собственные типы. Поставляются следующие predefined типы псевдонимов:

- Имя хоста в DNS
- Область Kerberos
- DN создателя
- Корневое DN
- Адрес TCP/IP
- Имя хоста в DNS LDAP

Псевдонимы позволяют абстрагироваться от имен конкретных реестров при разработке приложений, использующих EIM. В документации к приложениям можно указать псевдонимы, используемые приложением. Администратор EIM создаст соответствующие псевдонимы для реальных определений реестров.

После того как администратор создаст псевдоним для определения реестра в EIM, приложение сможет определить имя этого реестра с помощью операции определения имени по псевдониму. После этого приложение сможет указывать реальное имя реестра в вызовах API для выполнения «Операции поиска в EIM» на стр. 16.

Определения реестров систем и приложений

В некоторых случаях приложениям нужны не все идентификаторы из конкретного реестра пользователей, а только некоторые из них. Для этого в EIM предусмотрено два типа реестров: реестры систем и реестры приложений.

Определение реестра системы представляет полный реестр пользователей рабочей станции или сервера. Такой тип определений следует применять для реестров, обладающих следующими характеристиками:

- Реестр предоставляется операционной системой (например, AIX^(R) или OS/400^(R)) или изолированным продуктом управления защитой (например, z/OS Security Server Resource Access Control - RACF^(R)).
- В реестре хранятся идентификаторы пользователей, уникальные в рамках конкретного приложения (например, Lotus Notes^(R)).
- В реестре хранятся распределенные идентификаторы пользователей (например, субъекты Kerberos или отличительные имена LDAP).

Определение реестра приложения представляет подмножество идентификаторов пользователей в пределах реестра системы. Эти идентификаторы обладают какими-либо особыми атрибутами и применяются конкретным приложением или набором приложений. Такой тип определений следует применять для идентификаторов, обладающих следующими характеристиками:

- Идентификаторы пользователей приложения (набора приложений) не хранятся в отдельном реестре.
- Идентификаторы пользователей приложения (набора приложений) хранятся в реестре, в котором также хранятся иные идентификаторы пользователей.

Выполнение операций поиска в EIM не зависит от типа реестра. Типизация реестров нужна только для упрощения работы с идентификаторами пользователей. Ответственность за управление идентификаторами пользователей отдельных приложений можно возложить на администратора соответствующего реестра.

На рисунке 7 показан пример создания в EIM определения реестра системы для реестра z/OS Security Server RACF. Для пользователей RACF, применяющих продукт z/OS UNIX System Services (z/OS UNIX), создано отдельное определение реестра приложения. В реестре пользователей системы System C хранятся сведения об идентификаторах DAY1, ANN1 и SMITH1. Двум из этих идентификаторов (DAY1 и SMITH1) предоставлен доступ к z/OS UNIX в системе System C. Этим идентификаторам присвоены уникальные атрибуты, позволяющие определить, что им нужен доступ к системе z/OS UNIX. Для всего реестра пользователей RACF администратор EIM создал определение реестра System_C_RACF. Помимо этого, администратор EIM создал определение реестра System_C_UNIX для пользователей, для которых задан атрибут доступа к z/OS UNIX.

Рисунок 7: Определения в EIM для реестра RACF и пользователей z/OS UNIX

z/OS RACF сервера защиты



Реестр	Тип
System_C_RACF	RACF
System_C_UNIX	RACF
System_A_WAS	WebSphere LTPA

Связи EIM

Связь EIM - это сочетание идентификатора EIM, назначенного физическому лицу или объекту, и идентификатора этого лица или объекта в конкретном реестре. Создав связи между идентификатором EIM и всеми идентификаторами пользователя в разных реестрах, можно получить единый идентификатор пользователя и применять его в пределах предприятия. В EIM предусмотрены API, позволяющие приложениям определять идентификаторы пользователей в конкретных реестрах по их идентификаторам в EIM. Эта процедура называется *поиском идентификаторов*.

Перед тем, как приступить к созданию связей, нужно создать в EIM идентификатор пользователя и определения реестров, в которых хранятся его идентификаторы на предприятии. Связь задает соответствие между идентификатором EIM и идентификаторами в отдельных реестрах и содержит следующие данные:

- Идентификатор EIM
- Имя пользователя
- Определение реестра EIM
- Тип связи

Для разных способов применения идентификаторов предусмотрено несколько типов связей EIM. Идентификаторы пользователей могут применяться для идентификации, проверки прав доступа, либо и для того, и для другого.

Идентификацией называется процедура проверки личности пользователя. Проверка личности заключается в сопоставлении идентификатора, указанного пользователем, с некими секретными данными, - например, паролем.

Проверка прав доступа - это процедура удостоверения факта того, что пользователю разрешено выполнение операции, которую он пытается выполнить. Ранее практически всегда для идентификации и проверки прав доступа использовались одни и те же идентификаторы, которые хранились в едином реестре. "Операции поиска в EIM" на стр. 16 позволяют приложениям определять идентификаторы пользователей в определенных реестрах по их идентификаторам в других реестрах.

В EIM предусмотрено три типа связей: исходные, целевые и административные.

Исходная связь

Если идентификатор пользователя используется для *идентификации*, для него нужно создать исходную связь с идентификатором EIM. Исходные связи позволяют определять идентификаторы пользователей в нужных реестрах по их идентификаторам в других реестрах. Если для пользователя существует только одна исходная связь, то операция поиска альтернативных идентификаторов не даст результатов.

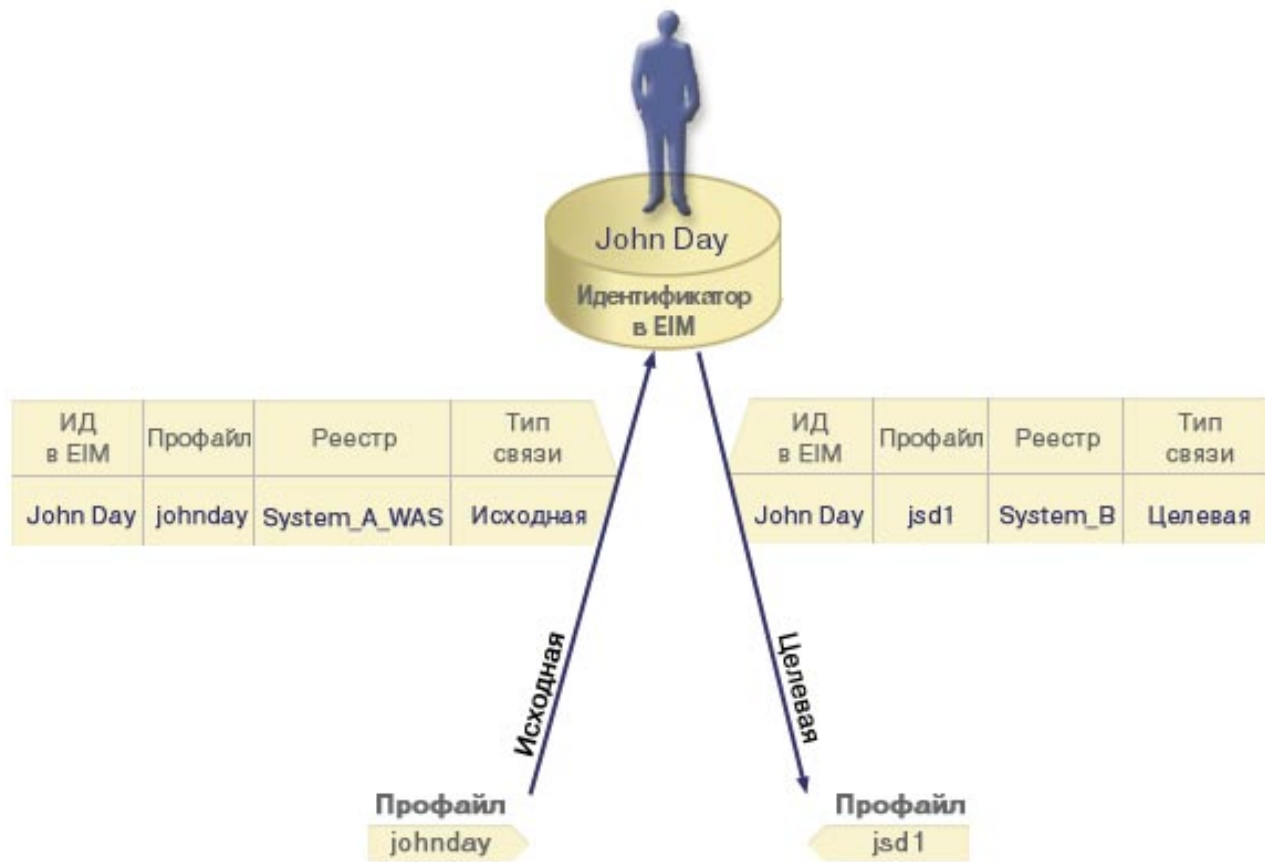
Целевые связи

Если идентификатор пользователя используется для *проверки прав доступа*, для него нужно создать целевую связь с идентификатором EIM. Целевые связи позволяют получать идентификаторы пользователей в качестве результата операции поиска в EIM. Если для пользователя существует только одна целевая связь, то операция поиска альтернативных идентификаторов не даст результатов.

В некоторых случаях для одного и того же пользователя нужно создать как исходные, так и целевые связи. Это требуется тогда, когда пользователь применяет систему одновременно в качестве клиента и сервера, а также для администраторов. Например, пользователь может входить в систему с машины Windows и после этого работать с сервером AIX. Кроме того, пользователю периодически требуется входить в систему с сервера AIX. В такой ситуации нужно создать для пользователя как исходную, так и целевую связь между его идентификаторами в AIX и в EIM. Для обычных пользователей обычно достаточно создать только целевые связи.

На рис. 6 показаны примеры исходной и целевой связей. Администратор создал две связи для идентификатора John Day для того, чтобы связать его с двумя идентификаторами этого пользователя. Исходная связь использует идентификатор LTPA johnday в системе System_A_WAS. Целевая связь использует идентификатор пользовательского профайла jsd1 OS/400 в системе B. Благодаря этому можно определить неизвестный идентификатор пользователя в целевой системе (jsd1) по его известному идентификатору в исходной системе (johnday).

Рисунок 6: Целевая и исходная связи для идентификатора EIM John Day.



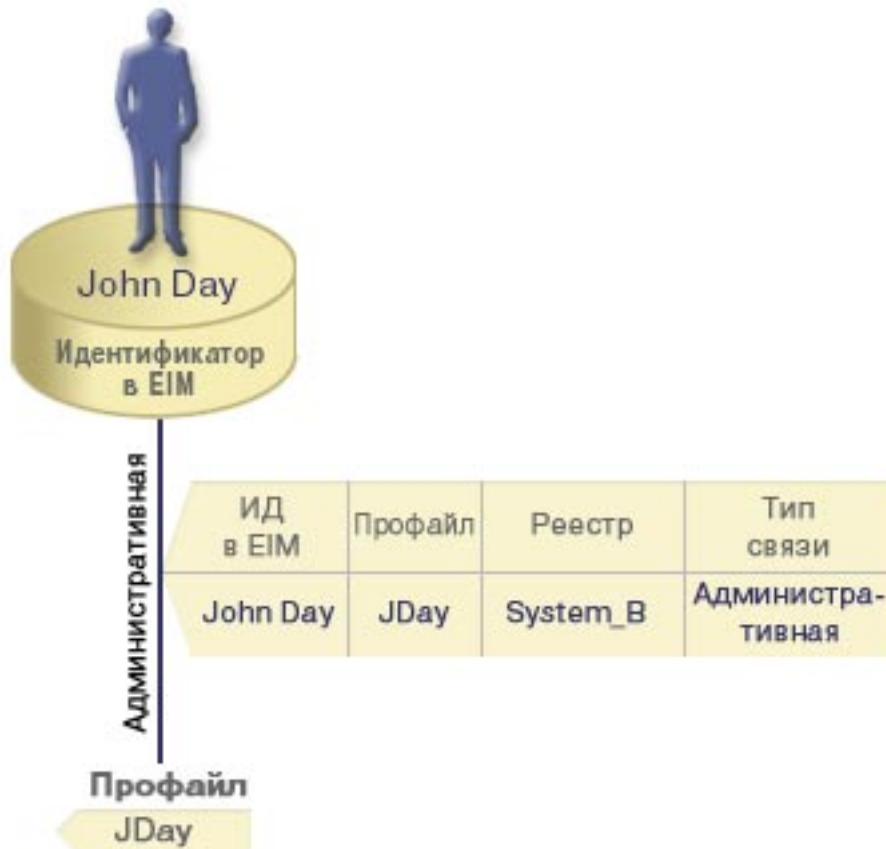
Административные связи

Административные связи применяются для идентификации того, что пользователь EIM выполняет особую функцию в той или иной системе. Этот тип связей обычно применяется при работе с реестрами пользователей, требующими особой защиты.

Операция поиска административной связи в EIM не выдает никаких результатов. Административные связи также не выдаются в качестве результата любых других операций поиска в EIM.

На рис. 7 показан пример административной связи. В данном примере пользователю John Day назначен один идентификатор в системе А и другой идентификатор в системе В, при этом система В требует особой защиты. Администратору системы нужно гарантировать то, что пользователи системы В смогут подключаться к этой системе только локально. Администратор должен запретить приложениям выполнять идентификацию пользователя John Day во внешних системах. Создав административную связь с идентификатором этого пользователя в системе В (JDay), администратор EIM указывает, что у пользователя John Day есть учетная запись в системе В, но при этом EIM не предоставляет никаких сведений об идентификаторе JDay в операциях поиска EIM. Даже приложения системы В не смогут определить, у каких пользователей EIM есть административные связи для их локальных идентификаторов в системе.

Рисунок 7: Административные связи EIM для пользователя John Day



Операции поиска в EIM

Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в некоем целевом реестре по известной им информации об этом пользователе. Операции поиска выполняются в границах домена EIM. Предусмотрено два вида операций поиска, в зависимости от типа предоставляемых исходных данных: поиск идентификаторов пользователей и поиск идентификаторов EIM.

Если приложению известен *идентификатор пользователя*, то для выполнения операции поиска оно должно указать имя определения исходного реестра EIM и имя определения целевого реестра EIM. При этом для указанного идентификатора пользователя должна существовать исходная "Связи EIM" на стр. 13.

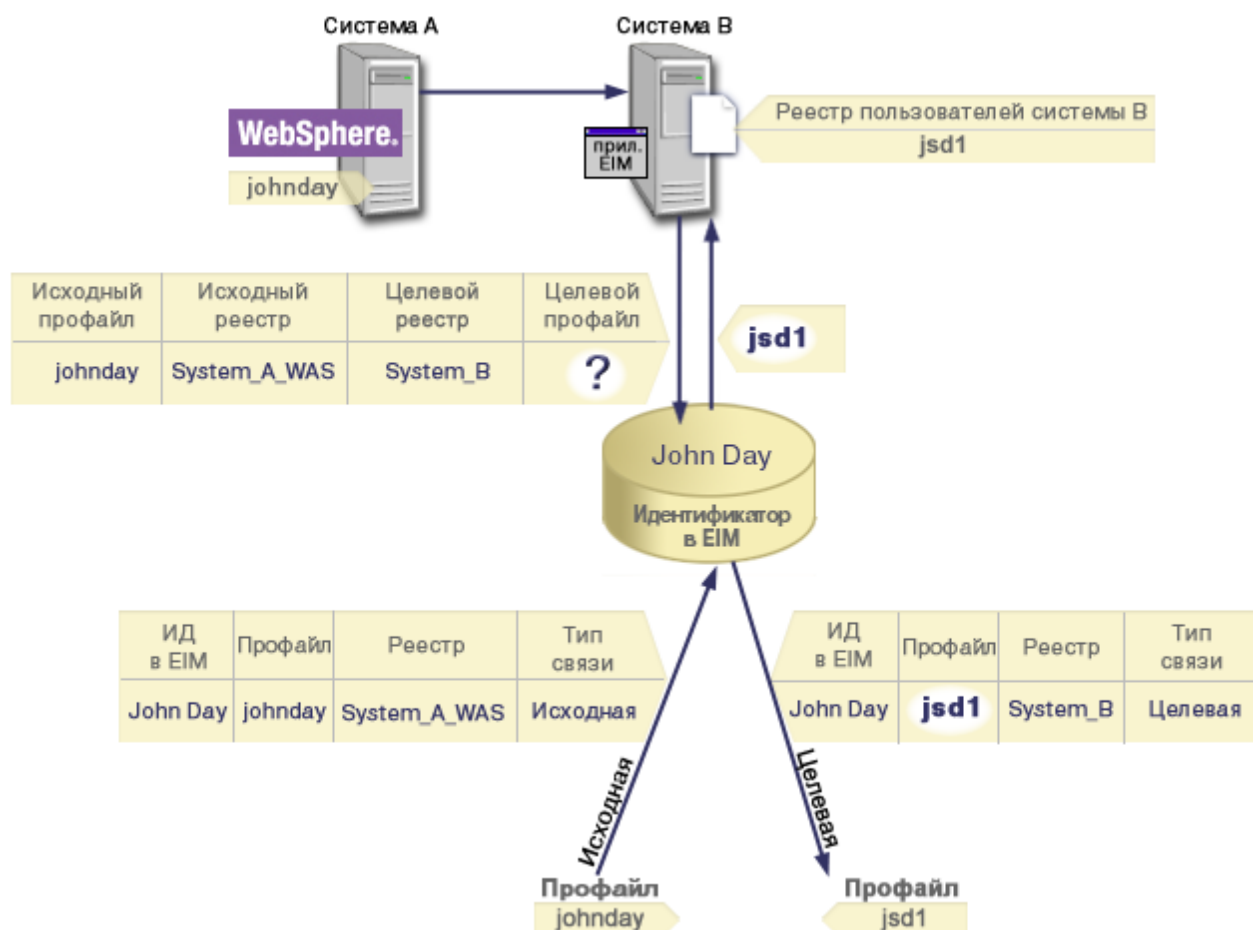
Если приложению известен *идентификатор EIM*, приложение должно предоставить имя определения целевого реестра EIM. Для успешного выполнения операции поиска в EIM для пользователя должна существовать связь в целевом реестре.

Информация, предоставленная приложением, передается контроллеру домена EIM, в котором хранятся все данные EIM, и сначала выполняется поиск исходных данных, предоставленных приложением. После того как будет определен идентификатор EIM (он либо указывается приложением напрямую, либо определяется по данным, указанным приложением), выполняется поиск целевой связи для этого идентификатора в указанном целевом реестре.

На рис. 10 пользователь johnday подключается к серверу Websphere Application Server по протоколу Lightweight Third-Party Authentication (LPTA) с системы А. Сервер Websphere Application Server в системе А вызывает программу системы В для доступа к данным системы В. Эта программа вызывает API EIM для определения прав доступа пользователя системы А. Программа предоставляет

следующие данные для выполнения операции: johnday в качестве имени пользователя, System_A_WAS в качестве исходного реестра и System_B в качестве целевого реестра. Эта информация передается контроллеру домена EIM, после чего контроллер находит исходную связь. Затем по исходной связи контроллер домена выполняет поиск целевой связи, и в результате находит пользователя John Day в реестре System_B. После этого идентификатор пользователя (jsd1) возвращается приложению.

Рисунок 10: Операция поиска в EIM по идентификатору пользователя johnday



Права доступа EIM

Права доступа определяют, какие операции пользователю разрешено выполнять в EIM. В число таких операций могут входить административные операции и операции поиска. Изменение прав доступа разрешено только администраторам EIM. Права доступа EIM могут предоставляться только пользователям, определенным на контроллере домена EIM.

Ниже приведены краткие описания функций, которые разрешено выполнять различным категориям пользователей EIM:

- **Администратор сервера LDAP.** Этой категории пользователей разрешено создание доменов EIM. Доступны следующие операции:
 - Создать домен
 - Удалить домен
 - Создать или удалить идентификатор EIM
 - Создать или удалить определение реестра EIM

- Создать или удалить исходную, целевую или административную связь
- Выполнить операцию поиска в EIM
- Получить связь, идентификатор EIM или определение реестра EIM
- Добавить, удалить или показать сведения о правах доступа EIM
- **Администратор EIM.** Этой категории пользователей разрешено изменение любых данных в домене EIM. Доступны следующие операции:
 - Удалить домен
 - Создать или удалить идентификатор EIM
 - Создать или удалить определение реестра EIM
 - Создать или удалить исходную, целевую или административную связь
 - Выполнить операцию поиска в EIM
 - Получить связь, идентификатор EIM или определение реестра EIM
 - Добавить, удалить или показать сведения о правах доступа EIM
- **Администратор идентификаторов EIM.** Этой категории пользователей разрешено изменять идентификаторы EIM, исходные и административные связи. Доступны следующие операции:
 - Создать идентификатор EIM
 - Добавить или удалить исходную связь
 - Добавить или удалить административную связь
 - Выполнить операцию поиска в EIM
 - Получить связь, идентификатор EIM или определение реестра EIM
- **Поиск в EIM.** Этой категории пользователей разрешено выполнять поиск данных в EIM. Доступны следующие операции:
 - Выполнить операцию поиска в EIM
 - Получить связь, идентификатор EIM или определение реестра EIM
- **Администратор реестров EIM.** Этой категории пользователей разрешены все операции над реестрами EIM. Доступны следующие операции:
 - Добавить или удалить целевую связь
 - Выполнить операцию поиска в EIM
 - Получить связь, идентификатор EIM или определение реестра EIM
- **Администратор конкретного реестра EIM.** Этой категории пользователей разрешены все операции над конкретным реестром EIM. Доступны следующие операции:
 - Добавить или удалить целевую связь в определении реестра EIM
 - Выполнить операцию поиска в EIM
 - Получить связь, идентификатор EIM или определение реестра EIM

Следующие таблицы упорядочены по задачам EIM. В таблица приведены сведения обо всех API EIM и категориях пользователей, которым разрешено выполнять отдельные операции с этими API.

Таблица 1: Работа с доменами

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

Таблица 2: Работа с идентификаторами

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-

Таблица 3: Работа с реестрами

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Таблица 4: Работа со связями

При вызове API `eimAddAssociation()` и `eimRemoveAssociation()` нужно указать 4 параметра, определяющие тип добавляемой или удаляемой связи. Права доступа, необходимые для выполнения операции, зависят от типа связи. В следующей таблице права доступа указаны для всех типов связей.

EIM API	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddAssociation (для административных связей)	X	X	X	-	-	-

EIM API	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddAssociation (для исходных связей)	X	X	X	-	-	-
eimAddAssociation (для исходных и целевых связей)	X	X	X	-	X	X
eimAddAssociation (для целевых связей)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (для административных связей)	X	X	X	-	-	-
eimRemoveAssociation (для исходных связей)	X	X	X	-	-	-
eimRemoveAssociation (для исходных и целевых связей)	X	X	X	-	X	X
eimRemoveAssociation (для целевых связей)	X	X	-	-	X	X

Таблица 5: Поиск

EIM API	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

Таблица 6: Работа с правами доступа

EIM API	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

Общие сведения о LDAP в рамках EIM

Технология преобразования идентификаторов в рамках предприятия (EIM) предусматривает применение сервера LDAP в качестве “Контроллер домена EIM” на стр. 6 - централизованного хранилища данных. При настройке EIM для сервера iSeries в качестве идентификационных данных для доступа к контроллеру домена используются отличительные имена LDAP.

Для эффективного применения отличительных имен LDAP при работе с EIM рекомендуем вам ознакомиться со следующими сведениями о LDAP:

- “Отличительное имя LDAP”
- “Родительское отличительное имя LDAP”

Отличительное имя LDAP

Отличительное имя (DN) LDAP - это запись простого протокола доступа к каталогам (LDAP), обозначающая и описывающая пользователя, который обладает правами доступа к серверу LDAP. Сервер LDAP настраивается с помощью мастера Настройки EIM для хранения информации домена EIM. Отличительные имена LDAP могут применяться для работы с этими данными EIM, чтобы настроить на сервере iSeries “Создание единого входа в сеть с помощью EIM” на стр. 22.

Отличительные имена состоят из имени самой записи и имен расположенных над ней в каталоге LDAP объектов, указанных в порядке возрастания уровней. Полное отличительное имя LDAP может иметь вид `cn=Tim Jones, o=IBM, c=US`. В каждой записи, по крайней мере, один атрибут содержит ее имя. Атрибут, содержащий имя, называется относительным отличительным именем (RDN) записи. Запись, расположенная над RDN, называется родительским отличительным именем LDAP. В данном примере, `cn=Tim Jones` - имя записи, то есть, RDN. `o=IBM, c=US` - родительское DN записи `cn=Tim Jones`. В разделе “Родительское отличительное имя LDAP” приведена дополнительная информация о применении этих имен в EIM.

Так как данные EIM хранятся на сервере LDAP, то для идентификации “Контроллер домена EIM” на стр. 6 может применяться отличительные имена LDAP. Настраивая EIM на сервере iSeries также можно использовать отличительные имена LDAP. Например, отличительные имена LDAP могут применяться при:

- Настройке сервера LDAP в качестве контроллера домена. Для этого создается и применяется отличительное имя LDAP, обозначающее администратора сервера LDAP. Если сервер LDAP не настроен в системе, то его можно создать в процессе создания нового домена и добавления в него сервера с помощью мастера Настройки EIM.
- Выборе в мастере Настройки EIM типа идентификатора пользователя, применяемого для подключения к контроллеру домена EIM. Отличительное имя - один из доступных типов пользователей. Отличительное имя LDAP должно представлять пользователя, обладающего правами на создание объектов в локальном пространстве имен сервера LDAP.
- Выборе в мастере Настройки EIM типа пользователя, применяемого для выполнения операций EIM от имени функций операционной системы. Эти операции включают поиск связанного идентификатора и удаление связей при удалении локального пользовательского профайла OS/400. Отличительное имя - один из доступных типов пользователей.
- Подключении к контроллеру домена для администрирования EIM, например, для управления реестрами и идентификаторами и выполнения операций поиска связанных идентификаторов.

Дополнительная информация об отличительных именах и их применении в протоколе LDAP приведена в разделе Принципы LDAP.

Родительское отличительное имя LDAP

Родительское отличительное имя (DN) LDAP - это запись в пространстве имен сервера каталогов простого протокола доступа к каталогам (LDAP). Записи сервера LDAP образуют иерархическую

структуру, которая может отражать политические, географические, организационные границы или границы областей. Отличительное имя считается родительским, если оно находится на высшем уровне пространства имен сервера LDAP.

Полное отличительное имя LDAP может иметь вид `cn=Tim Jones, o=IBM, c=US`. В каждой записи, по крайней мере, один атрибут содержит ее имя. Атрибут, содержащий имя, называется относительным отличительным именем (RDN) записи. Запись, расположенная над RDN, называется родительским отличительным именем. В данном примере, `cn=Tim Jones` - имя записи, то есть, RDN. `o=IBM, c=US` - родительское DN записи `cn=Tim Jones`.

Так как данные EIM хранятся на сервере LDAP, то для идентификации “Контроллер домена EIM” на стр. 6 может применять отличительные имена LDAP. Настраивая EIM на сервере iSeries также можно использовать “Отличительное имя LDAP” на стр. 21 и родительские отличительные имена. Например, создавая новый домен и добавляя в него сервер с помощью мастера Настройки EIM, можно указать родительское DN для создаваемого домена. Задав родительское DN, можно указать для домена расположение данных EIM в локальном пространстве имен LDAP. Если не указывать родительское DN, то данные EIM будут храниться в отдельном суффиксе в пространстве имен.

Дополнительная информация об отличительных именах и их применении приведена в разделе Принципы LDAP.

Создание единого входа в сеть с помощью EIM

EIM позволяет без лишних затрат создать на предприятии среду единого входа в сеть. Реализация EIM и Kerberos в OS/400 обеспечивает поддержку настоящей многоуровневой разнородной среды единого входа в сеть. Среда единого входа в сеть на предприятии обеспечивает следующие выгоды для пользователей, администраторов и разработчиков приложений:

Выгоды пользователей

В среде единого входа в сеть идентификации происходит при обращении пользователя к каждой новой системе; однако вводить пароль пользователю не нужно. EIM избавляет пользователей от необходимости запоминать несколько имен и паролей для работы с разными системами в сети. После того как пользователь был идентифицирован, он может работать со службами и приложениями в корпоративной сети, не вводя различные пароли для разных систем.

Выгоды администраторов

Для администратора, среда единого входа в сеть облегчает задачу управления на всем предприятии. Без единого входа в сеть пользователи и приложения могут сохранять пароли для различных систем, в результате чего снижается надежность защиты всей сети. На уменьшение этих рисков, связанных с защитой, уходит много времени и средств. Единый вход в сеть сокращает количество операций идентификации, обеспечивая, при этом, надежную защиту сети. Кроме того, среда единого входа в сеть сокращает издержки администрирования, связанные со сбросом забытых паролей.

Выгоды для разработчиков приложений

Для разработчиков приложений для неоднородных сетей EIM обеспечивает универсальную инфраструктуру для различных платформ. С помощью API EIM программисты могут создавать приложения, применяющие наиболее подходящий из существующих пользовательских реестров для идентификации и другой пользовательский реестр - для предоставления прав доступа. Разработчикам приложений не приходится реализовывать в своих программах поддержку пользовательских реестров конкретных систем, так как структура EIM позволяет создавать приложения, связывающие идентификаторы пользователей в этих реестрах с одним идентификатором EIM. Кроме того, EIM позволяет программистам не изменять семантику защиты этих приложений, а защита на уровне приложения значительно сокращает издержки разработки многоуровневых приложений, работающих на различных платформах.

Настройка единого входа в сеть на сервере iSeries

Среда единого входа в сеть реализована фирмой IBM с помощью двух применяемых совместно технологий: EIM и службы сетевой идентификации, в которой реализована поддержка Kerberos и API GSS. Настроив эти две технологии, администратор может создать среду единого входа в сеть. В системах Windows 2000, XP, AIX и zSeries протокол Kerberos применяется для идентификации пользователей в сети. В технологии Kerberos применяется сетевой защищенный центр рассылки ключей, выполняющий идентификацию субъектов (пользователей Kerberos) в сети. Пользователь получает паспорт Kerberos от центра рассылки ключей. Этот паспорт идентифицирует данного пользователя для других служб в рамках предприятия. Паспорт может быть передан пользователем службе, принимающей паспорт. Служба, принявшая паспорт, определяет и проверяет личность пользователя (в области или реестре пользователей Kerberos).

С помощью службы сетевой идентификации сервер iSeries можно добавить в область Kerberos, а EIM позволяет связать субъектов Kerberos с одним идентификатором EIM, представляющего данного пользователя в рамках всего предприятия. Другие идентификаторы пользователя, такие как имя пользователя OS/400, также можно связать с этим идентификатором EIM. С помощью этих связей EIM система OS/400 и приложения могут определить пользовательский профайл OS/400, соответствующий пользователю или объекту, который представлен субъектом Kerberos. Информацию EIM можно представить в виде дерева, корнем которого является идентификатор EIM, а ветви - список идентификаторов пользователя, связанных с данным идентификатором EIM.

На примере приведенной ниже схемы представьте, что пользователь Джон Смит входит в сеть с компьютера с операционной системой Windows и обращается к экземпляру OS/400 для работы с приложением, поддерживающим Kerberos. Джону не приходится указывать свое имя пользователя OS/400. Такие приложения могут найти соответствующее имя пользователя OS/400 с помощью связи с идентификатором EIM Джона. Джону Смиту больше не нужен пароль в его пользовательском профайле OS/400, так как этот пользовательский профайл не применяется для идентификации; он нужен только для предоставления прав доступа.

Рисунок 1. Среда единого входа в сеть



В разделе Сценарий: Настройка единого входа в сеть приведен пример настройки службы сетевой идентификации и EIM для создания среды единого входа в сеть.

Следующие приложения поддерживают единый вход в сеть:

- Навигатор iSeries
- Эмулятор PC5250
- Архитектура распределенных реляционных баз данных ^(TM)(DRDA)^(R)
- NetServer
- QFileSvr.400

Планирование работы с EIM

Технология EIM объединяет широкий набор функций и служб сервера iSeries. Перед началом настройки EIM на сервере рекомендуем вам определить, какие возможности EIM нужны в вашей среде.

Сначала нужно определить общие требования к защите сети и настроить соответствующие средства защиты. Технология EIM в значительной степени упрощает идентификации пользователей в рамках

предприятия. Совместно с функцией сетевого входа в систему технология EIM позволяет организовать единую среду входа в систему в масштабах всей организации.

Следующая таблица позволит вам определить, что нужно установить до начала настройки EIM.

Контрольная таблица по планированию	Ответы
Версия OS/400 (5722-SS1) - V5R2 или выше?	
На серверах iSeries установлен продукт Cryptographic Access Provider (5722-AC3)?	
Установлен ли продукт iSeries Access for Windows (5722-XE1) на персональных компьютерах, применяемых для работы с серверами iSeries, и на серверах iSeries?	
Установлен ли компонент Сеть Навигатора iSeries на всех PC в вашей сети и во всех системах iSeries?	
Настроен ли в сети сервер LDAP, планируете ли вы применять его в качестве контроллера домена EIM, и известны ли вам DN и пароль администратора LDAP?	
Если сервер LDAP настроен в данный момент, можно ли временно приостановить его работу? (Это потребуется на одном из этапов настройки EIM.)	
Есть ли у вас особые права доступа *SECADM, *ALLOBJ и *IOSYSCFG?	
Установлены ли последние PTF?	

Если вы планируете применять протокол Kerberos для идентификации пользователей, вам потребуется установить сетевую службу идентификации. Подробная информация об этом приведена в разделе Планирование применения сетевой службы идентификации.

Если вы планируете применять единую среду входа в систему, рекомендуем вам ознакомиться с примером, приведенным в разделе Пример:Реализация единой среды входа в систему.

Установка необходимых компонентов Навигатора

Для настройки среды единого входа в систему с помощью EIM и службы сетевой идентификации необходимо установить компоненты Навигатора Сеть и Защита. EIM входит в компонент Сеть, а служба сетевой идентификации - в компонент Защита. Если применение службы сетевой идентификации не планируется, то устанавливать компонент Навигатора Защита не нужно.

Для того чтобы установить компонент Навигатора Сеть или проверить его установку, убедитесь в том, что на PC, с помощью которого осуществляется управление сервером iSeries, установлен продукт iSeries Access for Windows.

Для установки компонента Сеть:

1. Выберите **Пуск** → **Программы** → **IBM iSeries Access for Windows** → **Выборочная установка**.
2. Следуйте инструкциям, приведенным в окне. В окне **Выбор компонентов** разверните **Навигатор** и выберите опцию **Сеть**.
Для применения службы сетевой идентификации необходимо также установить компонент **Защита**.
3. Выполните все остальные этапы Выборочной установки.

Настройка службы сетевой идентификации

Служба сетевой идентификации позволяет применять функции идентификации Kerberos на сервере iSeries. EIM может применяться на сервере и без этой службы; однако применение защиты Kerberos в системе обеспечивает множество преимуществ.

Применение службы сетевой идентификации вместе с EIM позволяет настроить “Создание единого входа в сеть с помощью EIM” на стр. 22. Среда единого входа в систему облегчает работу пользователей и администраторов. Пользователям приходится запоминать меньше имен и паролей, а администраторам - отслеживать меньше информации о каждом пользователе. Так как среда единого входа в систему обеспечивает универсальный интерфейс для всех платформ и различных систем, которые могут быть объединены в одну сеть, то снижаются издержки разработки приложений и управления сетью.

Если служба сетевой идентификации не настроена на данном сервере iSeries и на всех серверах в сети, то ознакомьтесь рекомендациями по планированию, приведенными в разделе Планирование службы сетевой идентификации. Если вы уже работали со службой сетевой идентификации, то перейдите к разделу Настройка службы сетевой идентификации, чтобы начать процедуру настройки.

Настройка EIM

Для применения единого входа в сеть в нескольких операционных системах без внесения изменений в соответствующие стратегии защиты необходимо настроить EIM и службу сетевой идентификации. Однако настройка службы сетевой идентификации не является предварительным требованием для настройки и применения EIM.

В начале процедуры настройки EIM на сервере iSeries для применения функции единого входа в сеть используется мастер Настройки EIM. В зависимости от существующей конфигурации и потребностей, с помощью этого мастера можно присоединиться к существующему домену или создать новый домен и присоединиться к нему.

Мастер настройки EIM позволяет без затруднений создать базовую конфигурацию EIM. Например, если еще не настроен сервер LDAP или служба сетевой идентификации, то мастер Настройки EIM позволяет выполнить эти задачи.

Создав с помощью мастера базовую конфигурацию EIM, необходимо выполнить некоторые дополнительные операции для настройки среды единого входа в сеть. Пример настройки в вымышленной компании среды единого входа в сеть с помощью службы сетевой идентификации и EIM приведен в разделе Сценарий: Настройка единого входа в сеть.

Перед непосредственной настройкой функции с помощью мастера Настройки EIM необходимо выполнить все операции “Планирование работы с EIM” на стр. 24, чтобы определить, как именно будет применяться EIM и служба сетевой идентификации для реализации среды единого входа в сеть. Завершив планирование, можно с помощью мастера настроить EIM на сервере iSeries двумя способами: создав новые домены или присоединившись к существующим. В следующих разделах приведены инструкции по настройке EIM:

“Создание нового домена и присоединение к нему” на стр. 27

Эта задача позволяет создать домен EIM для сети и добавить в этот домен сервер iSeries. Мастер создает новый домен и настраивает в качестве его контроллера локальный сервер LDAP. Кроме того, если на сервере iSeries не настроены функции Kerberos, то мастер предлагает запустить Мастер настройки Службы сетевой идентификации. Выполнив эту задачу, можно добавить серверы iSeries в созданный домен. Для добавления других серверов в этот домен, установите соединение с каждым из них и добавьте эти серверы с помощью мастера Настройки EIM.

“Присоединение к существующему домену” на стр. 30

Настроив с помощью мастера Настройки EIM контроллер домена и домен EIM, выберите эту задачу, чтобы добавить другие серверы iSeries в созданный домен. Эту задачу необходимо выполнить для каждого сервера iSeries в сети, на котором будет применяться EIM. По завершении работы мастера следует ввести информацию о домене, в который добавляется сервер, включая сведения о соединении (например, номер порта и информацию о применении

защиты Transport Layer Security (TLS)/Secure Sockets Layer (SSL) в контроллере домена EIM. Если на сервере iSeries не настроены функции Kerberos, то мастер предлагает запустить Мастер настройки Службы сетевой идентификации.

Запуск мастера Настройки EIM

Для запуска мастера Настройки EIM выполните следующие действия:

1. Запустите Навигатор.
2. Войдите на сервер iSeries, для которого необходимо настроить EIM. Если EIM настраивается для нескольких серверов iSeries, то начните с сервера, на котором будет настроен контроллер домена EIM.
3. Разверните **Сеть** → **EIM**.
4. Щелкните правой кнопкой мыши **Конфигурация** и выберите **Настроить...**, чтобы запустить мастер Настройки EIM.
5. Выберите способ **Присоединиться к существующему домену** или **Создать домен и присоединиться к нему**.

Настроив с помощью мастера Настройки EIM контроллер домена и добавив в домен серверы iSeries, необходимо выполнить следующие задачи, чтобы завершить настройку EIM:

1. “Добавление пользовательского реестра” на стр. 38 в домен EIM для других серверов и приложений, которые будут входить в домен EIM.
2. “Создание идентификатора EIM” на стр. 36 в домене для каждого уникального пользователя или объекта системы, входящих в домен EIM.
3. “Создание связи” на стр. 35 между различными идентификаторами пользователей или объектов с созданными идентификаторами EIM.

Создание нового домена и присоединение к нему

Мастер Настройки EIM позволяет настроить на сервере iSeries сервер LDAP в качестве “Контроллер домена EIM” на стр. 6. При необходимости, мастер настройки EIM проверяет наличие данных базовой конфигурации сервера LDAP.

Кроме того, если на сервере iSeries не настроены функции Kerberos, то мастер предлагает запустить Мастер настройки Службы сетевой идентификации. По завершении работы этого мастера создается новый домен EIM, текущий сервер iSeries добавляется в этот домен, и заданные пользовательские реестры добавляются в домен.

Для выполнения этой задачи с помощью данного мастера необходимы специальные права доступа системного администратора (*SECADM), права доступа ко всем объектам (*ALLOBJ) и права на настройку системы (*IOSYSCFG).

Для того чтобы запустить мастер Настройки EIM, создать новый домен EIM и добавить в него сервер, выполните следующие действия в Навигаторе:

Примечание: Этот мастер также настраивает локальный сервер LDAP в качестве контроллера создаваемого домена EIM.

1. Откройте **Сеть** → **EIM**.
2. Щелкните правой кнопкой мыши **Конфигурация** и выберите **Настроить...**, чтобы запустить мастер Настройки EIM.
3. На **Начальной** странице мастера выберите **Создать домен и присоединиться к нему** и нажмите кнопку **Далее**.
4. Если служба сетевой идентификации не настроена на сервере iSeries, то откроется окно **Настройка служб сетевой идентификации**. В этом окне предлагается настроить службу

сетевой идентификации. Если нажать кнопку **Да**, то будет запущен мастер настройки службы сетевой идентификации. По завершении настройки службы сетевой идентификации продолжается работа мастера Настройки EIM.

5. Если локальный сервер LDAP не настроен, то откроется окно **Настройка сервера каталогов**. Введите в этом окне следующие данные, чтобы настроить локальный сервер LDAP:
 - В поле **Порт** подтвердите номер порта по умолчанию, **389**, или другой номер порта для незащищенного обмена данными EIM с сервером каталогов.
 - В поле **Отличительное имя** укажите отличительное имя LDAP администратора сервера LDAP. Мастер Настройки EIM создает это DN администратора LDAP и с его помощью настраивает сервер LDAP в качестве контроллера создаваемого домена.
 - В поле **Пароль** введите пароль для администратора LDAP.
 - В поле **Подтверждение пароля** введите этот пароль еще раз.
 - Нажмите кнопку **Далее**.
6. В окне **Укажите контроллер домена** введите следующие данные:
 - В поле **Домен** укажите имя создаваемого домена EIM. Подтвердите имя **EIM**, указанное по умолчанию, или введите другое имя. Имя не может содержать такие специальные символы, как = + < > , # ; \ и *.
 - В поле **Описание** введите описание этого домена.
 - Нажмите кнопку **Далее**.
7. В окне **Укажите родительское DN домена** можно указать родительское DN для создаваемого домена. Задав родительское DN, можно указать для домена расположение данных EIM в локальном пространстве имен LDAP. Если не указывать родительское DN, то данные EIM будут храниться в отдельном суффиксе в пространстве имен. Для того чтобы указать родительское DN, выберите из списка локальный суффикс LDAP или введите текст для создания нового родительского DN. Указывать родительское DN для создаваемого домена необязательно.
8. В окне **Укажите пользователя для соединения** выберите **тип пользователя** для соединения. Доступны следующие типы пользователей: Отличительное имя и пароль, файл ключей и субъект Kerberos или субъект и пароль Kerberos. Типы пользователей, связанные с Kerberos, можно выбрать только в том случае, если на локальном сервере iSeries установлена служба сетевой идентификации. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:
 - Если выбрано **Отличительное имя и пароль**, то введите следующие данные:
 - В поле **Отличительное имя** укажите отличительное имя (DN) администратора сервера LDAP, обладающего правами на создание объектов в локальном пространстве имен сервера LDAP. Если на одном из предыдущих этапов с помощью этого мастера был настроен сервер LDAP, то укажите отличительное имя администратора LDAP, заданное на том этапе.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз.
 - Если выбрано **Файл ключей и субъект Kerberos**, то введите следующие данные:
 - В поле **Файл ключей** укажите имя файла ключей на сервере iSeries для пользователя, обладающего правами на создание объектов в локальном пространстве имен сервера LDAP. Вместо этого, можно нажать кнопку **Обзор** и выбрать файл ключей.
 - В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
 - В поле **Область** введите имя области Kerberos для этого субъекта. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
 - Если выбрано **Субъект Kerberos и пароль**, то введите следующие данные:

- В поле **Субъект** укажите имя субъекта Kerberos, соответствующее пользователю, который обладает правами на создание объектов в локальном пространстве имен сервера LDAP.
 - В поле **Область** введите имя области Kerberos для этого субъекта.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
- Выберите **Проверить соединение**, чтобы проверить информацию о пользователе для подключения к контроллеру домена.
 - Нажмите кнопку **Далее**.
9. В окне **Информация реестра** выберите тип пользовательских реестров для добавления в домен EIM. Выберите один из типов пользовательских реестров или оба типа:
- Выберите **OS400** для добавления пользовательского реестра, представляющего локальный реестр в домене EIM. Введите в соответствующем поле имя реестра для создания в домене. Имя реестра EIM - произвольная строка, обозначающая тип реестра и отдельный экземпляр этого реестра.
 - Выберите **Kerberos** для добавления домен EIM пользовательского реестра Kerberos. Введите в соответствующем поле имя реестра для создания в домене, выбрав, при необходимости, опцию **В идентификаторах пользователей Kerberos учитывается регистр символов**.
 - Нажмите кнопку **Далее**.
10. В окне **Укажите пользователя системы EIM** выберите тип пользователя, с помощью которого система будет выполнять операции EIM от имени функций операционной системы. Эти операции включают поиск связанного идентификатора и удаление связей при удалении локального пользовательского профайла OS/400. Доступны следующие типы пользователей: Отличительное имя и пароль, файл ключей и субъект Kerberos или субъект и пароль Kerberos. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:

Примечание: Указанный пользователь должен, по крайней мере, обладать правами на поиск связанных идентификаторов и управление реестрами локальных пользователей. Если у заданного пользователя нет этих прав доступа, то некоторые функции операционной системы, связанные с единым входом в сеть и удалением пользовательских профайлов, могут не работать.

11. Если выбрано **Отличительное имя и пароль**, то введите следующие данные:
- В поле **Отличительное имя** укажите отличительное имя, обозначающее пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз.
12. Если выбрано **Субъект Kerberos и пароль**, то введите следующие данные:
- В поле **Субъект** укажите имя субъекта Kerberos, обозначающее пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM.
 - В поле **Область** введите имя области Kerberos для этого субъекта.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
13. Если выбрано **Файл ключей и субъект Kerberos**, то введите следующие данные:
- В поле **Файл ключей** укажите имя файла ключей на сервере iSeries для пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM. Вместо этого, можно нажать кнопку **Обзор** и выбрать файл ключей.

- В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
 - В поле **Область** введите имя области Kerberos для этого субъекта. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
14. Выберите **Проверить соединение**, чтобы проверить соединение созданного системного пользователя с контроллером домена.
 15. Нажмите кнопку **Далее**.
 16. На панели **Отчет** проверьте указанную информацию о конфигурации. Если все данные указаны верно, нажмите кнопку **Готово**.

По завершении работы мастера будет создана базовая конфигурация EIM. Однако для завершения настройки EIM для данного сервера, необходимо выполнить следующие задачи:

1. “Добавление домена в папку Управление доменами” на стр. 34 в папку Управление доменами EIM.
2. “Добавление пользовательского реестра” на стр. 38 в домен EIM для других серверов и приложений, которые будут входить в домен EIM.
3. “Создание идентификатора EIM” на стр. 36 в домене для каждого уникального пользователя или объекта системы, входящих в домен EIM.
4. “Создание связи” на стр. 35 между различными идентификаторами пользователей или объектов с созданными идентификаторами EIM.

Кроме того, можно с помощью Secure Sockets Layer (SSL) или Transport Layer Security (TLS) “Настройка защищенного соединения с контроллером домена EIM”.

Настройка защищенного соединения с контроллером домена EIM

“Создание нового домена и присоединение к нему” на стр. 27 с помощью мастера Настройки, можно настроить защищенное соединение с контроллером домена EIM с помощью протоколов Secure Sockets Layer (SSL) или Transport Layer Security Protocol (TLS). Для того чтобы настроить поддержку SSL или TLS для EIM, необходимо выполнить следующие задачи:

1. Настроить SSL для сервера LDAP, выполняющего функции контроллера домена.
2. С помощью Диспетчера цифровых сертификатов (DCM) создать сертификат, необходимый для обеспечения поддержки SSL на сервере LDAP.
3. С помощью DCM to присвоить этот сертификат серверу LDAP.
4. В свойствах конфигурации EIM указать, что на сервере iSeries применяется защищенное соединение SSL.
5. Указать в свойствах всех доменов EIM, что для управления доменом с помощью Навигатора применяется соединение SSL.

Присоединение к существующему домену

Мастер Настройки EIM позволяет добавить сервер в существующий домен EIM. Для применения этой функции мастера Настройки EIM необходимо, чтобы в сети был настроен домен EIM и контроллер этого домена. В мастере необходимо указать информацию о домене, включая сведения о соединении с контроллером домена EIM. Мастер сохраняет эти данные на сервере iSeries и затем с их помощью устанавливает соединение с контроллером домена EIM. Мастер также создает пользовательский реестр EIM, представляющий реестр пользовательских профайлов OS/400 на данном сервере iSeries.

Для выполнения этой задачи с помощью данного мастера необходимы специальные права доступа системного администратора (*SECADM) и права доступа ко всем объектам (*ALLOBJ).

Для того чтобы запустить мастер Настройки EIM и добавить сервер в существующий домен EIM, выполните следующие действия в Навигаторе:

1. Разверните **Сеть** → **EIM**.
2. Щелкните правой кнопкой мыши **Конфигурация** и выберите **Настроить...**, чтобы запустить мастер Настройки EIM. После запуска мастера введите в полях форм следующие данные:
3. На **начальной** странице мастера выберите опцию **Присоединиться к существующему домену** и нажмите кнопку **Далее**.
4. Если служба сетевой идентификации не настроена на сервере iSeries, то откроется окно **Настройка служб сетевой идентификации**. В этом окне предлагается настроить службу сетевой идентификации. Если нажать кнопку **Да**, то будет запущен мастер настройки службы сетевой идентификации. По завершении настройки службы сетевой идентификации продолжается работа мастера Настройки EIM.
5. В окне **Укажите контроллер домена** введите следующие данные:
 - В поле **Имя контроллера домена** укажите имя системы, выполняющей функции контроллера домена, в который необходимо добавить сервер iSeries.
 - Нажмите **Применять Secure Sockets Layer (SSL)** для применения защиты SSL при получении данных EIM от контроллера домена.
 - Выберите **Проверить соединение**, чтобы проверить конфигурацию контроллера домена.

Примечание: Если была выбрана опция защиты SSL и получено сообщение об ошибке, то, возможно, на сервере LDAP не настроены функции SSL.

- Нажмите кнопку **Далее**.
6. В окне **Укажите пользователя для соединения** выберите **тип пользователя** для соединения. Доступны следующие типы пользователей: Отличительное имя и пароль, файл ключей и субъект Kerberos или субъект и пароль Kerberos. Типы пользователей, связанные с Kerberos, можно выбрать только в том случае, если на локальном сервере iSeries установлена служба сетевой идентификации. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:
 - Если выбрано **Отличительное имя и пароль**, то введите следующие данные:
 - В поле **Отличительное имя** укажите отличительное имя (DN) администратора сервера LDAP, обладающего правами на создание объектов в локальном пространстве имен сервера LDAP.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз.
 - Если выбрано **Файл ключей и субъект Kerberos**, то введите следующие данные:
 - В поле **Файл ключей** укажите имя файла ключей на сервере iSeries для пользователя, обладающего правами на создание объектов в локальном пространстве имен сервера LDAP. Вместо этого, можно нажать кнопку **Обзор** и выбрать файл ключей.
 - В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
 - В поле **Область** введите имя области Kerberos для этого субъекта. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
 - Если выбрано **Субъект Kerberos и пароль**, то введите следующие данные:
 - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее пользователю, который обладает правами на создание объектов в локальном пространстве имен сервера LDAP.
 - В поле **Область** введите имя области Kerberos для этого субъекта.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.

- Выберите **Проверить соединение**, чтобы проверить информацию о пользователе для подключения к контроллеру домена.
 - Нажмите кнопку **Далее**.
7. На странице **Укажите домен** выберите имя домена, в которых необходимо добавить сервер, и нажмите кнопку **Далее**.
8. В окне **Информация реестрах** выберите тип пользовательских реестров для добавления в домен EIM. Выберите один из типов пользовательских реестров или оба типа:
- Выберите **OS400** для добавления пользовательского реестра, представляющего локальный реестр в домене EIM. Введите в соответствующем поле имя реестра для создания в домене. Имя реестра EIM - произвольная строка, обозначающая тип реестра и отдельный экземпляр этого реестра.
 - Выберите **Kerberos** для добавления домен EIM пользовательского реестра Kerberos. Введите в соответствующем поле имя реестра для создания в домене, выбрав, при необходимости, опцию **В идентификаторах пользователей Kerberos учитывается регистр символов**. Можно принять значение по умолчанию; имя реестра Kerberos совпадает с именем области. Применение совпадающих имен реестра Kerberos и домена может повысить производительность получения информации из реестра. Дополнительная информация об определении пользовательских реестров в EIM приведена в разделе "Определения реестров EIM" на стр. 10.
 - Нажмите кнопку **Далее**.
9. В окне **Укажите пользователя системы EIM** выберите тип пользователя, с помощью которого система будет выполнять операции EIM от имени функций операционной системы. Эти операции включают поиск связанного идентификатора и удаление связей при удалении локального пользовательского профайла OS/400. Доступны следующие типы пользователей: Отличительное имя и пароль, файл ключей и субъект Kerberos или субъект и пароль Kerberos. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:
- Если выбрано **Отличительное имя и пароль**, то введите следующие данные:
 - В поле **Отличительное имя** укажите отличительное имя, обозначающее пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз.
 - Если выбрано **Субъект Kerberos и пароль**, то введите следующие данные:
 - В поле **Субъект** укажите имя субъекта Kerberos, обозначающее пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM.
 - В поле **Область** введите имя области Kerberos для этого субъекта.
 - В поле **Пароль** введите пароль для пользователя.
 - В поле **Подтверждение пароля** введите этот пароль еще раз. Имена субъекта и области уникально определяют пользователей Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.
 - Если выбрано **Файл ключей и субъект Kerberos**, то введите следующие данные:
 - В поле **Файл ключей** укажите имя файла ключей на сервере iSeries для пользователя OS/400, под управлением профайла которого устанавливается соединение с контроллером домена EIM. Вместо этого, можно нажать кнопку **Обзор** и выбрать файл ключей.
 - В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
 - В поле **Область** введите имя области Kerberos для этого субъекта.
 - Выберите **Проверить соединение**, чтобы проверить соединение созданного системного пользователя.
 - Нажмите кнопку **Далее**.

10. На панели **Отчет** проверьте указанную информацию о конфигурации. Если все данные указаны верно, нажмите кнопку **Готово**.

По завершении работы мастера будет создана базовая конфигурация EIM. Однако для завершения настройки EIM для данного сервера, необходимо выполнить следующие задачи:

1. “Добавление домена в папку Управление доменами” на стр. 34, в который вошел сервер, в папку Управление доменами EIM.
2. “Добавление пользовательского реестра” на стр. 38 в домен EIM для других серверов и приложений, которые будут входить в домен EIM.
3. “Создание идентификатора EIM” на стр. 36 в домене для каждого уникального пользователя или объекта системы, входящих в домен EIM.
4. “Создание связи” на стр. 35 между различными идентификаторами пользователей или объектов с созданными идентификаторами EIM.

Кроме того, для применения среды единого входа в систему необходимо настроить службу сетевой идентификации на данном сервере iSeries.

Управление EIM

Настроив EIM на сервере iSeries, можно приступить к выполнению различных задач по управлению доменом и информацией EIM. В следующих разделах описаны конкретные задачи управления EIM на сервере iSeries в корпоративной сети.

“Управление доменами EIM”

Работа с информацией EIM в домене EIM и свойствах домена EIM.

“Управление связями” на стр. 34

Управление связями между идентификаторами пользователей и идентификаторами EIM всех пользователей сети предприятия.

“Управление идентификаторами EIM” на стр. 36

Управление идентификаторами EIM, связанными с пользователями предприятия.

“Управление правами доступа пользователей EIM” на стр. 37

Обеспечение защиты информации EIM с помощью прав доступа EIM, определяющих функции EIM, которые могут выполнять пользователи.

“Управление пользовательскими реестрами” на стр. 38

Работа с пользовательскими реестрами, добавленными в домен EIM.

Управление доменами EIM

Навигатор позволяет осуществлять управление всеми доменами EIM. Для управления доменом EIM этот домен должен находиться в папке Навигатора Управление доменами. Для управления информацией в домене, “Создание нового домена и присоединение к нему” на стр. 27, необходимо добавить его в папку Управление доменами.

С помощью любого соединения с iSeries можно управлять любым доменом EIM, расположенным в той же сети. Для управления доменом не нужно, чтобы сервер iSeries, с которым установил соединение Навигатор, входил в этот домен.

Существуют следующие задачи управления доменом EIM:

- “Добавление домена в папку Управление доменами” на стр. 34
- “Подключение к домену” на стр. 34
- “Удаление домена” на стр. 34

- “Удаление домена из папки Управление доменами”

Добавление домена в папку Управление доменами

Для добавления домена необходимы права доступа *SECADM. Для добавление существующего домена EIM в папку Управление доменами выполните следующие действия.

1. Разверните **Сеть** → **EIM**.
2. Щелкните правой кнопкой мыши на папке **Управление доменами** и выберите **Добавить домен....**
3. Укажите обязательные сведения домене и соединении.
4. Нажмите **ОК**, чтобы добавить домен.

Подключение к домену

Если соединение с необходимым доменом EIM не установлено, то его следует установить. Подключиться к домену EIM можно даже в том случае, если сервер iSeries не входит в этот домен.

Для подключения к домену EIM выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Выберите домен, с которым необходимо установить соединение. Если нужный домен отсутствует в списке, то следует “Добавление домена в папку Управление доменами”.
3. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение и выберите пункт **Установить соединение....**
4. Укажите тип пользователя и обязательные сведения о пользователе для подключения к контроллеру домена EIM.
5. Нажмите кнопку **ОК**.

Удаление домена

Для выполнения этой задачи необходимы права доступа администратора LDAP или EIM. Перед удалением домена EIM следует сначала удалить все реестры и информацию об идентификаторах EIM из этого домена.

Для удаления домена EIM выполните следующие действия.

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Удалите из домена EIM все пользовательские реестры.
3. Удалите из домена EIM все идентификаторы EIM.
4. Щелкните правой кнопкой мыши на удаляемом домене и выберите пункт **Удалить....**
5. В окне **Подтверждение удаления** нажмите кнопку **Да**.

Удаление домена из папки Управление доменами

После внесения всех необходимых изменений ненужный домен EIM можно удалить из папки Управление доменами.

Для удаления домена выполните следующие действия:

1. Разверните **Сеть** → **EIM**.
2. Щелкните правой кнопкой мыши на папке **Управление доменами** и выберите **Удалить домен....**
3. Выберите в папке Управление доменами удаляемый домен EIM.
4. Нажмите кнопку **ОК**, чтобы удалить этот домен.

Управление связями

“Связи EIM” на стр. 13 определяет отношение между “Идентификатор EIM” на стр. 7 и пользователем в реестре. Например, можно создать связь между пользовательским профайлом OS/400 или

субъектом Kerberos и идентификатором EIM. С помощью этой связи можно определить, какой идентификатор EIM соответствует локальному пользовательскому профайлу iSeries или субъекту Kerberos.

Создание и сохранение связей между идентификаторами пользователей и соответствующими идентификаторами EIM значительно упрощает выполнение задач администрирования, целью которых является ведение учета учетных записей пользователей в различных системах в сети.

Управление этими связями позволяет применять в сети “Создание единого входа в сеть с помощью EIM” на стр. 22. Для применения функции единого защищенного входа в сеть необходимо своевременно вносить изменения в эти связи.

Существует три типа связей: исходная, целевая и административная. Для создания и обслуживания связей между идентификаторами пользователей и соответствующими идентификаторами EIM можно выполнять следующие задачи:

- “Создание связи”
- “Удаление связи”

Создание связи

Для реализации среды с единым входом в сеть необходимо создать “Связи EIM” на стр. 13 между различными идентификаторами пользователя или объекта и одним “Идентификатор EIM” на стр. 7 этого пользователя или объекта. Существует три типа связей: целевая, исходная и административная.

Для создания исходной или административной связи необходимы права доступа администратора идентификаторов или администратора EIM. Для создания целевой связи необходимы права доступа администратора всех реестров, администратора конкретного реестра или права доступа администратора EIM.

Для создания связи с идентификатором EIM выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM.
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы** чтобы просмотреть список идентификаторов EIM.
5. Щелкните правой кнопкой мыши на необходимом идентификаторе EIM и выберите **Свойства...**
6. Выберите вкладку **Связи**.
7. Нажмите **Добавить...** чтобы открыть окно **Добавить связь**.
8. Выберите **Справка** для получения дополнительной информации по заполнению полей.
9. Указав все необходимые значения, нажмите **ОК**.

Удаление связи

Для удаления административной или исходной связи необходимы права доступа администратора идентификаторов или администратора EIM. Для удаления целевой связи необходимы права доступа администратора для выбранных реестров (включая целевой реестр), администратора реестров или администратора EIM.

Для удаления связи выполните следующие действия.

1. Разверните **Сеть** → **EIM** → **Управление доменами**.

2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**.
5. Щелкните правой кнопкой мыши на необходимом идентификаторе EIM и выберите **Свойства...**
6. Выберите вкладку **Связи** чтобы просмотреть текущие связи идентификатора EIM.
7. Выберите связь для удаления.
8. Щелкните **Удалить**, чтобы удалить связи.
9. Нажмите кнопку **ОК**.

Управление идентификаторами EIM

Обслуживание “Идентификатор EIM” на стр. 7, представляющих пользователей сети, играет ключевую роль в обеспечении защиты. Список пользователей на предприятии практически постоянно меняется, одни сотрудники приходят, другие - увольняются, а третьи - переезжают из одного офиса в другой. Эти изменения обуславливают необходимость контроля за учетными записями пользователей и их доступом к системам сети. Создание и связывание идентификаторов EIM со всеми идентификаторами каждого пользователя значительно упрощает эту задачу.

“Создание единого входа в сеть с помощью EIM” на стр. 22 облегчает также адаптацию сотрудника при переходе в другой отдел предприятия. При смене рабочего места могут измениться права доступа и процедура входа в систему. Функция единого входа в сеть избавляет пользователей от необходимости запоминать новые имена пользователей и пароли для новых систем.

Управление идентификаторами EIM пользователей на предприятии включает выполнение множества повседневных задачи. Для управления идентификаторами EIM в сети и доменах предназначены следующие задачи:

- “Создание идентификатора EIM”
- “Добавление псевдонима для идентификатора EIM” на стр. 37
- “Удаление идентификатора EIM” на стр. 37

Информация об управление связями приведена в разделе “Управление связями” на стр. 34.

Создание идентификатора EIM

Для создания идентификатора EIM необходимы права доступа администратора идентификаторов или администратора EIM.

Для создания идентификатора EIM для пользователя или объекта выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке **Управление доменами**, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши **Идентификаторы** и выберите пункт **Создать идентификатор...**
5. Выберите **Справка** для получения дополнительной информации по заполнению полей.

6. Указав все необходимые значения, нажмите **ОК**.

Добавление псевдонима для идентификатора EIM

Пользователь может создать псевдоним для применения в качестве дополнительного отличительного имени “Идентификатор EIM” на стр. 7. Такие псевдонимы могут применяться для того, чтобы различать идентификаторы EIM. Например, если в системе есть два пользователя с именем Иванов И.И., то для того чтобы различить этих пользователей было легче, одному из них можно присвоить псевдоним Иванов Иван Иванович, а другому - Иванов Илья Ильич.

Для добавления псевдонима для идентификатора необходимы права доступа администратора идентификаторов или администратора EIM.

Для добавления псевдонима для идентификатора EIM выполните следующие действия.

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши на необходимом идентификаторе EIM и выберите **Свойства**. Если идентификаторы EIM не созданы, то перейдите к разделу “Создание идентификатора EIM” на стр. 36.
5. Укажите имя псевдонима для данного идентификатора EIM и выберите **Добавить**.
6. Нажмите кнопку **ОК**, чтобы сохранить изменения.

Удаление идентификатора EIM

Для удаления идентификатора EIM необходимы права доступа администратора EIM.

Для удаления идентификатора EIM выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**.
5. Выберите идентификаторы EIM для удаления.
6. Щелкните правой кнопкой мыши на удаляемых идентификаторах и выберите пункт **Удалить**.
7. В окне **Подтверждение удаления** нажмите кнопку **Да**, чтобы удалить выбранные идентификаторы EIM.

Управление правами доступа пользователей EIM

В EIM определено несколько типов прав доступа EIM, необходимых для выполнения различных операций в домене. К этим операциям относятся такие функции управления доменом, как создание идентификаторов, просмотр реестров и “Операции поиска в EIM” на стр. 16. Наделять и лишать других пользователей прав доступа могут только пользователи, обладающие правами доступа администратора EIM.

Краткое описание каждой группы прав доступа и подробные сведения о доступе, обеспечиваемом каждым из типов прав доступа к определенным функциям EIM, приведены в разделе “Права доступа EIM” на стр. 17.

Для изменения прав доступа EIM пользователя выполните следующие действия:

1. Откройте в Навигаторе **Сеть** → **EIM** → **Управление доменами**.
2. Разверните необходимый домен EIM. Если соединение с данным доменом не установлено, появится приглашение на подключение. Установите соединение с доменом, с помощью учетной записи пользователя, обладающего правами доступа администратора EIM.
3. Щелкните правой кнопкой мыши на этом домене EIM и выберите пункт **Права доступа...**
4. В окне **Изменение прав доступа EIM** укажите пользователя, для которого необходимо изменить права доступа EIM.
5. Нажмите кнопку **ОК**.
6. В окне **Изменение прав доступа EIM** внесите необходимые изменения в права доступа выбранного пользователя.
7. Затем нажмите кнопку **ОК**, чтобы сохранить изменения.

Управление пользовательскими реестрами

Перед “Создание связи” на стр. 35 между идентификаторами в пользовательских реестрах и соответствующими “Идентификатор EIM” на стр. 7 необходимо определить в домене EIM пользовательский реестр:

Следующие задачи применяются для управления пользовательскими реестрами в домене EIM.

- “Добавление пользовательского реестра”
- “Добавление псевдонима в пользовательский реестр” на стр. 39
- “Определение частного типа пользовательского реестра в EIM” на стр. 39
- “Удаление пользовательского реестра” на стр. 40
- “Удаление псевдонима из пользовательского реестра” на стр. 41

Добавление пользовательского реестра

Для добавления пользовательского реестра необходимы права доступа администратора EIM. Подробные сведения об этих правах доступах и полномочиях обладающего ими пользователя приведены в разделе “Права доступа EIM” на стр. 17.

Для добавления пользовательского реестра в домен EIM выполните следующие действия.

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Установите соединение с необходимым доменом EIM под управлением пользовательского профайла с правами доступа администратора EIM.
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши на пункте **Пользовательские реестры** и выберите **Добавить реестр...**
5. Укажите обязательные сведения о пользовательском реестре. Кроме того, можно задать для пользовательского реестра информацию о псевдониме.
6. Щелкните **ОК**, чтобы сохранить информацию и добавить пользовательский реестр в домен EIM.

Добавление псевдонима в пользовательский реестр

Пользователь или разработчик приложения может создать псевдоним для применения в качестве дополнительного отличительного имени пользовательского реестра. Такие псевдонимы могут применяться для того, чтобы различать пользовательские реестры. Например, разработчики приложений и администраторы с помощью псевдонимов пользовательских реестров указывают, какие реестры EIM должно применять приложение. Информация о применении псевдонимов с пользовательскими реестрами приведена в разделе “Определения реестров EIM” на стр. 10.

Для добавления псевдонима в пользовательский реестр необходимо обладать одними из следующих прав доступа: администратора EIM, администратора всех реестров, администратора реестра, для которого выполняется эта задача.

Для добавления псевдонима в пользовательский реестр в домене EIM выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Пользовательские реестры**, чтобы просмотреть список реестров в домене.
5. Щелкните правой кнопкой мыши на пользовательском реестре, в который необходимо добавить псевдоним, и выберите **Свойства...**
6. Щелкните на вкладке **Псевдоним** в окне **Свойства**.
7. Укажите имя и тип добавляемого псевдонима. Можно указать тип псевдонима, отсутствующий в списке типов.
8. Выберите **Добавить**.
9. Щелкните **ОК**, чтобы сохранить изменения.

Определение частного типа пользовательского реестра в EIM

Для того чтобы задать определение нового типа пользовательского реестра в EIM, необходимо указать тип реестра в формате **идентификатор_объекта-нормировка**, где **идентификатор_объекта** - значение в десятичном формате с точками, например, 1.2.3.4.5.6.7, а **нормировка** - значение **caseExact** или **caseIgnore**. Например идентификатор объекта (OID) для OS/400 - 1.3.18.0.2.33.2-caseIgnore.

Для обеспечения уникальности создаваемых идентификаторов объектов (OID) эти OID следует получить у уполномоченных органов по регистрации OID. Уникальность OID исключает возможность возникновения конфликтов с OID, созданными другими организациями или приложениями.


Получить OID можно двумя способами:

- **Зарегистрировать объект в уполномоченной организации.**
Этот метод подходит в случае, когда необходимо получить небольшое число фиксированных OID. Например, эти OID могут представлять стратегии применения сертификатов для пользователей на предприятии.
- **Зарезервировать в уполномоченном органе сегмент и назначить в нем собственные OID.**
Данный метод резервирования диапазона идентификаторов объектов подходит для создания большого числа OID или в случае, когда назначенные OID будут изменяться. Зарезервированный сегмент состоит из первых чисел, с которых должен начинаться **идентификатор-объекта** в


формате с десятичными точками. Примером зарезервированного сегмента является 1.2.3.4.5.. На его основе можно создать отдельные OID. Например, можно было бы создать OID в формате 1.2.3.4.5.x.x.x).

Дополнительная информация о регистрации созданных OIDs в уполномоченной организации приведена на следующих Web-сайтах:


- Американский национальный институт стандартов (ANSI) - организация в США, уполномоченная регистрировать названия организаций в рамках общей программы регистрации, осуществляемой Международной организацией по стандартизации (ISO) и Международным телекоммуникационным союзом (ITU). Информационная страница с формой заявления

расположена на Web-сайте ANSI http://web.ansi.org/public/services/reg_org.html . Сегмент OID ANSI для организаций - 2.16.840.1. За резервирование сегментов OID ANSI взимает плату. На получение зарезервированного сегмента OID от ANSI уходит приблизительно две недели. Для резервирования нового сегмента OID ANSI присваивает число (NEWNUM): 2.16.840.1.NEWNUM.


- В большинстве стран и регионов ведением реестра OID занимается национальные ассоциации по стандартизации. Как и сегмент ANSI, сегменты, присваиваемые этими организациями, как правило, начинаются с OID 2.16. Информацию об организации, занимающейся ведением реестра OID в конкретной стране, не всегда легко получить. Адреса национальных органов членов ISO

можно найти на сайте <http://www.iso.ch/adresse/membodies.html> . Этот сайт содержит почтовые адреса и адреса электронной почты. Во многих случаях, помимо этого, указан Web-сайт.

- Вместо этого, можно начать со схем NSAP DCC ISO. Аббревиатура NSAP расшифровывается как Точка доступа к сетевой услуге и применяется во многих международных стандартах. Реестр схем


размещен на сайте <http://www.fei.org.uk> под заголовком ISO DCC NSAP . На этом Web-сайте в настоящее время приведены контактные данные 13 организаций, регистрирующих названия, некоторые из которых присваивают также и OID.

- Комитет по предоставлению адресов Internet (IANA) регистрирует частные номера предприятий, являющиеся идентификаторами объектов, в сегменте 1.3.6.1.4.1. По настоящий момент IANA зарегистрировал адреса более 7500 компаний. Страница с формой заявления расположена по

адресу <http://www.iana.org/cgi-bin/enterprise.pl>  в разделе Private Enterprise Numbers. Регистрация в IANA обычно занимает около недели. IANA предоставляет OID бесплатно. IANA присваивает адрес (NEWNUM), и новый сегмент OID имеет формат 1.3.6.1.4.1.NEWNUM.

- Федеральное правительство США ведет Реестр объектов защиты компьютеров (CSOR). CSOR - уполномоченный орган для присвоения имен в сегменте 2.16.840.1.101.3, который в настоящее время регистрирует объекты для меток защиты, алгоритмов шифрования и стратегий сертификатов. OID стратегий применения сертификатов регистрируются в сегменте 2.16.840.1.101.3.2.1. CSOR предоставляет OID стратегий учреждениям федерального правительства США. Дополнительная информация о CSOR приведена на Web-сайте

<http://csrc.nist.gov/csor/> .

Дополнительная информация об идентификаторах объектов (OID) стратегий сертификатов приведена на Web-сайте <http://csrc.nist.gov/csor/pkireg.htm> .

Удаление пользовательского реестра

В результате удаления пользовательского реестра из домена EIM удаляются все связи между идентификаторами EIM и идентификаторами пользователя, указанными в удаленном пользовательском реестре. Если после удаления реестра снова добавить его в домен EIM, то удаленные связи восстановлены не будут.

Для удаления пользовательского реестра необходимы права доступа администратора EIM.

Для удаления пользовательского реестра выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM.
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Пользовательские реестры**, чтобы просмотреть список пользовательских реестров в домене.
5. Щелкните правой кнопкой мыши на удаляемом пользовательском реестре и выберите пункт **Удалить....**
6. В окне **Подтверждение** нажмите кнопку **Да**, чтобы удалить пользовательский реестр.

Удаление псевдонима из пользовательского реестра

Для удаления псевдонима из пользовательского реестра необходимы права доступа администратора реестров и администратора выбранных реестров (включая, реестры, которые будут применяться) или права доступа администратора EIM.

Для удаления псевдонима из пользовательского реестра в домене EIM выполните следующие действия:

1. Разверните **Сеть** → **EIM** → **Управление доменами**.
2. Для выполнения этой задачи должно быть установлено соединение с соответствующим доменом EIM:
 - Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
 - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену” на стр. 34.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Пользовательские реестры**, чтобы просмотреть список реестров в домене.
5. Щелкните правой кнопкой мыши на пользовательском реестре, из которого необходимо удалить, и выберите пункт **Свойства**.
6. Щелкните на вкладке **Псевдоним** в окне **Свойства**.
7. Выберите удаляемый псевдоним и нажмите кнопку **Удалить**.
8. Нажмите кнопку **ОК**, чтобы сохранить изменения.

API EIM

Существует несколько интерфейсов прикладных программ (API) EIM, с помощью которых приложения могут выполнять операции EIM от своего имени или от имени пользователя приложения. Эти API позволяют выполнять операции поиска связанных идентификаторов, различные функции управления и настройки EIM, а также вносить изменения в информацию и получать данные.

API EIM подразделяются на несколько категорий:

- Операции обработки и работы с соединениями EIM
- Управление доменами EIM
- Операции с реестрами
- Операции с идентификаторами EIM
- Управление связями EIM
- Операции поиска связанных идентификаторов EIM

- Управление правами доступа EIM

В приложениях, осуществляющих с помощью этих API управление данными EIM в домене EIM, как правило, применяется следующая модель:

1. Получить описатель EIM
2. Установить соединение с доменом EIM
3. Выполнить необходимые задачи
4. Применить API управления EIM или поиска связанного идентификатора EIM
5. Выполнить необходимые задачи
6. Перед завершением работы, уничтожить описатель EIM

Подробные сведения и полный список API EIM на сервере iSeries приведен в разделе API преобразования идентификаторов в рамках предприятия (EIM).

Устранение неполадок EIM

EIM включает несколько технологий и состоит из нескольких приложений и функций. Так как существует несколько подходов к устранению неполадок, то подробная информация и инструкции по устранению неполадок и исправлению наиболее распространенных ошибок приведены в следующих разделах:

- “Невозможно подключиться к контроллеру домена”
- “Вывод списка идентификаторов EIM занимает много времени” на стр. 43
- ““Зависание” мастера настройки EIM во время завершающего этапа обработки” на стр. 43
- “Описатель EIM более не действителен” на стр. 43
- “Идентификационные и диагностические сообщения Kerberos” на стр. 43

Невозможно подключиться к контроллеру домена

Сбои при попытках подключиться к контроллеру домена могут быть вызваны разными причинами. При обнаружении причины неполадки проверьте следующее:

- Проверьте, правильно ли заданы следующие элементы:
 - Имя контроллера домена
 - Порт
 - ИД пользователя и пароль
- Убедитесь, что контроллер домена активен. Если роль контроллера домена играет сервер iSeries, то вы можете воспользоваться Навигатором и выполнить следующие действия:
 1. Разверните **Сеть** → **Серверы** → **TCP/IP**.
 2. Убедитесь, что Сервер каталогов находится в состоянии **Запущен**. Если сервер остановлен, щелкните правой кнопкой мыши на **Сервер каталогов** и выберите **Запустить....**

Убедившись, что контроллер домена активен, попробуйте еще раз подключиться к домену.

1. Разверните **Сеть** → **Enterprise Identity Mapping** → **Управление доменами**.
2. Выберите домен, с которым необходимо установить соединение. Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу “Добавление домена в папку Управление доменами” на стр. 34.
3. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Установить соединение....**
4. Укажите тип пользователя и обязательные сведения о пользователе для подключения к контроллеру домена EIM.
5. Нажмите кнопку **ОК**.

Вывод списка идентификаторов EIM занимает много времени

При открытии в Навигаторе папки Идентификаторы может уйти длительное время на создание списка идентификаторов. Если домен содержит большое число идентификаторов EIM, то рекомендуется ограничить критерии поиска для отображения списка идентификаторов EIM.

Для настройки представления списка идентификаторов EIM выполните следующие действия:

1. Откройте в Навигаторе **Сеть** → **EIM** → **Управление доменами**.
2. Разверните домен, в котором необходимо просмотреть список идентификаторов EIM.
3. Щелкните правой кнопкой мыши на пункте **Идентификаторы** и выберите **Настроить это представление** → **Включить в список....**
4. Укажите критерии отбора идентификаторов. В качестве символа подстановки можно указать звездочку (*).
5. Нажмите кнопку ОК.

Если после этого выбрать **Идентификаторы**, то будут показаны только идентификаторы EIM, отвечающие указанным критериям. Для просмотра полного списка идентификаторов EIM выполните описанные выше действия и укажите в настройке представления опцию **Все идентификаторы**.

"Зависание" мастера настройки EIM во время завершающего этапа обработки

Если мастер "зависает" на завершающем этапе обработки, то это может означать, что он ожидает запуска контроллера домена. Убедитесь, что запуск сервера LDAP прошел без ошибок. В случае серверов iSeries просмотрите записи для задания QDIRSRV, подсистема QSYSWRK, в протоколе задания.

Для просмотра протокола задания выполните следующие действия:

1. Откройте в Навигаторе **Управление заданиями** → **Подсистемы** → **Qsyswrk**.
2. Щелкните правой кнопкой мыши на **Qdirsrv** и выберите **Протокол задания**.

Описатель EIM более не действителен

Если во время работы с EIM посредством Навигатора пользователь получает сообщение об ошибке с указанием о том, что описатель EIM более не действителен, то это означает, что соединение с контроллером домена прервано.

Для повторного подключения к контроллеру домена выполните следующие действия:

1. Откройте в Навигаторе **Сеть** → **Enterprise Identity Mapping** → **Управление доменами**.
2. Щелкните правой кнопкой мыши на нужном домене и выберите пункт **Подключиться заново....**
3. Укажите сведения о соединении.
4. Нажмите кнопку **ОК**.

Идентификационные и диагностические сообщения Kerberos

При использовании протокола Kerberos для идентификации в EIM, в случае возникновения ошибки в операциях идентификации или преобразования идентификаторов, в протокол задания заносится диагностическое сообщение CPD3E3F. Это диагностическое сообщение содержит главный и вспомогательный код состояния, указывающие, где возникла неполадка. Для наиболее распространенных ошибок в сообщениях приводятся инструкции по исправлению.

Для устранения неполадки обратитесь к справочной информации, связанной с полученным диагностическим сообщением.

Информация, связанная с EIM

Рекомендуем вам ознакомиться с другими технологиями, связанными с EIM. Информация об этих технологиях приведена в следующих разделах документации Information Center:

- **Служба сетевой идентификации**

Этот раздел содержит информацию о настройке службы сетевой идентификации на сервере iSeries. Служба сетевой идентификации позволяет подключить сервер iSeries к существующей сети Kerberos. Применение службы сетевой идентификации вместе с EIM позволяет создать среду единого входа в сеть.

- **Службы каталогов (LDAP)**

Этот раздел содержит общие сведения и инструкции по настройке Служб каталогов (LDAP). На сервере LDAP хранятся данные EIM и связи идентификаторов.



Напечатано в Дании