IBM

System i

Безопасность
Преобразование идентификаторов в рамках предприятия

версия 6 выпуск 1

System i

Безопасность
Преобразование идентификаторов в рамках предприятия

версия 6 выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 133.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761–SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

Содержание

Преобразование идентификаторов в рамках предприятия

Технология преобразования идентификаторов в рамках предприятия (EIM) для платформы System i представляет собой реализованную в i5/OS инфраструктуру IBM, позволяющую администраторам и разработчикам приложений решить проблему управления множеством существующих на предприятии.

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.

EIM позволяет создать систему правил преобразования идентификаторов пользователей, зарегистрированных в различных реестрах. Такие правила преобразования называются связями. EIM также предоставляет набор API, позволяющих создавать на различных платформах приложения, использующие функции преобразования идентификаторов для поиска связей между идентификаторами пользователей. Кроме того, EIM можно применять совместно со службой сетевой идентификации - реализацией Kerberos в i5/OS - для обеспечения среды единого входа в систему.

Для настройки и обслуживания EIM предназначен Навигатор System i, графический пользовательский интерфейс System i. Применение EIM позволяет платформе System i воспользоваться интерфейсами i5/OS для идентификации пользователей с помощью службы сетевой идентификации. Приложения и операционная система i5/OS могут получать паспорта Kerberos и определять, каким пользовательским профайлам они соответствуют, с помощью EIM.

Дополнительные сведения о принципах работы EIM и о возможностях применения EIM на вашем предприятии приведены в следующих разделах:

Новое в выпуске V6R1

Новая или значительно измененная информация в сборнике разделов о преобразовании идентификаторов в рамках предприятия (EIM).

Новые и измененные функции EIM

- В предыдущих выпусках i5/OS EIM поддерживала преобразования идентификаторов только одного локального пользователя на систему. В i5/OS V6R1 EIM поддерживает выбор преобразований идентификаторов нескольких локальных пользователей в одной системе, используя IP-адрес целевой системы для выбора преобразований идентификаторов необходимого локального пользователя.

Кроме того, был обновлен раздел Единый вход в систему, подробно описывающий реализацию EIM в составе среды с единым входом в систему для сокращения затрат на управление паролями. В этом разделе описано множество примеров конфигураций среды с единым входом в систему, а также даны подробные инструкции по реализации этих конфигураций.

Как найти новую или измененную информацию

В этом документе новая и измененная информация обозначается следующим образом:

- Значок » отмечает начало новой или измененной информации.
- Значок « отмечает конец новой или измененной информации.

Более подробные сведения о дополнениях и изменениях, внесенных в этот выпуск, приведены в документе Информация для пользователей.

Документация в формате PDF к преобразованию идентификаторов в рамках предприятия

Файл PDF этой информации можно просмотреть и напечатать.

Для просмотра или загрузки этого документа в формате PDF щелкните на ссылке EIM (около 1820 Кб).

Можно просмотреть и загрузить следующие связанные разделы в формате PDF:

- Документ Службы сетевой идентификации (около 1398 Кб) содержит инструкции по настройке службы сетевой идентификации вместе с EIM для создания среды с единым входом в систему.
- Сервер каталогов IBM Tivoli для i5/OS (LDAP) (около 1700 Кб) содержит инструкции по настройке сервера LDAP, который может применяться в качестве контроллера домена EIM, а также сведения о дополнительных параметрах конфигурации LDAP.

Сохранение файлов PDF

Для того чтобы сохранить файл PDF на рабочей станции для дальнейшего просмотра или печати, выполните следующие действия:

1. Щелкните правой кнопкой мыши на ссылке на файл PDF в браузере.
2. Щелкните на опции локального сохранения PDF.
3. Перейдите в каталог, в котором нужно сохранить документ PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка Adobe Reader

Для просмотра и печати этих PDF-файлов требуется программа Adobe Reader. Бесплатную копию программы Adobe можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html) .

Обзор технологии преобразования идентификаторов в рамках предприятия

Преобразование идентификаторов в рамках предприятия (EIM) помогает решить проблемы, возникающие при попытке управления несколькими пользовательскими реестрами.

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. EIM 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. В такой среде пользователям и администраторам приходится затрачивать очень много усилий. Администраторы часто тратят свое высокооплачиваемое рабочее время не на управление предприятием, а на разрешение проблем, связанных с забытыми паролями и 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 нисколько не облегчает жизнь пользователей и администраторов.

Текущие подходы к решению проблемы

В настоящее время существует несколько походов 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 многоуровневых неоднородных 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.

EIM обеспечивает преобразование один-несколько (другими словами, одному пользователю в реестре может соответствовать несколько идентификаторов). Администратору не требуется обеспечивать преобразование всех идентификаторов из реестров пользователей. EIM также обеспечивает преобразование много-один (т.е. несколько пользователей могут применять один и тот же идентификатор пользователя из определенного реестра).

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 связать идентификатор пользователя Windows в реестре Kerberos с пользовательским профайлом i5/OS в другом реестре и обеспечить доступ к тем ресурсам i5/OS, к которым есть права доступа у пользовательского профайла i5/OS.

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. EIM хранит 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.

EIM в сочетании со службой сетевой идентификации, представляющей собой реализацию Kerberos в i5/OS, обеспечивает возможность создания среды с единым входом в систему. Вы можете создавать приложения, использующие API GSS и EIM для получения паспортов Kerberos и установления соответствия с идентификатором пользователя, находящимся в другом реестре. Связь между идентификаторами пользователей обеспечивается путем создания связей идентификаторов, косвенным образом устанавливающие соответствие между идентификаторами пользователей посредством идентификатора EIM, либо путем создания связей стратегий, косвенным образом устанавливающие соответствие между группой идентификаторов пользователей и одним целевым идентификатором пользователя.

Функция преобразования идентификаторов требует от администраторов выполнения следующих задач:

1. Настройка в сети домена EIM. Для создания контроллера домена и настройки доступа к этому домену вы можете воспользоваться мастером настройки EIM. С помощью мастера вы можете создать домен EIM и контроллер домена как в локальной, так и в удаленной системе. Если домен EIM уже существует, то вы можете включить систему в его состав.
2. Выбор на сервере каталогов, выполняющем функции контроллера домена EIM, пользователей, которым разрешено управлять информацией домена EIM, просматривать эту информацию, а также включение этих пользователей в группы управления доступом EIM.

3. Создание определений реестров EIM для тех реестров пользователей, которые будут входить в состав домена EIM. Несмотря на то, что в домене EIM можно определить любой реестр пользователей, следует создавать определения реестров пользователей только для тех приложений и операционных систем, которые поддерживают EIM.
4. Выбор задач, которые необходимо выполнить для завершения настройки в соответствии с требованиями конфигурации EIM:
   - Создание идентификаторов EIM для каждого уникального пользователя в домене и создание для них связей идентификаторов.
   - Создание связей стратегий.
   - Выполнение перечисленных операций в различных сочетаниях.

   Информация, связанная с данной

   Обзор единого входа в систему

Концепции EIM

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

На рис. 1 показан пример реализации EIM на предприятии. Три сервера выступают в роли клиентов EIM и содержат поддерживающие EIM приложения, запрашивающие данные EIM с помощью операций поиска EIM (6). В контроллере домена (1) хранится информация о домене EIM (2), содержащая идентификатор EIM (3), связи (4) между идентификаторами EIM и пользовательскими идентификаторами, а также определениями реестра EIM (5).

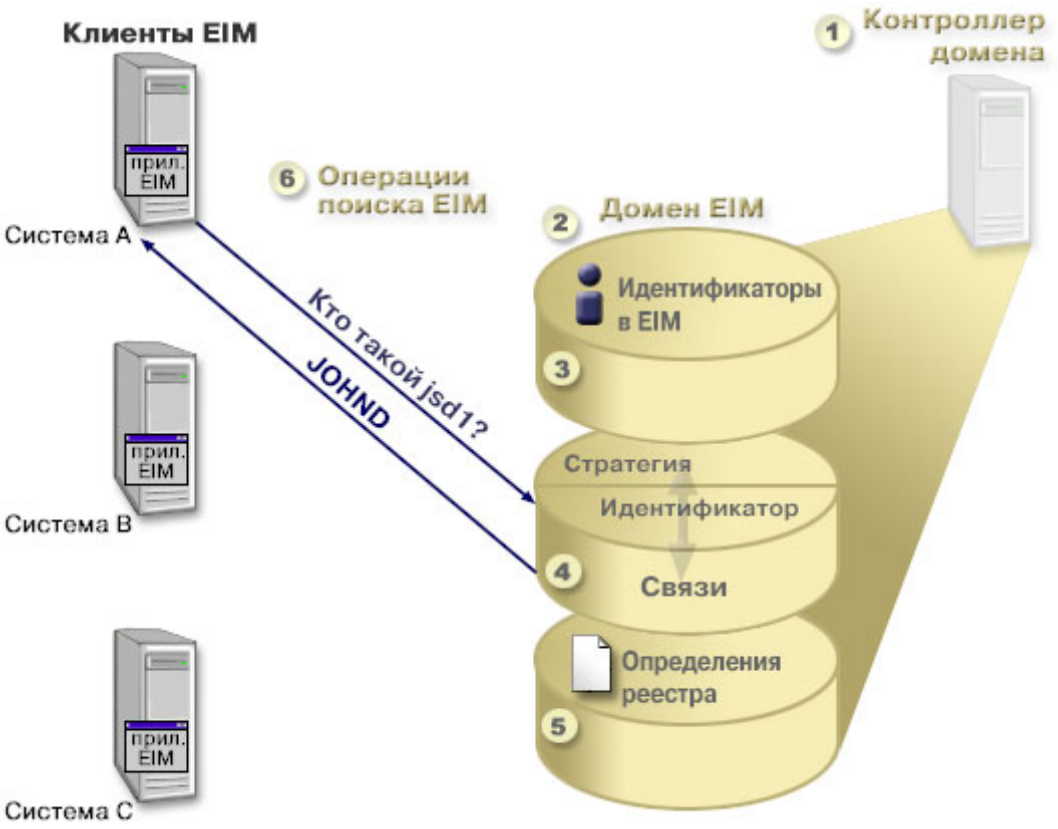


Рисунок 1. Пример реализации EIM

Дополнительные сведения о EIM eServer приведены в следующих разделах:

Контроллер домена EIM

Контроллер домена EIM - это сервер Упрощенного протокола доступа к каталогам (LDAP), настроенный для управления одним или несколькими доменами EIM. В домене EIM содержатся все идентификаторы, связи EIM и реестры пользователей домена. Системы (клиенты EIM) используют данные домена в операциях поиска EIM.

В настоящее время функции контроллера домена EIM могут выполняться продуктом IBM Tivoli Directory Server for i5/OS на некоторых платформахIBM eServer.Клиентами могут быть любые системы, поддерживающие API EIM. Клиенты выполняют операции поиска 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.

Примечание: Если вы планируете настроить сервер каталогов в удаленной системе, то применяемый сервер каталогов должен обеспечивать поддержку EIM. EIM требует размещения контроллера домена на сервере каталогов, поддерживающем простой протокол доступа к каталогам (LDAP) версии 3. Кроме того, сервер каталогов должен поддерживать применяемую схему EIM. Продукт IBM Tivoli Directory Server for i5/OS обеспечивает такую поддержку.

Понятия, связанные с данным

“Операции преобразования идентификаторов EIM” на стр. 27
Приложение или операционная система с помощью API EIM могут выполнять операции поиска, позволяющие установить соответствие между идентификатором пользователя в одном реестре и другим

идентификатором в другом реестре. Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в неком целевом реестре по известной им информации об этом пользователе.

“Схема LDAP и другие особенности EIM” на стр. 49
Информация о требованиях сервера каталога для работы с EIM.

Домен EIM

Домен EIM - это каталог сервера LDAP, в котором хранятся данные EIM.

Домен EIM содержит все идентификаторы, связи и реестры пользователей EIM, а также данные управления доступом. Системы (клиенты EIM) используют данные домена в операциях поиска связанного идентификатора EIM.

Домен EIM и реестр пользователей - это разные вещи. Реестр содержит идентификаторы пользователей, известные конкретной 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 назначены.

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 определяют связь между идентификаторами пользователей и реальными людьми, которым назначены эти идентификаторы.

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

В EIM хранятся следующие данные:

Определения реестров EIM

Каждое определение реестра EIM соответствует фактическому реестру пользователей, применяемому конкретной системой или группой систем предприятия. Для того чтобы реестр пользователей мог применяться в домене EIM, нужно создать его определение в домене. Вы можете создать два типа определений реестров: системный реестр пользователей и реестр пользователей приложения.

Идентификаторы EIM

Каждый созданный идентификатор EIM соответствует отдельному сотруднику или объекту предприятия. Создание идентификаторов EIM позволяет задавать однозначное соответствие между идентификаторами отдельного сотрудника или объекта, к которому относится данный идентификатор EIM.

Связи EIM

Связи EIM определяют взаимосвязь между идентификаторами пользователей. Связи должны определяться таким образом, чтобы клиенты EIM с помощью API EIM могли успешно выполнять операции преобразования EIM. Операции преобразования заключаются в поиске определенных в домене EIM связей. Существует два типа связей, которые вы можете создавать:

Связи идентификаторов

Связи идентификаторов позволяют определить однозначное соответствие между идентификаторами пользователя посредством определенного для этого пользователя идентификатора EIM. Связь EIM определяет соответствие между идентификатором EIM и идентификатором пользователя в одном из реестров предприятия. Связи идентификаторов содержат информацию, необходимую для сопоставления идентификаторов EIM и идентификаторов пользователей в различных реестрах. Связи идентификаторов особенно удобны в ситуациях, когда у пользователя есть идентификатор с особыми правами доступа или с другими привилегиями, которыми необходимо управлять путем создания однозначного соответствия между различными идентификаторами.

Связи стратегий

Связи стратегий позволяют определить взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах и одним целевым идентификатором пользователя в другом реестре. Каждая создаваемая связь стратегий EIM задает соответствие между исходной группой идентификаторов пользователей из одного реестра и одним-единственным целевым идентификатором пользователя. Как правило, связи стратегий создаются для преобразования группы пользователей с одинаковыми правами доступа в целевой идентификатор пользователя с требуемыми правами доступа.

Понятия, связанные с данным

“Определения реестров EIM” на стр. 11
Определение реестра EIM - это созданная в EIM запись, которая содержит данные об отдельном реестре пользователей предприятия. Реестр пользователей - это каталог, в котором содержатся идентификаторы пользователей отдельной системы или приложения.

“Идентификатор EIM” на стр. 9
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.

“Операции преобразования идентификаторов EIM” на стр. 27
Приложение или операционная система с помощью API EIM могут выполнять операции поиска, позволяющие установить соответствие между идентификатором пользователя в одном реестре и другим идентификатором в другом реестре. Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в неком целевом реестре по известной им информации об этом пользователе.

Идентификатор EIM

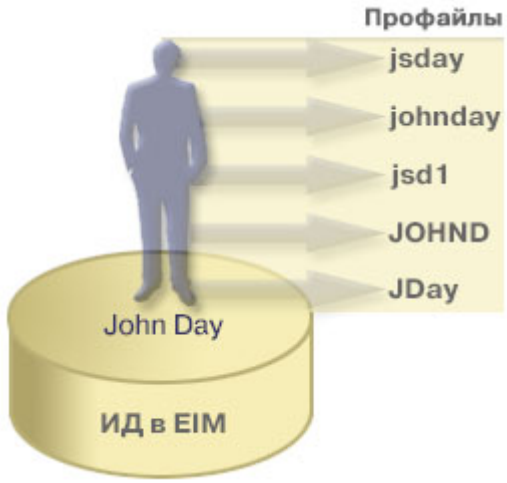
Идентификатор EIM - это уникальный идентификатор сотрудника или объекта на предприятии. Довольно часто сеть предприятия состоит из разнообразного аппаратного и программного обеспечения с несколькими независимыми реестрами пользователей. Часто это обусловлено требованиями различных платформ или реестров.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

С помощью EIM вы можете создавать уникальные идентификаторы EIM для сотрудников и объектов предприятия. После этого можно создать связи идентификаторов, задающие однозначное соответствие между идентификаторами EIM и различными идентификаторами сотрудников или объектов, представленных идентификаторами EIM. Такая процедура существенно упрощает создание разнородных многоуровневых приложений. Она также упрощает разработку и применение средств управления доступом пользователей.

Идентификатор EIM для пользователя

На рисунке 3 показан пример идентификатора EIM для пользователя *John Day*. В данном примере у пользователя *John Day* есть пять идентификаторов пользователей в четырех различных реестрах: `johnday`, `jsd1`, `JOHND`, `jsday` и `JDay`.

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

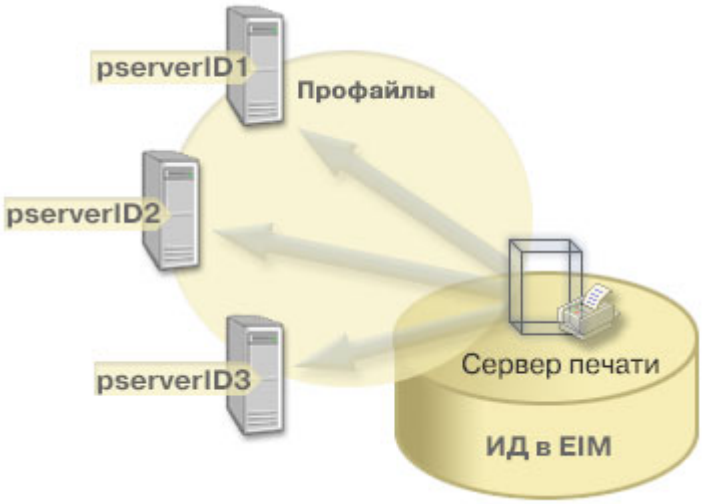


В EIM создаются связи между идентификатором пользователя `John Day` и его прочими идентификаторами в разных реестрах. После этого все приложения смогут пользоваться единым идентификатором пользователя, хранящимся в EIM.

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.



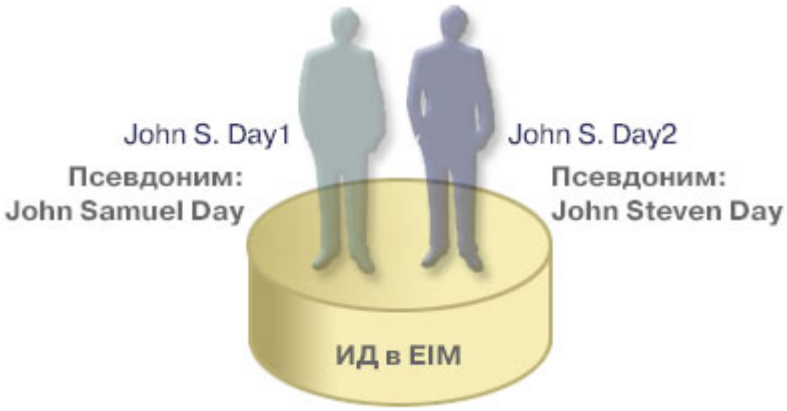
В EIM можно создать единый идентификатор для сервера печати, который будет применяться в масштабах предприятия. В данном примере идентификатор `Функции сервера печати` используется для идентификации сервера печати во всех системах предприятия. Идентификатор сервера в EIM (`Print server function`) привязывается ко всем отдельным идентификаторам этого сервера (`pserverID1`, `pserverID2` и `pserverID3`).Это устранит 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 предприятиях будут использоваться эти приложения.

Идентификаторы и псевдонимы EIM

Все идентификаторы EIM должны быть уникальны в пределах домена EIM. Псевдонимы упрощают работу в случаях, когда идентификаторы трудны для запоминания. Например, псевдонимы могут быть полезны в случаях, когда идентификатор пользователя в организации не совпадает с его реальным именем. 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. Для каждого идентификатора EIM можно создать произвольное число псевдонимов, указывающих, к какому именно сотруднику *John S. Day* относится данный идентификатор EIM. Например, в дополнительных псевдонимах можно указывать номера пользователей, номера отделов, должности и т.п. Например, для пользователя `John S. Day1` можно создать псевдоним `John Samuel Day`, а для пользователя `John S. Day2` - псевдоним `John Steven Day`.

Псевдонимы позволяют упростить поиск нужных идентификаторов EIM. Например, приложение, созданное для работы с EIM, может указать псевдоним, позволяющий позволяющий найти требуемый идентификатор пользователя EIM приложения. Администратор может добавить псевдоним к идентификатору EIM, чтобы приложение могло использовать его в операциях EIM вместо уникального идентификатора. Приложение может указывать эту информацию при вызове API `eimGetTargetFromIdentifier()` для выполнения операций поиска EIM при поиске требуемого идентификатора пользователя.

Понятия, связанные с данным

“Домен EIM” на стр. 7
Домен EIM - это каталог сервера LDAP, в котором хранятся данные EIM.

Определения реестров EIM

Определение реестра EIM - это созданная в EIM запись, которая 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 реестра пользователей является реестр z/OS Security Server Resource Access Control Facility (RACF). 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 субъекты области Kerberos и идентификаторы пользователей в домене Windows Active Directory domain, а также реестр пользовательских профайлов i5/OS.

Допускается определение вложенных реестров пользователей. В некоторых случаях приложениям нужны не все идентификаторы из конкретного реестра пользователей, а только некоторые из них. Например, реестр z/OS Security Server (RACF) может содержать внутренние реестры, распространяющиеся на отдельные подмножества пользователей общего реестра RACF.

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

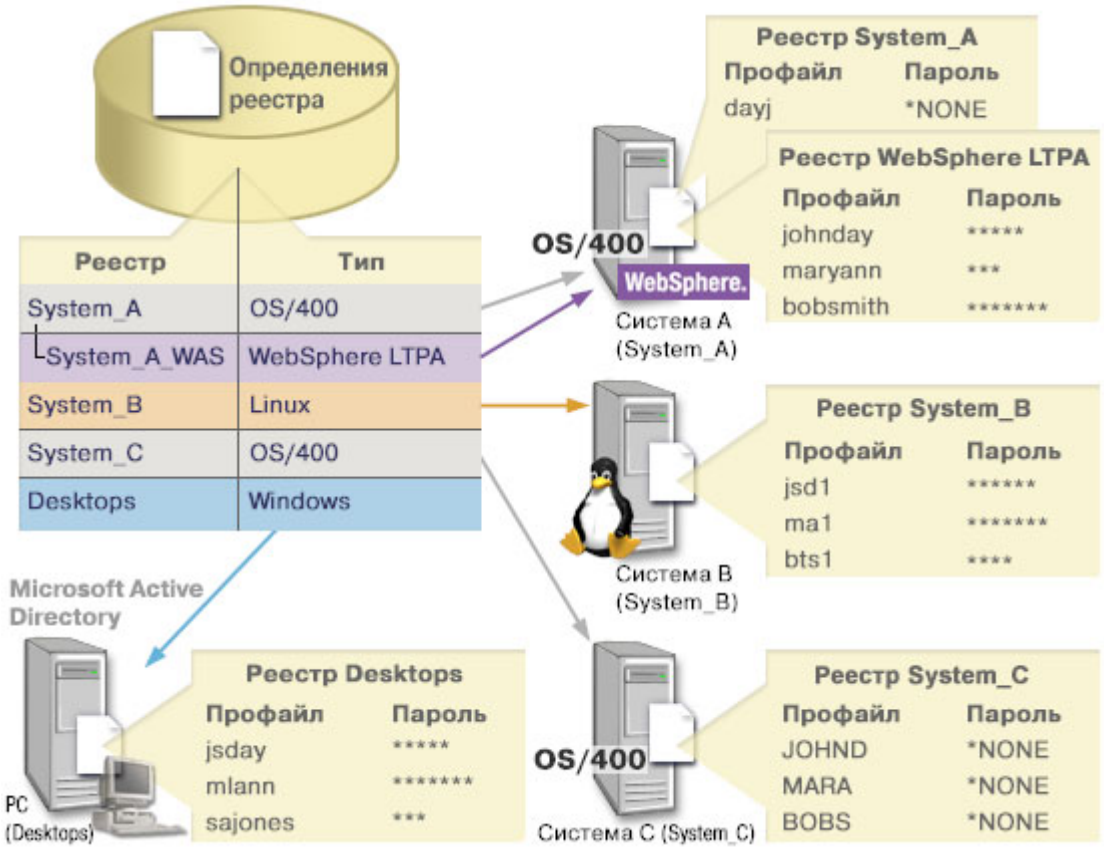
- Уникальное произвольное имя реестра EIM. Для каждого реестра пользователей в EIM создается отдельное определение. Для удобства рекомендуем присваивать определениям реестров в EIM простые и понятные идентификаторы. Например, в качестве идентификаторов можно использовать имена хостов (возможно, в сочетании с именем приложения, использующего реестр). Именами реестров в EIM могут быть любые алфавитно-цифровые строки. В именах могут содержаться пробелы.
- Тип реестра пользователей. В EIM поддерживается ряд заранее определенных типов реестров пользователей, обеспечивающих возможность взаимодействия с большинством распространенных системных реестров. Ниже перечислены некоторые из них:
  - AIX
  - Domino - полные имена
  - Domino - краткие имена
  - Kerberos
  - Kerberos - с учетом регистра символов
  - LDAP
  - - LDAP - краткое имя
  - Linux

- Novell Directory Server
- - Прочие
- - Прочие - с учетом регистра символов
- i5/OS (или OS/400)
- Tivoli Access Manager
- RACF
- Windows - локальный
- Windows - домен (Kerberos). (В этом типе реестра учитывается регистр символов.)
- X.509

Несмотря на то, что заранее определенные определения реестров охватывают почти все реестры пользователей операционных систем, может возникнуть ситуация, когда необходимо будет создать определение реестра, для которого в EIM нет заранее определенного типа. Из этой ситуации есть два выхода. Вы можете либо воспользоваться существующим определением реестра, которое соответствует параметрам вашего реестра пользователей, либо определить собственный тип реестра пользователей. Например, на рисунке 6 проиллюстрировано создание администратором реестра типа `WebSphere LTPA` для определения реестра приложения `System_A_WAS`.

На рисунке 6 администратор создал в EIM определения реестров пользователей систем A, B, C и Windows Active Directory, в которых хранятся субъекты Kerberos пользователей, применяемые при входе в систему рабочих станций. Кроме того, администратор создал определение реестра WebSphere (R) Lightweight Third-Party Authentication (LTPA), размещенного в системе A. Указанное администратором имя определения реестра позволяет легко определить тип реестра. Как правило, для идентификации реестров удобно применять IP-адреса или имена хостов. В данном примере рассматриваемому экземпляру определения реестра приложения WebSphere LTPA соответствует имя `System_A_WAS`. Администратор также указал, что родительским системным реестром для этого определения реестра приложения является реестр `System_A`.

Рисунок 6: Определения пяти реестров пользователей EIM.



Примечание: Для дальнейшего снижения количества операций, связанных с управлением паролями, администратор установил значение *NONE для паролей пользовательских профайлов i5/OS в системах A и C. В данном случае администратор настраивает среду с единым входом в систему, причем все пользователи работают только с приложениями, поддерживающими EIM, например, с System i Navigator. В такой ситуации администратор может удалить пароли пользовательских профайлов i5/OS, сократив тем самым количество паролей, которыми приходится управлять.

Понятия, связанные с данным

“Домен EIM” на стр. 7
Домен EIM - это каталог сервера LDAP, в котором хранятся данные EIM.

“Определение собственного типа реестра пользователей в EIM” на стр. 97
При создании определения реестра EIM вы можете указать один из нескольких заранее определенных типов реестров пользователей, представляющий фактический реестр пользователей, существующий в сети вашего предприятия.

Определения системных реестров

Определение системного реестра - это запись, создаваемая в EIM для представления и описания отдельного реестра пользователей на рабочей станции или на сервере.

Определения системных реестров EIM следует применять для реестров, обладающих следующими характеристиками:

- Реестр предоставляется операционной системой, например, AIX, i5/OS либо продуктом управления защитой, например, z/OS Security Server Resource Access Control Facility (RACF).
- В реестре хранятся идентификаторы пользователей, уникальные в рамках данного приложения, например, Lotus Notes.

- В реестре хранятся распределенные идентификаторы пользователей (например, субъекты Kerberos или отличительные имена LDAP).

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.

Задачи, связанные с данной

“Добавление определения реестра приложений” на стр. 95
Для создания определения реестра приложений необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Определения реестров приложений

Определение реестра приложения - это запись EIM, создаваемая для описания и представления подмножества идентификаторов пользователей в пределах системного реестра. Эти идентификаторы обладают какими-либо особыми атрибутами и применяются конкретным приложением или набором приложений.

Допускается определение вложенных реестров пользователей. Например, реестр z/OS Security Server (RACF) может содержать внутренние реестры, распространяющиеся на отдельные подмножества пользователей общего реестра RACF. В связи с такой структурой необходимо обязательно указывать для каждого создаваемого определения реестра приложения имя родительского системного реестра.

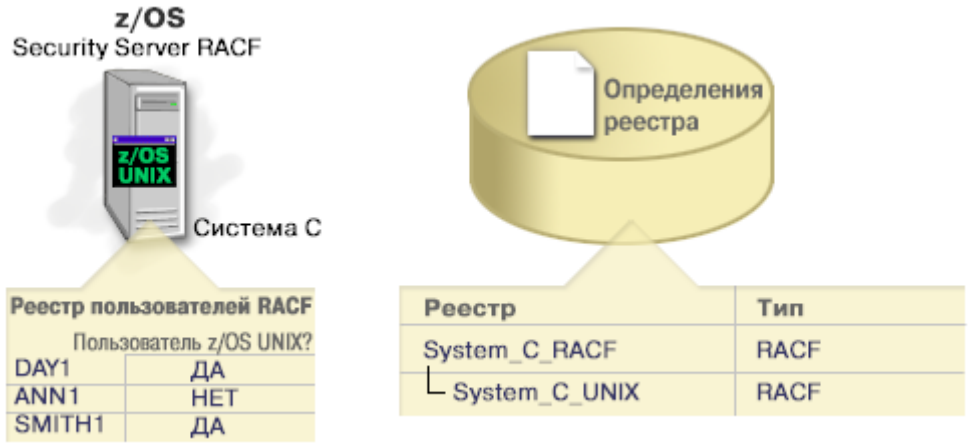
Определения реестров приложений EIM следует применять для реестров пользователей, обладающих следующими характеристиками:

- Идентификаторы пользователей приложения не хранятся в отдельном реестре пользователей этого приложения.
- Идентификаторы пользователей приложения хранятся в системном реестре, содержащем идентификаторы пользователей других приложений.

Операции поиска EIM выполняются правильно независимо от того, создан ли реестр пользователей как реестр приложения или системный реестр EIM. 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 приведен пример создания в EIM определения системного реестра z/OS сервера безопасности RACF. Для пользователей RACF, применяющих продукт z/OS(TM) UNIX System Services (z/OS UNIX), создано отдельное определение реестра приложения. В реестре пользователей RACF системы C хранятся сведения об идентификаторах `DAY1`, `ANN1` и `SMITH1`. Двум из этих идентификаторов (`DAY1` и `SMITH1`) предоставлен доступ к z/OS UNIX в системе C. Эти идентификаторы пользователей фактически соответствуют пользователям RACF с уникальными атрибутами, идентифицирующими их как пользователей z/OS UNIX. Для всего реестра пользователей RACF администратор EIM создал определение реестра `System_C_RACF`. Кроме того, администратор EIM создал определение реестра `System_C_UNIX` для пользователей, имеющих атрибуты z/OS UNIX.

Рисунок 7: Определение реестров EIM для реестра пользователей RACF и для пользователей z/OS UNIX



Групповое определение реестра

Логическая группировка определений реестров позволяет сократить объем работ, необходимых для настройки преобразования EIM. Можно управлять групповым определением реестра так же, как и отдельным определением реестра.

Все элементы группового определения реестра обычно содержат по крайней мере один общий пользовательский идентификатор, к которому следует добавить целевые или исходные связи. Группируя элементы можно создать только одну связь, вместо нескольких, с групповым определением реестра и пользовательским идентификатором.

Например, пользователь John Day входит в основную систему с пользовательским идентификатором `jday` и использует один пользовательский идентификатор `JOHND` в нескольких системах. Таким образом, реестр пользователей каждой системы одержит пользовательский профайл `JOHND`. Обычно, пользователь John Day создает отдельные целевые связи идентификатора EIM John Day для каждого отдельного реестра пользователей, содержащего пользовательский профайл. `JOHND` user identity. Для снижения объема необходимых работ, которые должен выполнить пользователь для настройки преобразования EIM, он может создать одно групповое определение реестра для всех реестров пользователей, содержащих пользовательский профайл `JOHND`. Затем он сможет создать одну целевую связь с идентификатором EIM `John Day` для группового определения реестра, вместо нескольких целевых связей с идентификатором EIM John Day для каждого отдельного определения реестра. Это позволяет связать пользовательский профайл John Day `jday` с пользовательским профайлом `JOHND`.

Информация о групповых определениях реестра:

- Все элементы (отдельные определения реестра) группового определения реестра должны быть указаны с одинаковым учетом регистра.
- Все элементы (отдельные определения реестра) группового определения реестра должны быть заданы в домене EIM перед добавлением в групповое определение реестра.
- Определение реестра может быть членом нескольких групп, но следует избегать использования отдельного реестра пользователей в качестве элемента нескольких групповых определений реестра, так как операция поиска может вернуть неоднозначные результаты. Групповое определение реестра не может быть элементом другого группового определения реестра.

Понятия, связанные с данным

“Примеры операций поиска: Пример 5” на стр. 36
Данный пример содержит сведения возврате операцией поиска неоднозначных результатов, содержащих групповые определения реестра.

Связи EIM

Связь EIM - это запись, создаваемая в домене EIM и определяющая взаимосвязь между идентификаторами пользователей в разных реестрах. Тип создаваемой связи определяет, будет ли взаимосвязь между идентификаторами непосредственной или косвенной.

В EIM можно создавать два типа связей: связи идентификаторов и связи стратегий. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними. Способ применения связей определяется общим планом реализации EIM.

Дополнительная информация о работе со связями приведена в следующих разделах:

Информация для поиска

При помощи EIM можно предоставить дополнительные данные, называемые информацией для поиска, которые позволяют более точно определить целевой идентификатор пользователя. Целевой идентификатор пользователя может быть задан либо в связи идентификаторов, либо в связи стратегий.

Информация для поиска представляет собой уникальную строку символов, которая может применяться API EIM `eimGetTargetFromSource` или `eimGetTargetFromIdentifier` в операциях поиска соответствий для более точного определения параметров поиска целевого идентификатора пользователя. Данные, указываемые в качестве информации для поиска, соответствуют параметру дополнительной информации о пользователях реестра этих API.

Информация для поиска необходима лишь в том случае, если операции поиска соответствий могут возвращать несколько целевых идентификаторов пользователей. Операция поиска соответствия может вернуть несколько целевых идентификаторов при выполнении следующих условий в любых сочетаниях:

- У идентификатора EIM есть несколько отдельных целевых связей с одним и тем же целевым реестром.
- Для идентификатора пользователя в исходной связи указано несколько идентификаторов EIM и каждый из этих идентификаторов EIM имеет целевую связь с одним и тем же целевым реестром, хотя в целевых связях каждого идентификатора может быть указан свой целевой идентификатор пользователя.
- Один и тот же целевой реестр указан в нескольких стратегиях домена по умолчанию.
- Один и тот же целевой реестр и один и тот же исходный реестр указаны в нескольких связях стратегий реестров по умолчанию.
- В нескольких связях стратегий фильтров сертификатов указан один и тот же исходный реестр X.509, фильтр сертификатов или целевой реестр.

Примечание: Такая ситуация может привести к возникновению ошибок в приложениях с поддержкой EIM, в том числе в продуктах и приложениях i5/OS, которые не могут применять подобные неоднозначные результаты поиска. Однако следует помнить, что базовые приложения i5/OS, такие как System i Access for Windows, не могут различать несколько возвращенных операцией поиска целевых идентификаторов пользователей с помощью информации для поиска. Следовательно, необходимо переопределить связи в домене, обеспечив возврат операциями поиска соответствий только одного идентификатора пользователя, что гарантирует приложениям i5/OS возможность успешного поиска соответствий и преобразования идентификаторов.

Информация для поиска позволяет избежать ситуаций, в которых операция поиска соответствий может вернуть несколько целевых идентификаторов пользователей. Для того чтобы операция поиска не возвращала несколько целевых идентификаторов, необходимо определить уникальную информацию для поиска в каждом целевом идентификаторе пользователя в каждой связи. Информация для поиска обязательно должна указываться в операциях поиска соответствий для обеспечения возврата уникального целевого идентификатора пользователя. В противном случае приложение, использующее EIM, не сможет точно выбрать необходимый целевой идентификатор пользователя.

Допустим, например, что у вас существует идентификатор EIM John Day, которому соответствуют два пользовательских профайла в A. Один из этих профайлов - JDUSER, а другой - JDSECADM, имеющий специальные права доступа системного администратора. Для идентификатора John Day определено две целевых связи. Одна из этих целевых связей указывает на идентификатор пользователя JDUSER в целевом реестре System_A и содержит определенную для JDUSER информацию для поиска user authority. Другая целевая связь указывает на идентификатор пользователя JDSECADM в целевом реестре System_A и содержит определенную для JDSECADM информацию для поиска security officer.

Если в операции поиска соответствия не задана информация для поиска, то будут возвращены оба идентификатора пользователей: JDUSER и JDSECADM. Если в операции поиска задана информация для поиска user authority, то будет возвращен только идентификатор пользователя JDUSER. Если в операции поиска задана информация для поиска security officer, то будет возвращен только идентификатор пользователя JDSECADM.

Примечание: Если вы удалите последнюю целевую связь для идентификатора пользователя (независимо от того, является ли она связь идентификаторов или связью стратегий), то при этом из домена будет также удален этот целевой идентификатор вместе со всей информацией для поиска.

Поскольку связи стратегий сертификатов и другие связи могут применяться в самых разных сочетаниях, то перед созданием и применением связей стратегий сертификатов необходимо внимательно изучить поддержку стратегий преобразования EIM и работу операций поиска.

Понятия, связанные с данным

“Поддержка и активация стратегий преобразования EIM” на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

“Операции преобразования идентификаторов EIM” на стр. 27
Приложение или операционная система с помощью API EIM могут выполнять операции поиска, позволяющие установить соответствие между идентификатором пользователя в одном реестре и другим идентификатором в другом реестре. Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в неком целевом реестре по известной им информации об этом пользователе.

“Связи стратегий домена по умолчанию” на стр. 21
Связи стратегий домена по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

“Связи стратегий реестра по умолчанию” на стр. 23
Связи стратегий реестра по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

Связи идентификаторов

Идентификатор EIM представляет определенного сотрудника предприятия или какой-либо объект. Связь идентификатора EIM описывает соответствие между этим идентификатором и записью реестра пользователей, также представляющей этого сотрудника. Создав связи между идентификатором EIM и всеми идентификаторами пользователя в различных реестрах, можно получить единый идентификатор пользователя и применять его в пределах предприятия.

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 позволяют приложениям определять идентификаторы пользователей в определенных реестрах по их идентификаторам в других реестрах.

Идентификатор EIM позволяет косвенно определить соответствие между такими идентификаторами пользователей, благодаря чему приложения могут находить различные идентификаторы пользователя EIM на основании одного известного идентификатора. В EIM предусмотрены API, позволяющие приложениям определять идентификаторы пользователей в конкретных реестрах по их идентификаторам в EIM. Эта процедура называется поиском соответствия идентификаторов.

В EIM администратор может определить три типа связей, описывающих соотношения между идентификатором EIM и идентификатором пользователя. Это следующие типы: исходная связь, целевая связь и административная связь. Тип созданной связи определяется способом применения идентификатора пользователя. Например, для пользователей, которые должны участвовать в операциях поиска соответствия, создаются исходные и целевые связи. Как правило, если идентификатор пользователя применяется для идентификации, то для него создается исходная связь. После этого создаются целевые связи для тех идентификаторов пользователей, которые применяются для проверки прав доступа.

Перед тем, как приступить к созданию связей идентификаторов, 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:

- Имя идентификатора EIM
- Идентификатор пользователя
- Имя определения реестра EIM
- Тип связи
- Дополнительно: Информация для поиска, позволяющая более точно выявить целевой идентификатор пользователя в целевой связи.

Исходная связь

Исходные связи позволяют определять идентификаторы пользователей в нужных реестрах по их идентификаторам в других реестрах.

Если идентификатор пользователя используется для *идентификации*, для него нужно создать исходную связь с идентификатором EIM. Например, исходную связь можно создать для субъекта Kerberos, поскольку такая форма идентификатора пользователя применяется для идентификации. Для обеспечения успешного поиска соответствия идентификаторов EIM необходимо, чтобы для каждого идентификатора EIM применялись и исходные и целевые связи.

Целевые связи

Целевые связи позволяют получать идентификаторы пользователей в качестве результата операции поиска в EIM. Для обычных пользователей обычно достаточно создать только целевые связи.

Если идентификатор пользователя используется для *проверки прав доступа*, для него нужно создать целевую связь с идентификатором EIM. Например, целевую связь можно создать для пользовательского профайла i5/OS, поскольку такая форма идентификатора пользователя позволяет определить, к каким ресурсам конкретной платформы System i. Для обеспечения успешного поиска соответствия идентификаторов EIM необходимо, чтобы для каждого идентификатора EIM применялись и исходные и целевые связи.

Взаимосвязь исходных и целевых связей

Для обеспечения успешного поиска соответствия идентификаторов необходимо создать по крайней мере одну исходную и одну целевую связь для каждого идентификатора EIM. Как правило, целевая связь

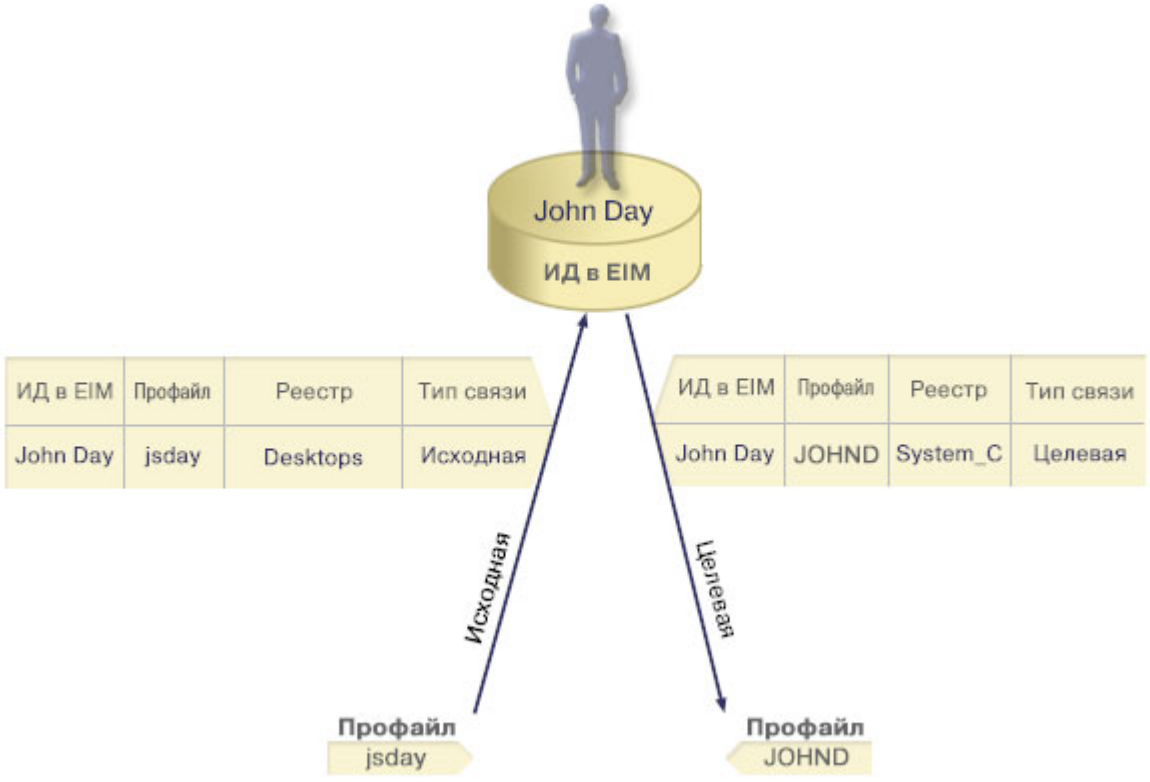
создается для каждого идентификатора пользователя в реестре пользователей, применяемым для проверки прав доступа к системе или в приложении, к которому относится этот реестр.

Допустим, например, что пользователи вашего предприятия обычно входят в систему и выполняют идентификацию с помощью Windows, а затем обращаются к платформе System i для выполнения различных задач. Пользователи входят в систему настольного компьютера с помощью ИД субъекта Kerberos, а затем входят на платформу System i с помощью пользовательского профайла i5/OS. Вы хотите создать среду с единым входом в систему, в которой пользователи могли бы проходить идентификацию в своих системах с помощью ИД субъекта Kerberos и больше не должны были бы вручную указывать идентификационные данные для входа на платформу System i.

Для достижения этой цели вы можете создать исходную связь субъекта Kerberos для каждого пользователя и идентификатора EIM этого пользователя. После этого вы должны будете создать целевую связь пользовательского профайла i5/OS для каждого пользователя и идентификатора EIM этого пользователя. Такая конфигурация гарантирует, что i5/OS сможет выполнить поиск соответствия идентификаторов и выбрать пользовательский профайл, точно соответствующий пользователю, обращающемуся к платформе System i после прохождения идентификации в своей локальной системе. После этого i5/OS предоставит пользователю доступ к ресурсам сервера в соответствии с параметрами пользовательского профайла, не требуя ввода идентификационных данных вручную.

На рисунке 6 приведен другой пример, в котором администратор EIM создает две связи (исходную и целевую) для идентификатора EIM `John Day`, определяя взаимосвязь между этим идентификатором и двумя другими идентификаторами пользователей. Администратор создает исходную связь для субъекта Kerberos `jsday` в реестре пользователей. `Desktops`. Он также создает целевую связь для пользовательского профайла `JOHND` i5/OS в реестре пользователей `System_C`. Благодаря этому можно определить неизвестный идентификатор пользователя в целевой системе (`JOHND`) по его известному идентификатору в исходной системе (`jsday`).

Рисунок 6: Целевая и исходная связь EIM для идентификатора EIM `John Day`



Предположим также, что администратор EIM знает , что John Day использует один профайл i5/OS jsd1 в пяти различных системах. В данной ситуации администратор должен создать шесть связей для идентификатора EIM John Day, чтобы задать взаимосвязь между идентификатором и пользователем в пяти реестрах пользователей: исходную связь для johnday, субъект Kerberos в реестре пользователей Desktop_A и пять целевых связей для jsd1, пользовательский профайл i5/OS в пяти реестрах пользователей: System_B, System_C, System_D, System_E и System_F. Для снижения объема работы, необходимой для настройки преобразования EIM, администратор EIM создает групповой определение реестра. Члены группового определения реестра включают в себя имена определения реестра System_B, System_C, System_D, System_E, and System_F. Группировка членов позволяет администратору создать одну целевую связь с групповым определением реестра и пользовательским профайлом, вместо нескольких связей с отдельными именами определений реестра. Исходная и целевая связь предоставляют способ получения приложениями неизвестных пользовательских профайлов (цель, jsd1) в пяти реестрах пользователей, представленных как элементы группового определения реестра на базе известного пользовательского профайла (источник, johnday) как часть операции поиска EIM.

В некоторых случаях для одного и того же идентификатора 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.

Примечание: Для обычных пользователей как правило бывает достаточно создать только целевые связи.

В некоторых случаях для одного и того же идентификатора 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.

Допустим, например, что администратор использует функцию централизованного управления в System i Navigator для управления центральной системой и несколькими конечными системами. Администратор запускает различные функции, которые могут фактически выполняться как в центральной системе, так и в конечных системах. В такой ситуации удобно было бы создать исходные и целевые связи для каждого идентификатора пользователя администраторов во всех системах. В этом случае независимо от того, из какой системы администратор обращается к другим системам, применяемый им идентификатор можно будет преобразовать в соответствующий идентификатор в целевой системе, с которой работает администратор.

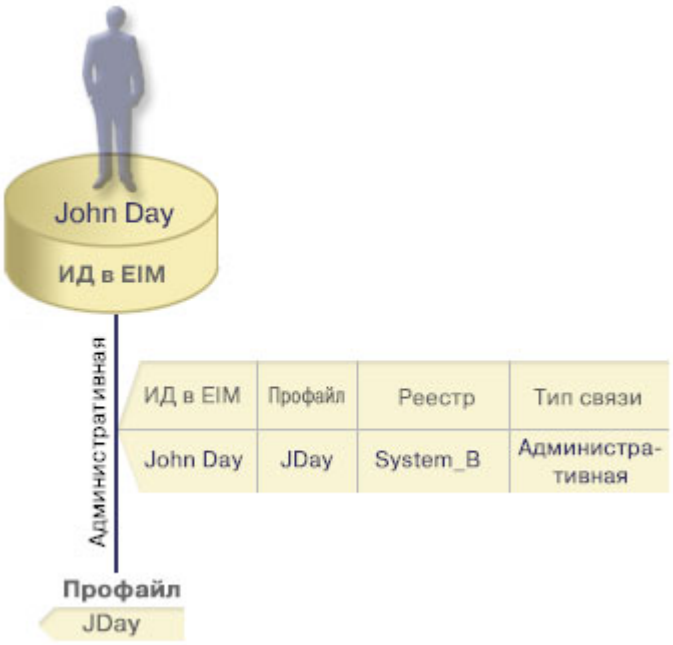
Административные связи

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.

Из-за особенностей этого типа связей, административные связи не могут применяться в операциях поиска соответствия EIM. Таким образом, операция поиска по исходному идентификатору пользователя с административной связью в EIM не вернет никаких результатов. Административные связи также не выдаются в качестве результата любых других операций поиска в EIM.

На рисунке 7 показан пример административной связи. В этом примере сотруднику по имени John Day в системе A предоставлен идентификатор пользователя John_Day, а в системе B, которая представляет собой систему с высокими требованиями к защите, - идентификатор JDay. Администратору системы необходимо гарантировать, что пользователи системы B 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 B (JDay), администратор EIM указывает, что у пользователя John Day есть учетная запись в системе B, но при этом EIM не предоставляет никаких сведений об идентификаторе JDay в операциях поиска EIM. Даже приложения системы B 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



Связи стратегий

Поддержка стратегий соответствия EIM позволяет администраторам EIM создавать и использовать связи стратегий, определяющие соответствие между несколькими идентификаторами пользователей в одном или нескольких реестрах и одним идентификатором пользователя в другом реестре.

Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM. Связи стратегий могут применяться как вместо связей идентификаторов, задающих однозначное соответствие между идентификатором EIM и отдельным идентификатором пользователя, так и в сочетании с такими связями.

Связи стратегий влияют только на те идентификаторы пользователей, для которых не существуют отдельные связи EIM. Если между идентификатором EIM и идентификатором пользователя есть связь идентификаторов, то приложению, выполняющему поиск соответствия, будет возвращен целевой идентификатор пользователя из этой связи, даже если существует связь стратегий и ее применение включено.

Существует три типа связей стратегий:

Понятия, связанные с данным

“Операции преобразования идентификаторов EIM” на стр. 27
Приложение или операционная система с помощью API EIM могут выполнять операции поиска, позволяющие установить соответствие между идентификатором пользователя в одном реестре и другим идентификатором в другом реестре. Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в неком целевом реестре по известной им информации об этом пользователе.

Связи стратегий домена по умолчанию:

Связи стратегий домена по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

Связи стратегий домена по умолчанию могут применяться для связывания исходного набора из нескольких идентификаторов пользователей (в данном случае - всех пользователей домена) с единым целевым идентификатором пользователя в заданном целевом реестре пользователей. В связи стратегий домена по умолчанию все пользователи домена являются исходными записями для преобразования, которые соответствуют одному целевому реестру и целевому идентификатору пользователя.

Для применения связей стратегии домена по умолчанию необходимо включить поиск соответствий с помощью связей стратегий для домена. Кроме того, необходимо включить поиск соответствий для целевого реестра пользователей. При настройке этих функций пользовательские реестры в связи стратегий можно будет применять в операциях поиска соответствий.

Связи стратегий домена по умолчанию применяются в том случае, когда операция поиска соответствий не обнаруживает в целевом реестре сведения, отвечающие связям идентификаторов, связям стратегий фильтров сертификатов или связям стратегий реестров по умолчанию. В результате все идентификаторы пользователей домена преобразуются в один целевой идентификатор пользователя, указанный в связи стратегии домена по умолчанию.

Допустим, например, что вы создали связь стратегий домена по умолчанию с целевым идентификатором пользователя `John_Day` в целевом реестре `Registry_xyz` и не создали никаких связей идентификаторов или других связей стратегий с этим идентификатором. Таким образом, при указании в операции поиска целевого реестра `Registry_xyz` стратегия домена по умолчанию гарантирует, что для всех идентификаторов пользователей домена, не имеющих других связей, в качестве результата будет возвращаться целевой идентификатор пользователя `John_Day`.

Для определения связи стратегии домена по умолчанию необходимо указать два значения:

- **Целевой реестр**. Целевой реестр представляет собой имя определения реестра EIM, содержащего идентификатор пользователя, в который преобразуются все идентификаторы пользователей домена.
- **Целевой пользователь**. В качестве целевого пользователя задается идентификатор пользователя, возвращаемый в качестве результата операции поиска соответствия EIM для данной связи стратегий.

Связь стратегии домена по умолчанию можно определить для каждого реестра в домене. Если на один и тот же целевой реестр указывает несколько связей стратегий домена, то необходимо определить для каждой из таких связей уникальную информацию для поиска, позволяющую операциям поиска различать эти связи. В противном случае операция поиска может вернуть несколько целевых идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.

Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед созданием и применением связей стратегий необходимо внимательно изучить поддержку стратегий преобразования EIM и работу операций поиска.

Примечание: Возможно, вам потребуется создать связь стратегии домена по умолчанию с целевым пользовательским профайлом, существующим в групповом определении реестра. Все пользователи домена являются исходными записями связи стратегии и соответствуют одному целевому пользовательскому профайлу в определении реестра целевой группы. Пользовательский профайл, заданный в связи стратегии домена по умолчанию, хранится вместе с элементами определения реестра группы.

Например, пользователь John Day использует тот же пользовательский профайл i5/OS `John_Day` в пяти различных системах: System B, System C, System D, System E и System F. Для снижения объема работ, необходимых для настройки преобразования EIM, администратор EIM создает групповое определение реестра с именем `Group_1`. К элементам группового определения реестра относятся имена определений реестров систем `System_B`, `System_C`, `System_D`, `System_E` и `System_F`. Группировка элементов позволяет администратору создать

отдельную целевую связь с групповым определением реестра и пользовательским профайлом, вместо создания нескольких связей с отдельными определениями реестра.

Администратор EIM создает связь стратегии домена по умолчанию с целевым профайлом пользователя `John_Day` в целевом реестре `Group_1`. В таком случае другие определенные связи идентификаторов или связи стратегии не действуют. Таким образом, при указании в операции поиска целевого реестра `Group_1` стратегия домена по умолчанию гарантирует, что для всех идентификаторов пользователей домена, не имеющих других связей идентификаторов, в качестве результата будет возвращаться целевой идентификатор пользователя `John_Day`.

Понятия, связанные с данным

"Информация для поиска" на стр. 16
При помощи EIM можно предоставить дополнительные данные, называемые информацией для поиска, которые позволяют более точно определить целевой идентификатор пользователя. Целевой идентификатор пользователя может быть задан либо в связи идентификаторов, либо в связи стратегий.

"Поддержка и активация стратегий преобразования EIM" на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

Связи стратегий реестра по умолчанию:

Связи стратегий реестра по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

Связи стратегий реестра по умолчанию могут применяться для связывания исходного набора из нескольких идентификаторов пользователей (в данном случае - пользователей реестра) с одним целевым идентификатором пользователя в заданном целевом реестре. В связи стратегий реестра по умолчанию все пользователи реестра являются исходными записями для преобразования, которые соответствуют одному целевому реестру и целевому идентификатору пользователя.

Для применения связей стратегий реестра по умолчанию необходимо включить поиск соответствий с помощью связей стратегий для домена. Кроме того, необходимо включить поиск соответствий для исходного реестра, а также включить поиск соответствий и применение связей стратегий для целевого реестра пользователей. При настройке этих функций пользовательские реестры в связи стратегий можно будет применять в операциях поиска соответствий.

Связи стратегий реестра по умолчанию применяются в том случае, когда операция поиска соответствий не обнаруживает в целевом реестре сведения, отвечающие связям идентификаторов, связям стратегий фильтров сертификатов или другим связям стратегий реестров по умолчанию. В результате все идентификаторы пользователей исходного реестра преобразуются в один целевой идентификатор пользователя, указанный в связи стратегии реестра по умолчанию.

Допустим, например, что вы создали связь стратегии реестра по умолчанию с исходным реестром `my_realm.com`, который содержит список субъектов области Kerberos. Для этой связи стратегий вы также указали целевой идентификатор пользователя `general_user1` в целевом реестре `os/400_system_reg`, представляющий собой пользовательский профайл в реестре пользователей i5/OS. В этом случае вы не создавали каких-либо связей идентификаторов или связей стратегий, применяемых к каким-либо идентификаторам пользователей в исходном реестре. Таким образом, при указании в операциях поиска соответствий целевого реестра `i5/OS_system_reg` и исходного реестра `my_realm.com` связь стратегий реестров по умолчанию гарантирует возврат целевого идентификатора пользователя `general_user1` для всех и идентификаторов пользователей из реестра `my_realm.com`, для которых не заданы конкретные связи идентификаторов или связи стратегий фильтров сертификатов.

Для определения связи стратегий реестров по умолчанию необходимо указать следующие три компонента:

- **Исходный реестр**. Это определение реестра, которое должно применяться в качестве источника в связи стратегий. Все идентификаторы пользователей исходного реестра должны соответствовать заданному в связи стратегий целевому пользователю.
- **Целевой реестр**. Целевой реестр представляет собой имя определения реестра EIM. Целевой реестр должен содержать целевой идентификатор пользователей, которому должны соответствовать все идентификаторы пользователей исходного реестра.
- **Целевой пользователь**. В качестве целевого пользователя задается идентификатор пользователя, возвращаемый в качестве результата операции поиска соответствия EIM для данной связи стратегий.

Вы можете определить несколько связей стратегии реестра по умолчанию. Если на один и тот же целевой реестр указывает несколько связей стратегий с одним и тем же исходным реестром, то необходимо определить для каждой из таких связей уникальную информацию для поиска, позволяющую операциям поиска различать эти связи. В противном случае операция поиска может вернуть несколько целевых идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.

Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед созданием и применением связей стратегий необходимо внимательно изучить поддержку стратегий преобразования EIM и работу операций поиска.

Примечание: Возможно, вам потребуется создать связь стратегии реестра по умолчанию с целевым пользовательским профайлом, существующим в групповом определении реестра. Все пользователи исходного реестра пользователей являются исходными записями связи стратегии и соответствуют одному целевому пользовательскому профайлу в определении реестра целевой группы. Пользовательский профайл, заданный в связи стратегии реестра по умолчанию, хранится вместе с элементами определения реестра группы.

Например, пользователь John Day использует один пользовательский профайл i5/OS `John_Day` в пяти различных системах: System_B, System_C, System_D, System_E и System_F. Для сокращения объема работ, необходимых для настройки преобразования EIM, администратор EIM создает групповое определение реестра с именем `Group_1`. Члены группового определения реестра включают в себя имена определения реестра `System_B, System_C, System_D, System_E, and System_F`. Группировка членов позволяет администратору создать одну целевую связь с групповым определением реестра и пользовательским профайлом, вместо нескольких связей с отдельными определениями реестра.

Администратор создал связь стратегии реестра по умолчанию с исходным реестром `my_realm.com`, который содержит список субъектов области Kerberos. Для этой связи стратегии он указывает целевой пользовательский профайл `John_Day` в целевом реестре `Group_1`. В таком случае, другие связи идентификатора или связи стратегии не действуют. Таким образом, при указании в операциях поиска соответствий целевого реестра `Group_1` и исходного реестра `my_realm.com` связь стратегий реестров по умолчанию гарантирует возврат целевого идентификатора пользователя `John_Day` для всех идентификаторов пользователей из реестра `my_realm.com` для которых не заданы конкретные связи идентификаторов.

Понятия, связанные с данным

“Информация для поиска” на стр. 16
При помощи EIM можно предоставить дополнительные данные, называемые информацией для поиска, которые позволяют более точно определить целевой идентификатор пользователя. Целевой идентификатор пользователя может быть задан либо в связи идентификаторов, либо в связи стратегий.

“Поддержка и активация стратегий преобразования EIM” на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

Связи стратегий фильтров сертификатов:

Связи стратегий фильтров сертификатов представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей. Связи стратегий фильтров сертификатов могут применяться для связывания исходного набора сертификатов с единым целевым идентификатором пользователя в заданном целевом реестре пользователей.

В связи стратегий фильтров сертификатов вы должны указать в качестве источника связи стратегий набор сертификатов из одного реестра X.509. Эти сертификаты связываются с единым указанным целевым реестром и целевым пользователем. В отличие от связи стратегий реестра по умолчанию, в которой источником связи стратегий являются все пользователи одного реестра, связи стратегий фильтров сертификатов характеризуются более гибкой областью применения. В качестве источника можно указать подмножество сертификатов из реестра. Область действия определяется указанным вами фильтром сертификатов для связи стратегий.

Примечание: Если необходимо связать все сертификаты, находящиеся в одном реестре пользователей X.509, с одним целевым идентификатором пользователя, то следует создать связь стратегии реестров по умолчанию.

Для применения связей стратегии фильтров сертификатов необходимо включить поиск соответствий с помощью связей стратегий для домена. Кроме того, необходимо включить поиск соответствий для исходного реестра, а также включить поиск соответствий и применение связей стратегий для целевого реестра пользователей. При настройке этих функций пользовательские реестры в связи стратегий можно будет применять в операциях поиска соответствий.

Если в операции поиска соответствия EIM исходным идентификатором пользователя является цифровой сертификат (после вызова в приложении API EIM `eimFormatUserIdentity()` для форматирования идентификатора пользователя), то EIM сначала проверит наличие связи между идентификатором EIM и указанным идентификатором пользователя. Если такой связи нет, то EIM сравнит указанную в DN информацию о сертификате с полной или частичной информацией DN, указанной в фильтре связи стратегий. Если информация DN в сертификате отвечает указанному фильтру, то EIM вернет целевой идентификатор пользователя, соответствующий связи стратегий. В результате сертификаты из исходного реестра X.509, отвечающие параметрам фильтра, будут связаны с целевым идентификатором пользователя в соответствии со связью стратегии фильтров сертификатов.

Допустим, например, что вы создали связь стратегии фильтров сертификатов с исходным реестром `certificates.x509`. Этот реестр содержит сертификаты всех сотрудников компании, включая те из них, с помощью которых все менеджеры отдела кадров могут обращаться к некоторым частным внутренним Web-страницам и другим ресурсам модели System i. Для этой связи стратегий вы также указали целевой идентификатор пользователей `hr_managers` в целевом реестре `system_abc`, представляющий собой пользовательский профайл в реестре пользователей i5/OS. Для того чтобы гарантировать применение в этой связи стратегий только сертификатов, принадлежащих менеджерам отдела кадров, вы указали фильтр сертификатов с отличительным именем субъекта (SDN) `ou=hrmgr,o=myco.com,c=us`.

В этом случае вы не создавали каких-либо связей идентификаторов или других связей стратегий фильтров сертификатов, применяемых к каким-либо идентификаторам пользователей в исходном реестре. Таким образом, при указании в операциях поиска целевого реестра `system_abc` и исходного реестра `certificates.x509` связь стратегий фильтра сертификатов гарантирует возврат целевого идентификатора пользователя `hr_managers` для всех сертификатов реестра `certificates.x509`, соответствующих указанному фильтру сертификатов и не имеющих собственных связей идентификаторов.

Для определения связи стратегий фильтра сертификатов необходимо указать следующую информацию:

- **Исходный реестр**. В качестве определения исходного реестра должен быть указан реестр пользователей X.509. Стратегия фильтров сертификатов создает связь между идентификаторами пользователей в этом реестре пользователей X.509 и одним целевым идентификатором пользователя. Эта связь применяется только к тем идентификаторам пользователей из реестра, которые отвечают параметрам заданного для этой стратегии фильтра сертификатов.

- **Фильтр сертификатов**. Фильтр сертификатов определяет набор схожих атрибутов сертификатов пользователей. Связь стратегий фильтров сертификатов устанавливает соответствие между сертификатами из реестра X.509 с перечисленными атрибутами и указанным целевым идентификатором пользователя. Фильтр задается на основании сочетания отличительного имени субъекта (SDN) и отличительного имени издателя (IDN), соответствующих тем сертификатам, которые должны применяться в качестве исходных. Заданный для стратегии фильтр сертификатов должен уже существовать в домене EIM.
- **Целевой реестр**. Определение целевого реестра представляет собой реестр пользователей, в котором хранится идентификатор пользователя, связываемый с сертификатами, отвечающими параметрам фильтра.
- **Целевой пользователь**. В качестве целевого пользователя задается идентификатор пользователя, возвращаемый в качестве результата операции поиска соответствия EIM для данной связи стратегий.

Поскольку связи стратегий сертификатов и другие связи могут применяться в самых разных сочетаниях, то перед созданием и применением связей стратегий сертификатов необходимо внимательно изучить поддержку стратегий преобразования EIM и работу операций поиска.

Примечание: Возможно, вам потребуется создать связь стратегии фильтрации сертификатов с целевым пользовательским профайлом, существующим в групповом определении реестра. Пользователи исходного реестра, отвечающие критериям, указанным в фильтре, являются исходными для связи стратегии и привязываются к целевому пользовательскому профайлу в целевом групповом определении реестра. Пользовательский профайл, заданный в связи стратегии фильтрации сертификатов, хранится вместе с элементами определения реестра группы.

Например, пользователь John Day использует тот же пользовательский профайл i5/OS `John_Day` в пяти различных системах: System B, System C, System D, System E и System F. Для снижения объема работ, необходимых для настройки преобразования EIM, администратор EIM создает групповое определение реестра. Члены группового определения реестра включают в себя имена определения реестра систем `System_B, System_C, System_D, System_E, and System_F`. Группировка пользователей позволяет администратору создать одиночную целевую связь с групповым определением реестра и пользовательским профайлом вместо нескольких связей с отдельными определениями реестра.

Администратор EIM создает связь стратегии фильтрации сертификатов, в которой задает подмножество сертификатов одного реестра X.509 в качестве источника связи стратегий. Он указывает целевой пользовательский профайл `John_Day` в целевом реестре `Group_1`. В данном случае другие указанные связи идентификатора или прочие связи стратегии фильтра сертификатов не действуют. Поэтому, когда в качестве целевого реестра операции поиска идентификаторов указан `Group_1`, все сертификаты в исходном реестре X.509, отвечающие критерию фильтра сертификатов, будут связаны указанным целевым пользовательским профайлом.

Фильтры сертификатов:

Фильтр сертификатов определяет набор схожих атрибутов сертификатов отличительных имен для группы сертификатов пользователей из исходного реестра пользователей X.509. Фильтр сертификатов можно использовать в качестве основы для связи стратегий фильтров сертификатов.

Фильтр сертификатов в связи стратегий определяет, какие сертификаты из указанного исходного реестра X.509 должны быть связаны с заданным целевым пользователем. При выполнении операций поиска соответствия преобразования идентификаторов в рамках предприятия (EIM) сертификаты, в которых информация DN субъекта и DN издателя соответствует параметрам фильтра, связываются с указанным целевым пользователем.

Допустим, например, что вы создали фильтр сертификатов с отличительным именем субъекта (SDN) `o=ibm,c=us`. Все сертификаты, содержащие такие DN в составе SDN, соответствуют параметрам фильтра, например, SDN `cn=JohnDay,ou=LegalDept,o=ibm,c=us`. Если существует несколько фильтров, параметрам которых отвечает сертификат, то наивысший приоритет будет имеет фильтр, параметры которого наиболее точно соответствуют сертификату. Допустим, например, что существует фильтр сертификатов с SDN `o=ibm,c=us` и фильтр с SDN `ou=LegalDept,o=ibm,c=us`. Если в исходном реестре X.509 есть сертификат с SDN `cn=JohnDay,ou=LegalDept,o=ibm,c=us`, то будет применяться второй, т.е. более точный фильтр. Если в исходном реестре X.509 есть сертификат с SDN `cn=SharonJones,o=ibm,c=us`, то будет применяться менее точный фильтр, поскольку сертификат лучше соответствует именно ему.

Для определения фильтра сертификатов можно задать одно из следующих значений или оба этих значения:

- Отличительное имя субъекта (SDN). Полное или частичное DN, указываемое в фильтре, должно соответствовать DN субъекта цифрового сертификата. Вы можете указать полную строку DN субъекта, либо одно или несколько частичных DN, которые могут составлять полное SDN.
- Отличительное имя издателя (IDN). Полное или частичное DN, указываемое в фильтре, должно соответствовать DN издателя цифрового сертификата. Вы можете указать полную строку DN издателя, либо одно или несколько частичных DN, которые могут составлять полное IDN.

Существует несколько способов создания фильтра сертификатов, включая применение API для форматирования фильтра стратегий EIM, позволяющего создать фильтр сертификатов путем использования сертификата в качестве шаблона для создания необходимых DN в требуемом порядке, а также формирования SDN и IDN.

Понятия, связанные с данным

“Отличительное имя” на стр. 48
Отличительное имя (DN) - это запись LDAP, уникальным образом идентифицирующая и описывающая запись сервера каталогов LDAP. Настроить хранение информации домена EIM на сервере каталогов можно с помощью мастера настройки EIM. Так как данные EIM хранятся на сервере каталогов, то контроллер домена EIM может применять для идентификации отличительные имена.

Информация, связанная с данной

Формат фильтра стратегий EIM (eimFormatPolicyFilter) API

Операции преобразования идентификаторов EIM

Приложение или операционная система с помощью API EIM могут выполнять операции поиска, позволяющие установить соответствие между идентификатором пользователя в одном реестре и другим идентификатором в другом реестре. Операция поиска в EIM - это процедура, в результате которой приложение или операционная система получают идентификатор пользователя в неком 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.

Когда приложение или операционная система вызывают API `eimGetTargetFromSource()` для получения целевого идентификатора пользователя в заданном реестре, то в качестве исходной информации они должны указать *исходный идентификатор пользователя*. При этом для указанного идентификатора пользователя, применяемого в операции поиска EIM, должна существовать исходная связь идентификатора, либо он должен попадать под действие связи стратегий. При вызове этого API приложение или операционная система должны передать следующие три значения:

- Исходный идентификатор пользователя, применяемый в качестве начальной точки поиска.
- Имя определения реестра EIM для исходного идентификатора пользователя.
- Имя определения реестра EIM, применяемого в операции поиска EIM в качестве целевого реестра. Это определение задает реестр пользователей, в котором находится искомый идентификатор пользователя.

Когда приложение или операционная система вызывают API `eimGetTargetFromIdentifier()` для заданного целевого реестра, то в качестве исходной информации они должны указать *идентификатор EIM*. При вызове этого API приложение должно передать следующие два значения:

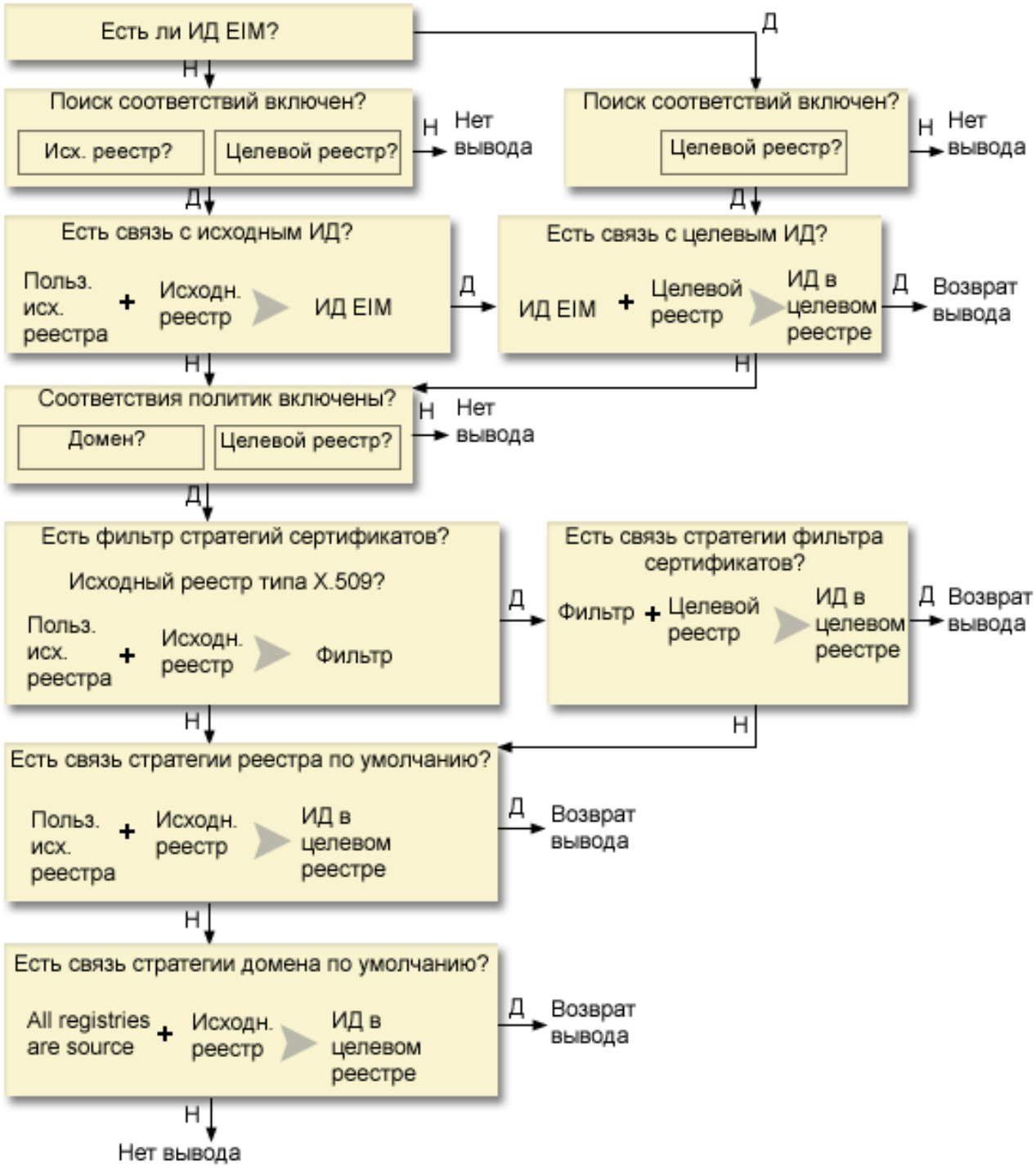
- Исходный идентификатор EIM, применяемый в качестве начальной точки поиска.
- Имя определения реестра EIM, применяемого в операции поиска EIM в качестве целевого реестра. Это определение задает реестр пользователей, в котором находится искомый идентификатор пользователя.

Для успешного выполнения операции поиска в EIM для пользователя должна существовать связь в целевом реестре. При этом может использоваться как целевая связь идентификаторов, так и связь стратегий.

Предоставленная информация передается в среду EIM, в которой выполняется поиск всех целевых идентификаторов пользователей. Поиск выполняется в порядке, проиллюстрированном на рисунке 10:

1. Целевые связи идентификаторов для идентификатора EIM. Идентификатор EIM можно получить одним из следующих способов: с помощью API `eimGetTargetFromIdentifier()` или с помощью информации, предоставляемой API `eimGetTargetFromSource()`.
2. Связь стратегии фильтра сертификатов.
3. Связь стратегии реестра по умолчанию.
4. Связь стратегии домена по умолчанию.

Рисунок 10: Диаграмма выполнения операции поиска EIM



Примечание: В следующей диаграмме операция поиска вначале проверяет отдельные определения реестра, такие как указанные исходные реестры или целевые реестры. Если операции поиска не удалось обнаружить преобразование с помощью отдельных определений реестра, он определяет, является ли отдельное определение реестра элементом группового определения реестра. Если это так, операция поиска проверяет групповое определение реестра для выполнения запроса поиска преобразования.

Операция поиска выполняется следующим образом:

1. Проверяется, разрешены ли операции поиска соответствия. В ходе проверки выясняется, разрешены ли операции поиска соответствия в указанном исходном и в целевом реестре. Если операции поиска соответствия запрещены в одном или в обоих реестрах, то операция прерывается и не возвращает целевой идентификатор пользователя.
2. Проверяется, существуют ли связи идентификаторов, соответствующие условиям поиска. Если был указан идентификатор EIM, то операция поиска будет применять имя этого идентификатора. В противном случае проверяется, существует ли исходная связь идентификаторов, соответствующая заданному исходному идентификатору пользователя и исходному реестру. Если такая связь существует, то она применяется для определения имени соответствующего идентификатора EIM. Затем по идентификатору EIM выполняется поиск целевой связи идентификаторов для идентификатора EIM, соответствующей указанному имени целевого определения реестра EIM. При наличии такой целевой связи идентификаторов операция поиска возвращает определенный в ней целевой идентификатор.
3. Проверяется, разрешено ли применение связей стратегий. Операция поиска проверяет, разрешено ли в домене преобразование идентификаторов с помощью связей стратегий. Проверяется также, разрешено ли применение связей стратегий в целевом реестре. Если применение связей стратегий в домене или в целевом реестре не разрешено, то операция прерывается и не возвращает целевой идентификатор пользователя.
4. Проверяются связи стратегий фильтров сертификатов. Операция поиска проверяет, относится ли исходный реестр к типу X.509. Если это так, то операция поиска проверяет, существует ли связь стратегии фильтра сертификатов, соответствующая указанным именам определений исходного и целевого реестра. Операция поиска проверяет, существуют ли в исходном реестре X.509 сертификаты, отвечающие условиям, заданным в связи стратегии фильтра сертификатов. Если связь стратегии существует и есть сертификаты, отвечающие условиям фильтрации, то операция поиска возвращает соответствующий этой связи целевой идентификатор пользователя.
5. Проверяется, существует ли связь стратегии реестра по умолчанию. Операция поиска проверяет, существует ли связь стратегии реестра по умолчанию, соответствующая заданным именам определений исходного и целевого реестра. Если связь стратегии существует, то операция поиска возвращает соответствующий этой связи целевой идентификатор пользователя.
6. Проверяется, существует ли связь стратегии домена по умолчанию. Операция поиска проверяет, существует ли связь стратегии домена по умолчанию, соответствующая определению целевого реестра. Если связь стратегии существует, то операция поиска возвращает соответствующий этой связи целевой идентификатор пользователя.
7. Операция поиска возвращает пустой набор результатов.

Для получения дополнительной информации об операциях поиска EIM просмотрите следующие примеры:

Понятия, связанные с данным

“Домен EIM” на стр. 7
Домен EIM - это каталог сервера LDAP, в котором хранятся данные EIM.

“Связи стратегий” на стр. 21
Поддержка стратегий соответствия EIM позволяет администраторам EIM создавать и использовать связи стратегий, определяющие соответствие между несколькими идентификаторами пользователей в одном или нескольких реестрах и одним идентификатором пользователя в другом реестре.

“Контроллер домена EIM” на стр. 6
Контроллер домена EIM - это сервер Упрощенного протокола доступа к каталогам (LDAP), настроенный для управления одним или несколькими доменами EIM. В домене EIM содержатся все идентификаторы, связи EIM и реестры пользователей домена. Системы (клиенты EIM) используют данные домена в операциях поиска EIM.

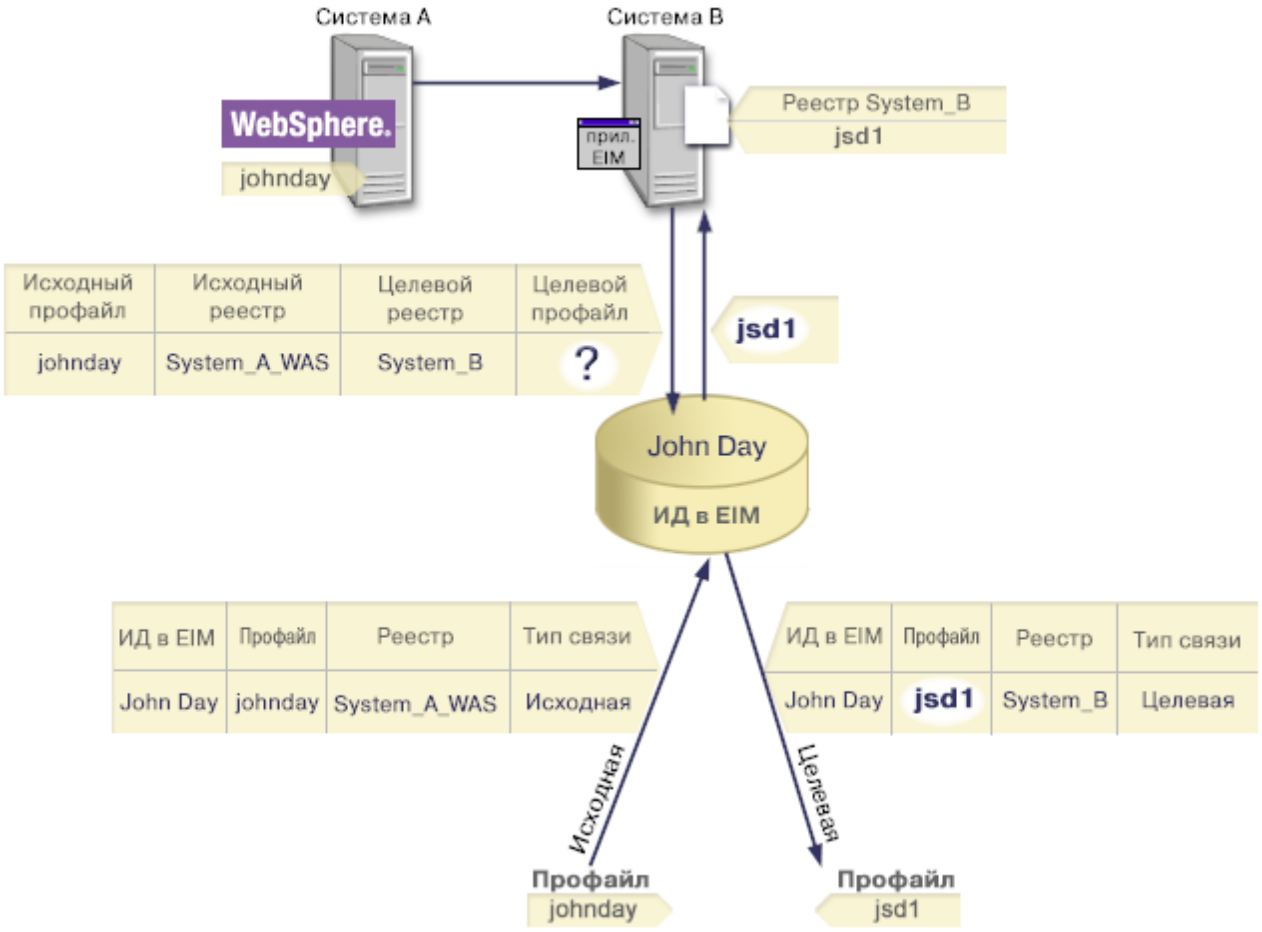
“Информация для поиска” на стр. 16
При помощи EIM можно предоставить дополнительные данные, называемые информацией для поиска, которые позволяют более точно определить целевой идентификатор пользователя. Целевой идентификатор пользователя может быть задан либо в связи идентификаторов, либо в связи стратегий.

Примеры операций поиска: Пример 1

Этот пример поясняет процесс поиска, применяемый операцией поиска, возвращающей целевой идентификатор пользователя с конкретных связей идентификаторов для известного идентификатора пользователя.

На рисунке 11 выполняется идентификация пользователя `johnday` на сервере приложений WebSphere с помощью алгоритма LPTA в системе A. Сервер приложений WebSphere в системе A вызывает программу в системе B для обращения к данным в этой системе. С помощью API EIM программа выполняет операцию поиска EIM, используя идентификатор пользователя в системе A в качестве источника. 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 в среду EIM, после чего выполняется поиск исходной связи идентификаторов, соответствующей заданной информации. Затем по идентификатору EIM `John Day` операция поиска EIM находит целевую связь идентификаторов, соответствующую имени определения целевого реестра EIM `System_B`. После этого идентификатор пользователя (`jsd1`) возвращается приложению.

Рисунок 11: Операция поиска EIM возвращает целевой идентификатор пользователя с помощью точной связи идентификаторов для известного идентификатора пользователя `johnday`



Примеры операций поиска: Пример 2

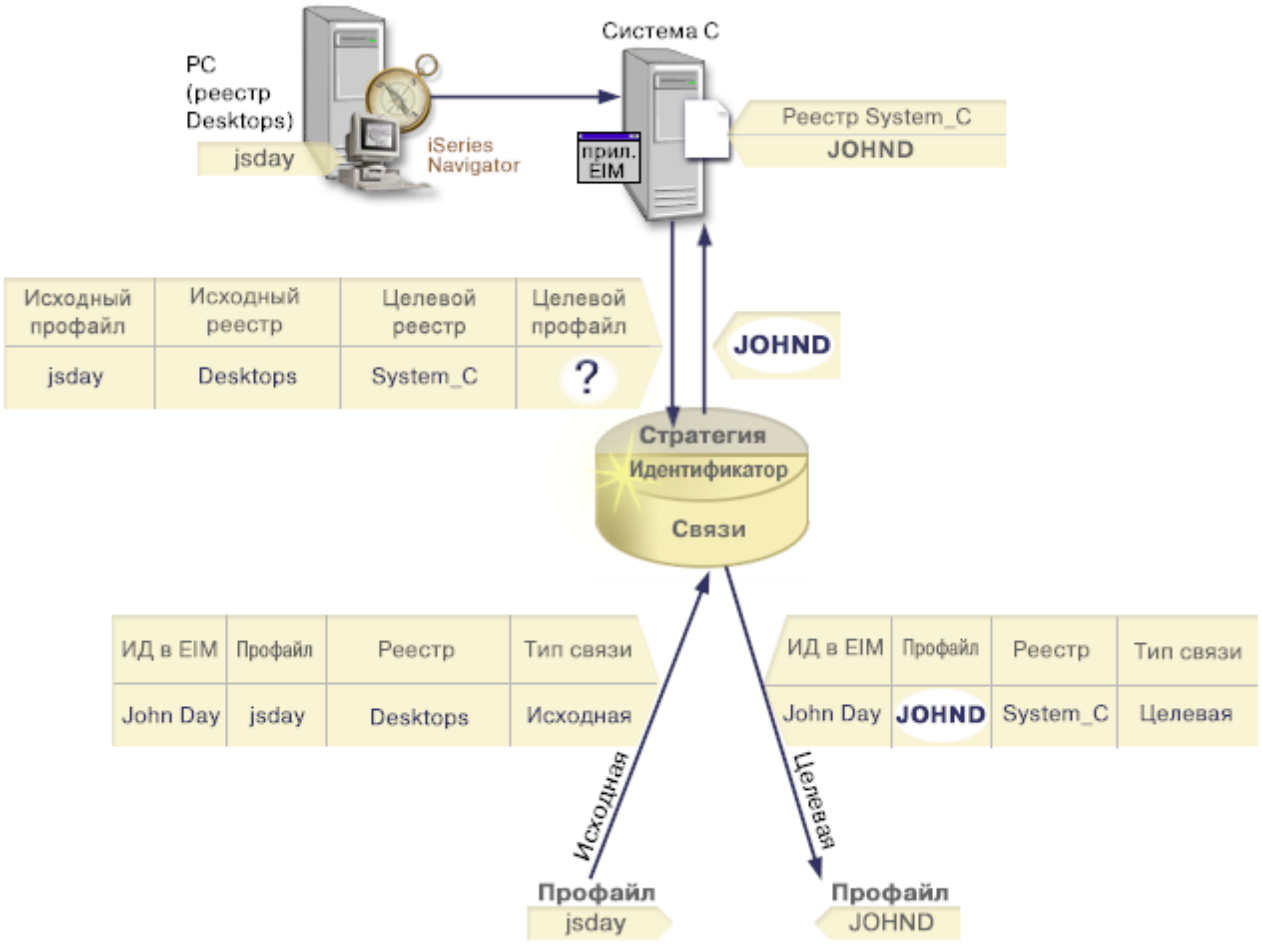
Этот пример поясняет процесс поиска, применяемый операцией поиска, возвращающей целевой идентификатор пользователя с конкретных связей идентификаторов для известного субъекта Kerberos.

На рисунке 12 администратор хочет связать пользователя Windows, зарегистрированного в реестре Windows Active Directory, с пользовательским профайлом i5/OS. Для идентификации Windows применяет Kerberos, а реестр Windows Active Directory определен в EIM под именем `Desktops`. Идентификатор пользователя, который администратор хочет связать с профайлом, - это субъект Kerberos `jsday`. Реестр i5/OS определен в EIM под именем `System_C`, а целевой пользовательский профайл называется `JOHND`.

Идентификатору EIM администратор присвоит имя `John Day`. После этого он создаст для этого идентификатора EIM две связи:

- Исходная связь с субъектом Kerberos `jsday` в реестре `Desktops`.
- Целевая связь с пользовательским профайлом i5/OS `JOHND` в реестре `System_C`.

Рисунок 12: Операция поиска EIM возвращает целевой идентификатор пользователя с помощью точной связи идентификаторов для известного субъекта Kerberos `jsday`



Такая конфигурация обеспечивает следующее преобразование субъекта Kerberos в пользовательский профайл i5/OS:

Исходный реестр и идентификатор пользователя	**--->**	**Идентификатор EIM**	**--->**	**Целевой идентификатор пользователя**
`jsday` в реестре `Desktops`	--->	John Day	--->	`JOHND` (в реестре `System_C`)

Операция поиска выполняется следующим образом:

1. Пользователь jsday входит в систему Windows и выполняет идентификацию с помощью субъекта Kerberos в реестре Windows Active Directory Desktops.
2. Пользователь открывает System i Navigator, чтобы получить доступ к данным, хранящимся в System_C.
3. i5/OS вызывает API EIM для выполнения операции поиска EIM с исходным идентификатором пользователя jsday, исходным реестром Desktops и целевым реестром System_C.
4. Операция поиска EIM проверяет, разрешены ли операции поиска соответствия в исходном реестре Desktops и в целевом реестре System_C. Такие операции разрешены.
5. Операция поиска проверяет наличие точной исходной связи идентификаторов, соответствующей исходному идентификатору пользователя jsday в реестре Desktops.
6. С помощью исходной связи идентификатора операция поиска находит идентификатор EIM John Day.
7. Затем по идентификатору EIM выполняется поиск целевой связи идентификаторов для идентификатора EIM, соответствующей определению целевого реестра EIM System_C.
8. Поскольку такая связь существует, то операция поиска возвращает определенный в этой связи целевой идентификатор пользователя JOHND.
9. После того, как целевой идентификатор пользователя будет найден, System i Navigator начнет работать под управлением пользовательского профайла JOHND. Права доступа пользователя к ресурсам и возможность выполнения операций в System i Navigator соответствуют параметрам профайла JOHND, а не идентификатора пользователя jsday.

Примеры операций поиска: Пример 3

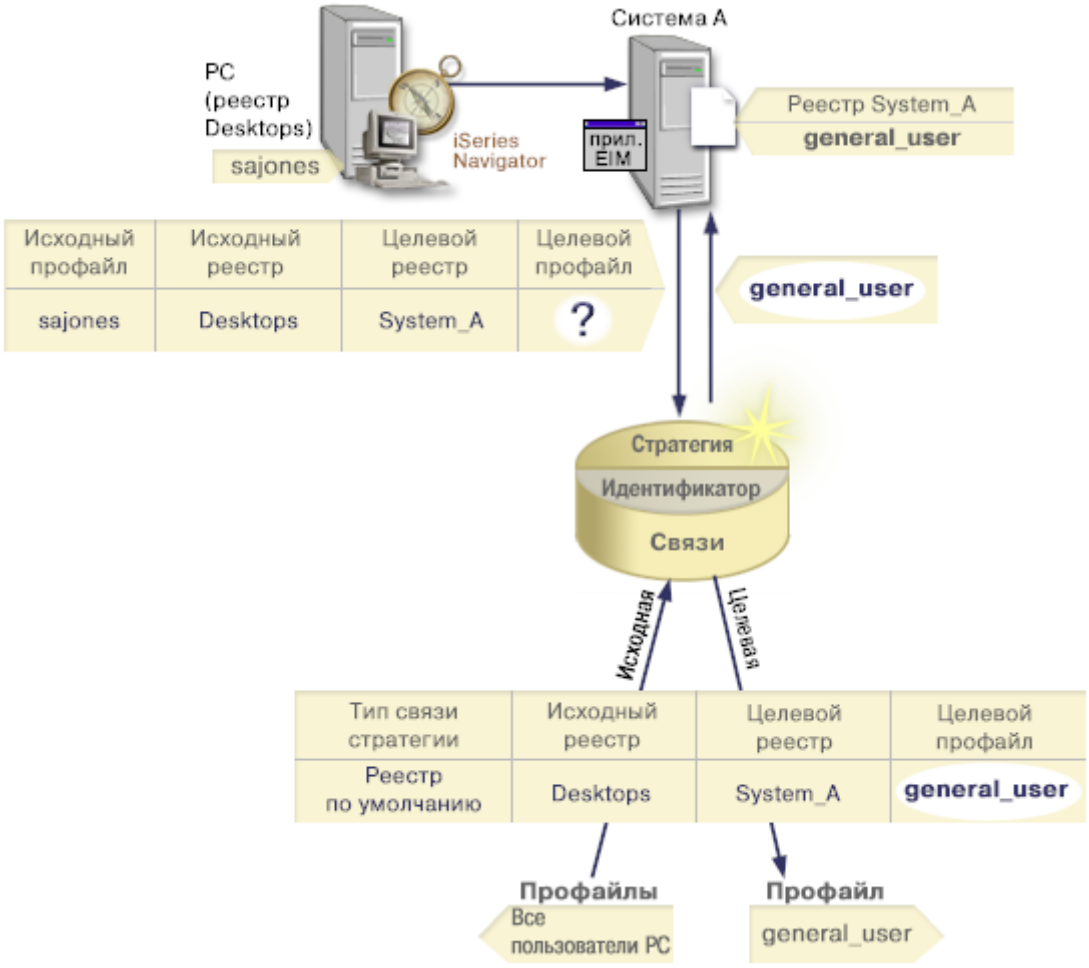
Этот пример поясняет процесс поиска, применяемый операцией поиска, возвращающей целевой идентификатор пользователя с помощью связи стратегии реестра по умолчанию.

В конфигурации, показанной на рисунке 13, администратор хочет связать всех пользователей рабочих станций, зарегистрированных в реестре Windows Active Directory, с пользовательским профайлом i5/OS general_user, определенным в среде EIM в реестре i5/OS registry that he named System_A. Для идентификации Windows применяет Kerberos, а реестр Windows Active Directory определен в EIM под именем Desktops. Один из идентификаторов пользователей, для которых администратор должен настроить преобразование, - это субъект Kerberos sajones.

Администратор создает связь стратегии реестра по умолчанию со следующей информацией:

- Исходный реестр Desktops.
- Целевой реестр System_A.
- Целевой идентификатор пользователя general_user.

Рисунок 13: Операция поиска возвращает целевой идентификатор пользователя с помощью связи стратегии реестра по умолчанию.



Такая конфигурация обеспечивает преобразование всех субъектов Kerberos из реестра `Desktops`, включая `sajones`, в пользовательский профайлi5/OS с именем `general_user`:

Исходный реестр и идентификатор пользователя	**--->**	**Связь стратегии реестра по умолчанию**	**--->**	**Целевой идентификатор пользователя**
`sajones` в реестре `Desktops`	--->	Связь стратегии реестра по умолчанию	--->	`general_user` в реестре `System_A`

Операция поиска выполняется следующим образом:

1. Пользователь `sajones` входит в систему Windows и выполняет идентификацию с помощью субъекта Kerberos в реестре `Desktops`.
2. Пользователь открывает System i Navigator, чтобы получить доступ к данным, хранящимся System A.
3. i5/OS вызывает API EIM для выполнения операции поиска EIM с исходным идентификатором пользователя `sajones`, исходным реестром `Desktops` и целевым реестром `System_A`.
4. Операция поиска EIM проверяет, разрешены ли операции поиска соответствия в исходном реестре `Desktops` и в целевом реестре `System_A`. Такие операции разрешены.
5. Операция поиска проверяет наличие точной исходной связи идентификаторов, соответствующей исходному идентификатору пользователя `sajones` в реестре `Desktops`. Точная связь идентификаторов не существует.
6. Операция поиска проверяет, разрешено ли в домене применение связей стратегий. Это разрешено.

7. Операция поиска проверяет, разрешено ли в целевом реестре применение связей стратегий (System_A). Это разрешено.
8. Операция поиска проверяет, является ли исходный реестр (Desktops) реестром X.509. Это не так.
9. Операция поиска проверяет, существует ли связь стратегии реестра по умолчанию, соответствующая имени определения исходного реестра (Desktops) и имени определения целевого реестра (System_A).
10. Операция поиска находит требуемую связь и возвращает целевой идентификатор пользователя general_user.

Иногда операция поиска EIM возвращает неоднозначные результаты. Результаты считаются неоднозначными, например, в том случае, если заданным условиям поиска соответствует несколько целевых идентификаторов пользователей. Некоторые приложения с поддержкой EIM, включая приложения и продукты i5/OS, не могут обрабатывать подобные неоднозначные результаты поиска и могут привести к непредсказуемым результатам. Для устранения этой ошибки могут потребоваться дополнительные действия. Например, для получения однозначного результата может потребоваться изменение конфигурации EIM или создание информации для поиска в каждом целевом идентификаторе пользователя. Кроме того, вы можете протестировать процедуру преобразования и определить, правильно ли действуют внесенные изменения.

Примеры операций поиска: Пример 4

Этот пример поясняет принцип работы операции поиска идентификаторов, возвращающей целевой идентификатор пользователя, являющегося членом группового определения реестра.

Администратор хочет связать пользователя Windows с пользовательским профайлом i5/OS. Kerberos является способом идентификации, используемым Windows, и именем реестра Kerberos, заданного администратором в EIM, является Desktop_A. Пользовательский идентификатор, который будет связан администратором, является субъектом Kerberos с именем jday. Именем определения реестра i5/OS, заданным администратором в EIM, является Group_1, пользовательским идентификатором, к которому администратор собирается выполнить привязку, является пользовательский профайл JOHND, существующий в трех отдельных реестрах: System_B, System_C и System_D. Каждый отдельный реестр является элементом группового определения реестра Group_1.

Администратор создает идентификатор EIM с именем John Day. После этого он создаст для этого идентификатора EIM две связи:

- Исходная связь с субъектом Kerberos jday в реестре Desktop_A.
- Целевая связь с пользовательским профайлом i5/OS JOHND в реестре Group_1 .

Такая конфигурация обеспечивает следующее преобразование субъекта Kerberos в пользовательский профайл i5/OS:

Исходный реестр и идентификатор пользователя	**--->**	**Идентификатор EIM**	**--->**	**Целевой идентификатор пользователя**
jday в реестре Desktop_A	--->	John Day	--->	JOHND (в групповом определении реестра Group_1)

Операция поиска выполняется следующим образом:

1. Пользователь (jday) входит в систему Windows в Desktop_A.
2. Пользователь открывает System i Navigator, чтобы получить доступ к данным, хранящимся в System_B.
3. i5/OS вызывает API EIM для выполнения операции поиска EIM с исходным идентификатором пользователя jday, исходным реестром Desktop_A и целевым реестром System_B.
4. Операция поиска EIM проверяет, разрешены ли операции поиска соответствия в исходном реестре (Desktop_A) и в целевом реестре (System_B).

5. Операция поиска проверяет наличие точной отдельной связи идентификаторов, соответствующей исходному идентификатору пользователя jday в реестре Desktop_A.
6. С помощью связи идентификатора операция поиска находит идентификатор EIM John Day.
7. С помощью данного имени идентификатора EIM операция поиска выполняет поиск индивидуальной целевой связи для идентификатора EIM, совпадающего с указанным именем целевого определения реестра EIM System_B. (Она отсутствует).
8. Операция поиска проверяет, является ли какой-либо исходный реестр (Desktop_A) элементом группового определения реестра. (Не является).
9. Операция поиска проверяет, является ли какой-либо целевой реестр (System_B) элементом группового определения реестра. Он является элементом группового определения реестра Group_1.
10. Затем по идентификатору EIM выполняется поиск индивидуальной связи идентификаторов для идентификатора EIM, соответствующей определению целевого реестра EIM Group_1.
11. Поскольку такая связь существует, то операция поиска возвращает определенный в этой связи целевой идентификатор пользователя JOHND.

Примечание: В некоторых случаях операция поиска EIM возвращает неоднозначные результаты, если заданным условиям поиска соответствует несколько целевых идентификаторов пользователей. Так как EIM не может возвратить одиночный целевой идентификатор пользователя, в приложениях с поддержкой EIM, включая приложения и продукты i5/OS, не предназначенные к обработке этих неоднозначных результатов, может произойти сбой или непредвиденная ситуация. Для устранения этой ошибки могут потребоваться дополнительные действия. Например, для получения однозначного результата может потребоваться изменение конфигурации EIM или создание информации для поиска в каждом целевом идентификаторе пользователя. Вы можете протестировать процедуру преобразования и определить, правильно ли действуют внесенные изменения.

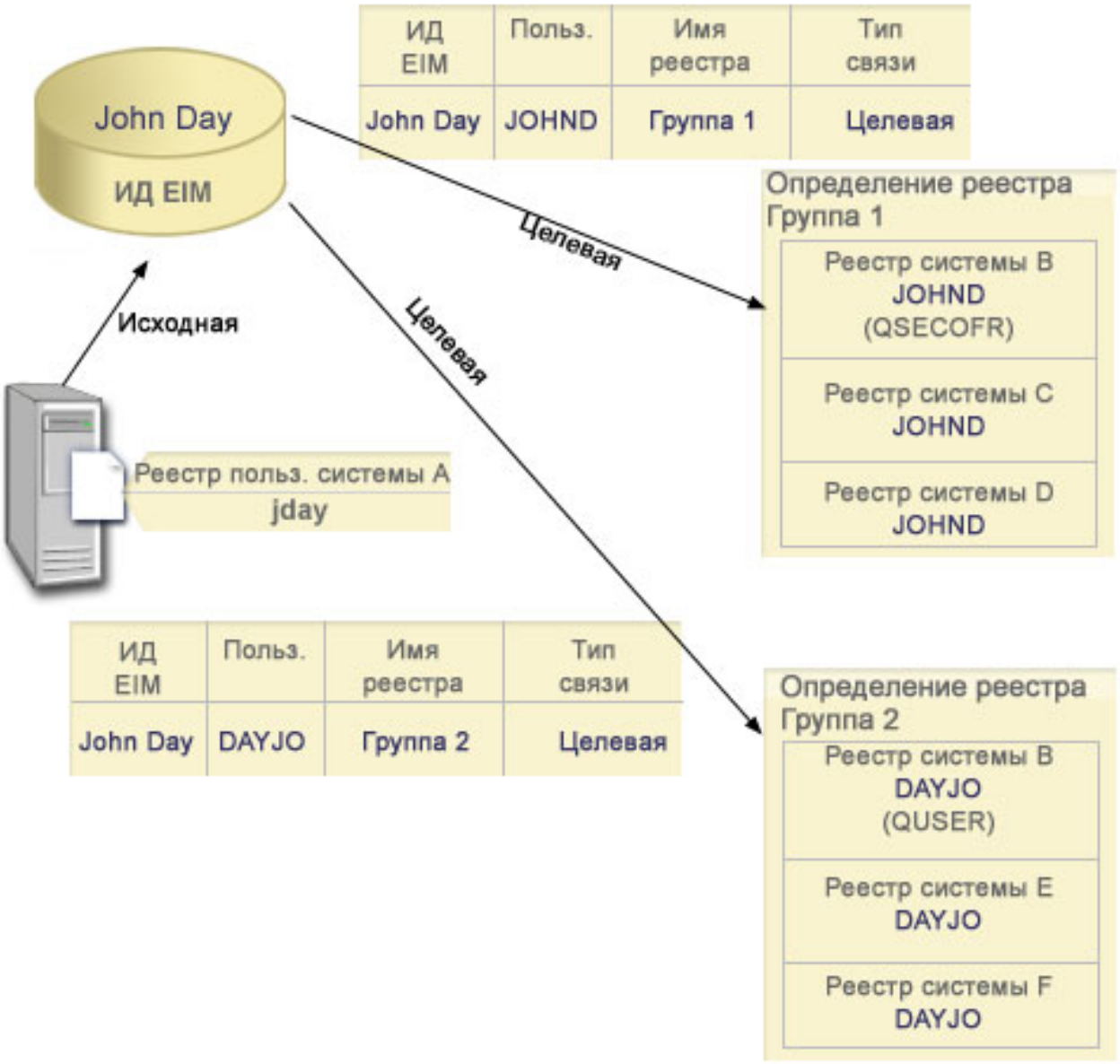
Примеры операций поиска: Пример 5

Данный пример содержит сведения возврате операцией поиска неоднозначных результатов, содержащих групповые определения реестра.

В некоторых случаях операция поиска возвращает неоднозначные результаты если заданным условиям поиска соответствует несколько целевых идентификаторов пользователей. Так как неоднозначные результаты могут привести к сбою приложения, использующего EIM, необходимо принять меры для предотвращения или устранения данной ситуации.

В частности будьте готовы к возврату неоднозначного результата операцией поиска идентификаторов при указании отдельного определения реестра пользователей в качестве элемента нескольких групповых определений реестра. Если отдельное определение реестра пользователей является элементом группового определения реестра и были созданы отдельные связи идентификаторов EIM или связи стратегии, использующие групповое определение реестра в качестве исходного или целевого реестра, операция поиска может вернуть неоднозначные результаты. Например, вы можете использовать два различных пользовательских профайла для двух разных типов выполняемых задач: вы выполняете задачи в качестве администратора защиты, для чего вам требуется пользовательский профайл с правами доступа QSECOFR, и вы выполняете обычные пользовательские задачи, и вам требуется пользовательский профайл с правами доступа QUSER. Если оба пользовательские профайла находятся в одном реестре пользователей, являющемся элементом двух разных групповых определений реестра, и вы создаете целевые связи идентификаторов для обоих целевых пользовательских профайлов, операция поиска обнаружит оба целевые пользовательские профайлы и вернет неоднозначный результат.

Следующий пример иллюстрирует возникновение неполадки при указании отдельного определения реестра в качестве элемента двух групповых определений реестра и вы указываете одно из групповых определений реестра в качестве целевого реестра для двух отдельных связей идентификаторов EIM.



Пример:

John Day использует следующие пользовательские профайлы в определении системного реестра с именем реестра пользователей `System B`:

- JOHND
- DAYJO

Реестр пользователей `System B` является элементом следующих групповых определений реестра:

- `Group 1`
- `Group 2`

Идентификатор EIM John Day имеет две целевые связи со следующими параметрами:

- Целевая связь: Целевой реестр `Group 1` содержит пользовательский профайл `JOHND` в реестре пользователей `System B`.

- Целевая связь: Целевой реестр Group 2 содержит пользовательский профайл DAYJO в реестре пользователей System B.

В данной ситуации операция поиска преобразований возвращает неоднозначные результаты так как критерию поиска соответствует несколько целевых пользовательских профайлов; оба пользовательские профайла (JOHND и DAYOJO) отвечают указанному критерию поиска.

Точно так же операция поиска идентификатора может вернуть неоднозначные результаты, если вы создали две связи стратегии (вместо одной связи идентификатора EIM), использующие групповые определения реестра в качестве целевых реестров.

для предотвращения операции поиска от возврата неоднозначного результата с групповыми определениями реестра, обратите внимание на следующие замечания:

- Укажите отдельный реестр пользователей в качестве элемента только одного группового определения реестра.
- Будьте осторожны при создании отдельных связей идентификаторов EIM или связей стратегии, использующих групповые определения реестра в качестве целевого или исходного реестра. Убедитесь, что групповое определение реестра является элементом только одного группового определения реестра. Имейте в виду, что если элемент целевого группового определения реестра также является элементом другого группового определения реестра, операция поиска может вернуть неоднозначные результаты.
- Если вы столкнулись с неоднозначными результатами, указав отдельное определение реестра в качестве элемента нескольких групповых определений реестра и вы создали отдельную связь идентификатора или связь стратегии, применяющую одно из этих групповых определений реестра в качестве исходного или целевого реестра, вы можете задать уникальные сведения для поиска для каждого целевого пользовательского профайла в каждой связи для более точного поиска.

Вы можете задать следующую информацию поиска для каждого целевого пользовательского профайла в примере с John Day:

- Для JOHND: задайте Administrator для поиска
- Для DAYJO: задайте User для поиска

Однако следует помнить, что базовые приложения i5/OS, такие как System i Access for Windows, не могут различать несколько возвращенных операцией поиска целевых идентификаторов пользователей с помощью информации для поиска. Следовательно, необходимо переопределить связи в домене, обеспечив возврат операциями поиска соответствий только одного идентификатора пользователя, что гарантирует приложениям i5/OS возможность успешного поиска соответствий и преобразования идентификаторов.

Понятия, связанные с данным

“Групповое определение реестра” на стр. 15
Логическая группировка определений реестров позволяет сократить объем работ, необходимых для настройки преобразования EIM. Можно управлять групповым определением реестра так же, как и отдельным определением реестра.

Поддержка и активация стратегий преобразования EIM

Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

Поддержка стратегий соответствия EIM позволяет включать и выключать применение связей стратегий как для всего домена в целом, так и для отдельных реестров пользователей. EIM также позволяет указать, может ли каждый конкретный реестр применяться в операциях поиска соответствий. Таким образом, использование поддержки стратегий соответствия позволяет более точно управлять способом возврата результатов при поиске соответствий.

По умолчанию во всех доменах EIM операции поиска соответствий, использующие связи стратегий, запрещены. В этом случае все выполняемые в домене операции поиска соответствий возвращают только результаты, полученные на основании связей между конкретными идентификаторами пользователей и идентификаторами EIM.

По умолчанию также включено применение всех реестров в операциях поиска соответствий, а применение связей стратегий в этих реестрах выключено. При включении связей стратегий для отдельного целевого реестра необходимо также включить соответствующую поддержку в домене.

В каждом отдельном реестре можно настроить применение связей стратегий и применение этого реестра в операциях поиска соответствий одним из следующих трех способов:

- Операции поиска соответствий для данного реестра запрещены. Другими словами, приложение, выполняющее поиск соответствий с применением этого реестра, не сможет получить результаты.
- Операции поиска соответствий могут использовать только конкретные связи между идентификаторами пользователей и идентификаторами EIM. В этом случае операции поиска соответствий в реестре разрешены, но связи стратегий в этом реестре не применяются.
- Операции поиска соответствий могут использовать конкретные связи между идентификаторами пользователей и идентификаторами EIM, когда такие связи существуют, либо связи стратегий, когда связи между отдельными идентификаторами не существуют.

Понятия, связанные с данным

"Информация для поиска" на стр. 16
При помощи EIM можно предоставить дополнительные данные, называемые информацией для поиска, которые позволяют более точно определить целевой идентификатор пользователя. Целевой идентификатор пользователя может быть задан либо в связи идентификаторов, либо в связи стратегий.

"Связи стратегий домена по умолчанию" на стр. 21
Связи стратегий домена по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

"Связи стратегий реестра по умолчанию" на стр. 23
Связи стратегий реестра по умолчанию представляют собой один из типов связей стратегий, которые могут применяться для создания множественных связей (несколько с одним) между идентификаторами пользователей.

"Создание связи стратегий" на стр. 106
Связь стратегий непосредственно определяет взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре.

Задачи, связанные с данной

"Включение связи стратегий для домена" на стр. 91
Связи стратегий представляют собой средство создания соответствий между группой идентификаторов и одним идентификатором пользователя в том случае, когда идентификатор EIM не существует.

"Включение поддержки поиска соответствий и связей стратегий для целевого реестра" на стр. 99
Поддержка стратегий преобразования преобразования идентификаторов в рамках предприятия (EIM) позволяет применять связи стратегий для создания соответствий между группой идентификаторов и одним идентификатором пользователя в том случае, когда идентификатор EIM не существует. Связь стратегий позволяет преобразовать исходный набор из нескольких идентификаторов пользователей в отдельный целевой идентификатор пользователя, определенный в заданном целевом реестре.

Управление доступом EIM

Пользователь EIM - это пользователь, обладающий правами доступа EIM в соответствии с членством в предопределенных группах пользователей LDAP выбранного домена.

При настройке прав доступа EIM пользователь добавляется в группу пользователей LDAP выбранного домена. Каждая группа LDAP имеет права доступа на выполнение определенных административных задач

EIM в этом домене. Тип задач (включая операции поиска соответствий EIM), выполнение которых разрешено пользователю EIM, определяется группой управления доступом, в состав которой входит пользователь EIM.

Примечание: Для настройки EIM вы должны подтвердить свои полномочия в контексте сети, а не только в контексте какой-либо одной системы. Права доступа на настройку EIM основаны не на правах доступа пользовательского профайла i5/OS, а на правах доступа EIM. Поскольку технология EIM представляет собой сетевой ресурс, а не ресурс какой-либо отдельной системы, то EIM при настройке не распознает специальные права доступа i5/OS, такие как *ALLOBJ или *SECADM. Однако после завершения настройки EIM права доступа на выполнение различных задач можно будет задавать на основе различных типов пользователей, включая пользовательские профайлы i5/OS. Например, IBM Tivoli Directory Server for i5/OS рассматривает профайлы i5/OS с правами доступа *ALLOBJ и *IOSYSCFG как профайлы администраторов каталога.

Добавлять пользователей в группу управления доступом EIM и изменять права доступа пользователей могут только пользователи с правами доступа администратора EIM. Для того чтобы пользователя можно было добавить в группу управления доступом EIM, этому пользователю должна соответствовать запись на сервере каталогов, выполняющем функции контроллера домена EIM. Кроме того, следует помнить, что в группу управления поиском EIM могут входить лишь отдельные категории пользователей. Идентификатор пользователя, определенный на сервере каталогов, может быть задан в формате субъекта Kerberos, отличительного имени LDAP или пользовательского профайла i5/OS.

Примечание: Для того чтобы в EIM в качестве типа пользователя был доступен субъект Kerberos, необходимо настроить в системе службу сетевой идентификации. Для того чтобы в EIM в качестве типа пользователя был доступен пользовательский профайл i5/OS, необходимо настроить на сервере каталогов суффикс системных объектов. Тем самым вы предоставите серверу каталогов возможность обращения к системным объектам i5/OS, в том числе к пользовательским профайлам i5/OS.

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

Администратор Упрощенного протокола доступа к каталогам (LDAP)

Администратору LDAP в каталоге соответствует особое отличительное имя (DN), определяющее его как администратора всего каталога в целом. Таким образом, у администратора LDAP есть доступ ко всем административным функциям EIM, а также доступ ко всем данным каталога. Пользователь с таким уровнем доступа может выполнять следующие операции:

- Создание домена.
- Удаление домена.
- Создание и удаление идентификаторов EIM.
- Создание и удаление определений реестров EIM.
- Создание и удаление исходных, целевых и административных связей.
- Создание и удаление связей стратегий.
- Создание и удаление фильтров сертификатов.
- Включение и выключение применения связей стратегий для домена.
- Включение и выключение операций поиска соответствий для реестра.
- Включение и выключение применения связей стратегий для реестра.
- Выполнение операций поиска EIM.
- Получение связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.
- Добавление, удаление и просмотр сведений об управлении доступом EIM.
- Изменение и удаление идентификационных данных зарегистрированного пользователя.

Администратор EIM

Членам этой группы управления доступом разрешено изменение любых данных в домене EIM. Пользователь с таким уровнем доступа может выполнять следующие операции:

- Удаление домена.
- Создание и удаление идентификаторов EIM.
- Создание и удаление определений реестров EIM.
- Создание и удаление исходных, целевых и административных связей.
- Создание и удаление связей стратегий.
- Создание и удаление фильтров сертификатов.
- Включение и выключение применения связей стратегий для домена.
- Включение и выключение операций поиска соответствий для реестра.
- Включение и выключение применения связей стратегий для реестра.
- Выполнение операций поиска EIM.
- Получение связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.
- Добавление, удаление и просмотр сведений об управлении доступом EIM.
- Изменение и удаление идентификационных данных зарегистрированного пользователя.

Администратор идентификаторов

Членам этой группы управления доступом разрешено изменять идентификаторы EIM, исходные и административные связи. Пользователь с таким уровнем доступа может выполнять следующие операции:

- Создание идентификаторов EIM.
- Добавление и удаление исходных связей.
- Добавление и удаление административных связей.
- Выполнение операций поиска EIM.
- Получение связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.

Поиск соответствий EIM

Членам этой группы управления доступом разрешено выполнение операций поиска соответствий EIM. Пользователь с таким уровнем доступа может выполнять следующие операции:

- Выполнение операций поиска EIM.
- Получение связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.

Администратор реестра

Членам этой группы управления доступом разрешено управление всеми определениями реестров EIM. Пользователь с таким уровнем доступа может выполнять следующие операции:

- Добавление и удаление целевых связей.
- Создание и удаление связей стратегий.
- Создание и удаление фильтров сертификатов.
- Включение и выключение операций поиска соответствий для реестра.
- Включение и выключение применения связей стратегий для реестра.
- Выполнение операций поиска EIM.

- Получение связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.

Администратор выбранных реестров

Членам этой группы управления доступом разрешено управлять информацией EIM только для заданного определения реестра (например, `Registry_X`). Члены этой группы управления доступом могут также добавлять и удалять целевые связи для заданного определения реестра пользователей. Для выполнения всех операций поиска соответствий и операций управления связями стратегий пользователь с такими правами доступа должен также входить в состав группы **Операции преобразования EIM**. Пользователь с таким уровнем доступа может выполнять следующие операции в заданных определениях реестров:

- Создание, удаление и просмотр целевых связей для заданных определений реестров EIM.
- Добавление и удаление связей стратегий домена по умолчанию.
- Добавление и удаление связей стратегий для заданных определений реестров.
- Добавление фильтров сертификатов для заданных определений реестров.
- Включение и выключение операций поиска соответствий для заданных определений реестров.
- Включение и выключение применения связей стратегий для заданных определений реестров.
- Получение идентификаторов EIM.
- Получение связей идентификаторов и фильтров сертификатов для заданных определений реестров.
- Получение информации об определении реестра EIM для заданных определений реестров.

Примечание: Если указанное определение реестра является групповым определением реестра, пользователь с правами Администратор выбранных реестров имеет доступ с правами администратора только к группе, но не к элементам группы.

Пользователь, одновременно входящий в группы управления доступом **Администратор выбранных реестров** и **Операции преобразования EIM**, может выполнять следующие операции:

- Добавление и удаление связей стратегий для заданных реестров.
- Выполнение операций поиска EIM.
- Получение всех связей идентификаторов, связей стратегий, фильтров сертификатов, идентификаторов EIM и определений реестров EIM.

Поиск одноразового разрешения

Эта группа прав доступа позволяет пользователям извлекать идентификационные сведения, например, пароль.

Если пользователь с данными правами доступа хочет выполнить дополнительную операцию EIM, он должен быть членом группы прав доступа, обеспечивающей доступ к данной операции EIM. Например, если пользователь хочет извлечь целевую связь из исходной связи, он должен быть членом одной из следующих групп:

- Администратор EIM
- Администратор идентификаторов
- Операции поиска связанных идентификаторов EIM
- Администратор реестра

Понятия, связанные с данным

“Особенности работы с пользовательскими профайлами i5/OS в EIM” на стр. 50
Возможность выполнения операций в EIM определяется не правами доступа вашего пользовательского профайла i5/OS, а правами доступа к EIM.

“Выявление требуемых навыков и ролей” на стр. 55
Технология преобразования идентификаторов в рамках предприятия (EIM) устроена таким образом, что

в небольшой организации отвечать за настройку и администрирование может один человек. В более крупных организациях эти обязанности можно распределить между несколькими сотрудниками.

Задачи, связанные с данной

“Управление правами доступа пользователей EIM” на стр. 120
Пользователь EIM - это пользователь, обладающий правами доступа в соответствии с членством в предопределенных группах пользователей LDAP. При настройке доступа EIM пользователь добавляется в соответствующую группу пользователей LDAP.

Группа управления доступом EIM: права доступа к API

Данная информация содержит таблицы, организованные с помощью операции преобразования идентификаторов в рамках предприятия (EIM), выполняемой API.

В каждой таблице приведены сведения обо всех API EIM и различных группах управления доступом EIM, которым разрешено выполнять соответствующие функции EIM.

Таблица 1. Работа с доменами

API EIM	Администратор LDAP	Администратор EIM	Администратор идентификаторов	Поиск соответствия в EIM	Администратор реестра	Администратор выбранного реестра
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 соответствия 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	-	-	-	-
eimGetAssociated Identifiers	X	X	X	X	X	X

Таблица 3. Работа с реестрами

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск соответствия в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddApplication Registry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Associations	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X

Таблица 3. Работа с реестрами (продолжение)

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск соответствия в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimListRegistry Users	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

Таблица 4. Работа со связями идентификаторов. 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.

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск соответствия в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddAssociation (для административных связей)	X	X	X	-	-	-
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. Работа со связями стратегий

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск соответствия в EIM	Администратор реестров EIM	Администратор конкретного реестра EIM
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

Таблица 6. Работа с записями соответствия

API EIM	Администратор LDAP	Администратор EIM	Администратор ИД EIM	Поиск соответствия 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 7. Работа со средствами доступа

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

Группа управление доступом EIM: права доступа к задачам EIM

В следующей таблице проиллюстрирована взаимосвязь между различными группами управления доступом EIM и задачами EIM, которые разрешено выполнять этим группам.

Несмотря на то, что администратор LDAP не указан в таблице, этот уровень доступа необходимо для создания нового домена EIM. Кроме того, администратор LDAP может выполнять те же операции, что и администратор EIM, но администратор EIM не получает автоматически прав доступа администратора LDAP.

Таблица 8. Таблица 1: Группы управления доступом EIM

Задача EIM	Администратор EIM	Администратор идентификаторов	Операции поиска соответствия EIM	Администратор реестра	Администратор выбранного реестра	Поиск одноразового разрешения
Создание домена	-	-	-	-	-	
Удаление домена	X	-	-	-	-	
Изменение домена	X	-	-	-	-	
Включение/ выключение связей стратегий для домена	X	-	-	-	-	
Поиск доменов	X	-	-	-	-	
Добавление реестра систем	X	-	-	-	-	
Добавление реестра приложений	X	-	-	-	-	
Удаление реестра	X	-	-	-	-	
Изменение реестра	X	-	-	X	X	
Включение/ выключение поиска соответствия для реестра	X	-	-	X	X	

Таблица 8. Таблица 1: Группы управления доступом EIM (продолжение)

Задача EIM	**Администратор EIM**	**Администратор идентификаторов**	**Операции поиска соответствия EIM**	**Администратор реестра**	**Администратор выбранного реестра**	**Поиск одноразового разрешения**
Включение/ выключение связей стратегий для реестра	X	-	-	X	X	
Поиск реестров	X	X	X	X	X	
Добавление ИД	X	X	-	-	-	
Удаление ИД	X	-	-	-	-	
Изменение ИД	X	X	-	-	-	
Поиск ИД	X	X	X	X	X	
Получение связанных ИД	X	X	X	X	X	
Добавление/ удаление административных связей	X	X	-	-	-	
Добавление/ удаление исходных связей	X	X	-	-	-	
Добавление/ удаление целевых связей	X	-	-	X	X	
Добавление/ удаление связей стратегий	X	-	-	X	X	
Добавление/ удаление фильтра сертификатов	X	-	-	X	X	
Поиск фильтра сертификатов	X	X	X	X	X	
Поиск связей	X	X	X	X	X	
Поиск связей стратегий	X	X	X	X	X	
Получение целевой связи из исходной	X	X	X	X	-	
Получение целевой связи по ИД	X	X	X	X	X	

Таблица 8. Таблица 1: Группы управления доступом EIM (продолжение)

Задача EIM	**Администратор EIM**	**Администратор идентификаторов**	**Операции поиска соответствия EIM**	**Администратор реестра**	**Администратор выбранного реестра**	**Поиск одноразового разрешения**
Изменение пользователей реестра	X	-	-	X	X	
Поиск пользователей реестра	X	X	X	X	X	
Изменение псевдонима реестра	X	-	-	X	X	
Поиск псевдонимов реестра	X	X	X	X	X	
Получение реестра по псевдониму	X	X	X	X	X	
Добавление/ удаление средств управления доступом EIM	X	-	-	-	-	
Просмотр элементов группы управления доступом	X	-	-	-	-	
Просмотр средств управления доступом EIM для выбранного пользователя	X	-	-	-	-	
Запрос средств управления доступом EIM	X	-	-	-	-	
Изменить одноразовое разрешение	X	-	-	-	-	-
Извлечь одноразовое разрешение	X	-	-	-	-	X
1 - Если указанное определение реестра является групповым определением реестра, пользователь с правами Администратор выбранных реестров имеет доступ с правами администратора только к группе, но не к элементам группы.						

Основная информация о применении LDAP в EIM

EIM применяет сервер LDAP в качестве контроллера домена для хранения данных EIM. В связи с этим вам обязательно следует ознакомиться со сведениями об LDAP, относящимися к настройке и применению EIM на предприятии. Например, вы можете использовать отличительные имена LDAP в качестве идентификаторов пользователей при настройке EIM и при идентификации в системе контроллера домена EIM.

Для более глубокого ознакомления с принципами работы и настройки EIM ознакомьтесь со следующими сведениями об LDAP:

Отличительное имя

Отличительное имя (DN) - это запись LDAP, уникальным образом идентифицирующая и описывающая запись сервера каталогов LDAP. Настроить хранение информации домена EIM на сервере каталогов можно с помощью мастера настройки EIM. Так как данные EIM хранятся на сервере каталогов, то контроллер домена EIM может применять для идентификации отличительные имена.

Отличительное имя состоит из имени самой записи и имен объектов, расположенных над ней в каталоге LDAP. Эти имена указываются в порядке возрастания уровней. Пример полного отличительного имени: `cn=Tim Jones, o=IBM, c=US`. По крайней мере один атрибут записи содержит ее имя. Атрибут, содержащий имя, называется относительным отличительными именем (RDN) записи. Запись, расположенная над RDN, называется родительским отличительным именем. В данном примере `cn=Tim Jones` - имя записи, или RDN. `o=IBM, c=US` - родительское DN записи `cn=Tim Jones`.

Поскольку данные EIM хранятся на сервере каталогов, то отличительные имена можно использовать в качестве идентификаторов пользователей на контроллере домена. Вы также можете использовать отличительное имя идентификатора пользователя, применявшегося для настройки EIM на платформе System i. Например, отличительные имена могут применяться в следующих ситуациях:

- Настройка сервера каталогов в качестве контроллера домена EIM. Для этого создается и применяется отличительное имя, идентифицирующее администратора LDAP на сервере каталогов. Если сервер каталогов не настроен в системе, то его можно создать в процессе создания нового домена и добавления в него сервера с помощью мастера настройки EIM.
- Выбор в мастере настройки EIM типа идентификатора пользователя, применяемого для подключения к контроллеру домена EIM. Отличительное имя - один из доступных типов пользователей. Отличительное имя должно представлять пользователя, которому предоставлены права на создание объектов в локальном пространстве имен сервера каталогов.
- Выбор в мастере настройки EIM типа пользователя, применяемого для выполнения операций EIM от имени функций операционной системы. Эти операции включают поиск соответствий и удаление связей при удалении локального пользовательского профайла i5/OS. Отличительное имя - один из доступных типов пользователей.
- Подключение к контроллеру домена для администрирования EIM, например, для управления реестрами и идентификаторами и выполнения операций поиска связанных идентификаторов.
- Создание фильтров сертификатов для определения области действия связи стратегии фильтра сертификатов. При создании фильтра сертификатов необходимо задать информацию об отличительном имени субъекта или выдавшей сертификат организации, либо информацию о сертификате. Эта информация определяет условия фильтрации, применяемые для выбора сертификатов, к которым применяется связь стратегии.

Понятия, связанные с данным

“Родительское отличительное имя” на стр. 49
Родительское отличительное имя (DN) - это запись в пространстве имен сервера каталогов LDAP. Записи сервера LDAP образуют иерархическую структуру, которая может отражать политические, географические, организационные границы или границы доменов. Отличительное имя считается родительским, если оно находится в пространстве имен сервера на уровне, непосредственно предшествующем рассматриваемому DN.

"Фильтры сертификатов" на стр. 26
Фильтр сертификатов определяет набор схожих атрибутов сертификатов отличительных имен для группы сертификатов пользователей из исходного реестра пользователей X.509. Фильтр сертификатов можно использовать в качестве основы для связи стратегий фильтров сертификатов.

Информация, связанная с данной

Общие сведения о сервере каталогов

Родительское отличительное имя

Родительское отличительное имя (DN) - это запись в пространстве имен сервера каталогов LDAP. Записи сервера LDAP образуют иерархическую структуру, которая может отражать политические, географические, организационные границы или границы доменов. Отличительное имя считается родительским, если оно находится в пространстве имен сервера на уровне, непосредственно предшествующем рассматриваемому DN.

Пример полного отличительного имени: `cn=Tim Jones, o=IBM, c=US`. По крайней мере один атрибут записи содержит ее имя. Атрибут, содержащий имя, называется относительным отличительными именем (RDN) записи. Запись, расположенная над RDN, называется родительским отличительным именем. В данном примере `cn=Tim Jones` - имя записи, или RDN. `o=IBM, c=US` - родительское DN записи `cn=Tim Jones`.

EIM использует сервер каталогов в качестве контроллера домена, на котором хранятся данные EIM. Родительское DN в сочетании с именем домена EIM определяет расположение данных домена EIM в пространстве имен сервера каталогов. При добавлении сервера в новый домен с помощью мастера настройки EIM можно указать родительское DN для создаваемого домена. Задав родительское DN, можно указать расположение данных домена EIM в пространстве имен LDAP. Если родительское DN указано не будет, то данные EIM будут храниться в отдельном суффиксе пространства имен. Расположение данных домена EIM по умолчанию: `ibm-eimDomainName=EIM`.

Понятия, связанные с данным

"Отличительное имя" на стр. 48
Отличительное имя (DN) - это запись LDAP, уникальным образом идентифицирующая и описывающая запись сервера каталогов LDAP. Настроить хранение информации домена EIM на сервере каталогов можно с помощью мастера настройки EIM. Так как данные EIM хранятся на сервере каталогов, то контроллер домена EIM может применять для идентификации отличительные имена.

Информация, связанная с данной

Общие сведения о сервере каталогов

Схема LDAP и другие особенности EIM

Информация о требованиях сервера каталога для работы с EIM.

EIM требует размещения контроллера домена на сервере каталогов, поддерживающем протокол LDAP версии 3. Кроме того, продукт сервера каталогов должен обеспечивать поддержку схемы EIM, а также следующих атрибутов и классов объектов:

- Атрибут ibm-entryUUID.
- Следующие типы атрибутов ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate
  - ownerSource
- Атрибуты EIM, включая три новых атрибута для поддержки связей стратегий:
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc

- ibm-eimDomainName, ibm-eimDomainVersion,
- ibm-eimRegistryAliases
- ibm-eimRegistryEntryName
- ibm-eimRegistryName
- ibm-eimRegistryType
- ibm-eimSourceUserAssoc
- ibm-eimTargetIdAssoc
- ibm-eimTargetUserName
- ibm-eimUserAssoc
- ibm-eimFilterType
- ibm-eimFilterValue
- ibm-eimPolicyStatus

• Классы объектов EIM, включая три новых класса для поддержки связей стратегий:
- ibm-eimApplicationRegistry
- ibm-eimDomain
- ibm-eimIdentifier
- ibm-eimRegistry
- ibm-eimRegistryUser
- ibm-eimSourceRelationship
- ibm-eimSystemRegsitry
- ibm-eimTargetRelationship
- ibm-eimFilterPolicy
- ibm-eimDefaultPolicy
- ibm-eimPolicyListAux

Понятия, связанные с данным

“Контроллер домена EIM” на стр. 6
Контроллер домена EIM - это сервер Упрощенного протокола доступа к каталогам (LDAP), настроенный для управления одним или несколькими доменами EIM. В домене EIM содержатся все идентификаторы, связи EIM и реестры пользователей домена. Системы (клиенты EIM) используют данные домена в операциях поиска EIM.

Концепции преобразований идентификаторов в рамках предприятия (EIM) для i5/OS

Технологию преобразования идентификаторов в рамках предприятия (EIM) можно реализовать на любой платформе IBM eServer. Однако при использовании EIM в модели System i следует иметь в виду ряд особенностей, связанных с реализацией System i.

Для того, чтобы больше узнать о приложениях i5/OS, активированных для EIM, замечаниях о пользовательских профайлах и других темах, которые помогут эффективно использовать EIM на платформе System i, см. следующую информацию:

Особенности работы с пользовательскими профайлами i5/OS в EIM

Возможность выполнения операций в EIM определяется не правами доступа вашего пользовательского профайла i5/OS, а правами доступа к EIM.

Существует ряд дополнительных задач, которые необходимо выполнить для настройки в i5/OS возможности взаимодействия с EIM. Эти дополнительные задачи требуют наличия пользовательского профайла i5/OS со специальными правами доступа.

Для настройки взаимодействия i5/OS с EIM с помощью System i Navigator у вашего пользовательского профайла должны быть следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)
- Права доступа на настройку системы (*IOSYSCFG)

Расширения команд работы с пользовательскими профайлами i5/OS для взаимодействия с EIM

После настройки в системе EIM вы сможете использовать новый параметр команд Создать пользовательский профайл (CRTUSRPRF) и Изменить пользовательский профайл (CHGUSRPRF). Этот параметр называется EIMASSOC. Этот параметр позволяет определять связи идентификаторов EIM для заданного пользовательского профайла из локального реестра.

При использовании данного параметра вы можете указать следующую информацию:

- Имя идентификатора EIM, который может быть применяться в качестве нового имени уже существующего идентификатора.
- Опция действия, позволяющая добавлять (*ADD), заменять (*REPLACE) или удалять (*REMOVE) указанную связь.

  Примечание: Для настройки новых связей указывайте опцию *ADD. Опция *REPLACE может применяться, например, в том случае, если вы определили связь с неправильным идентификатором. Опция *REPLACE удаляет все существующие связи записей локального реестра с другими идентификаторами, а затем добавляет новую связь, указанную в этом параметре. Опция *REMOVE позволяет удалить любые заданные связи выбранного идентификатора.
- Тип связи идентификатора: исходная, целевая, исходная и целевая, или административная.
- Опция создания указанного идентификатора EIM, если он еще не существует.

Для профайлов i5/OS обычно создаются целевые связи, особенно в среде с единым входом в систему. После создания с помощью команды необходимой целевой связи пользовательского профайла (а при необходимости и идентификатора EIM) вы можете создать соответствующую исходную связь. Создать исходную связь пользовательского профайла с другим идентификатором, например, с субъектом Kerberoeros, применяемым для входа в систему, можно с помощью System i Navigator.

При настройке EIM для системы вы указали идентификатор и пароль, которые должны применяться при выполнении операций EIM от имени операционной системы. У этого идентификатора должны быть права доступа EIM, достаточные для создания идентификаторов и добавления связей.

Пароли пользовательских профайлов i5/OS

Ваша основная задача, как администратора, заключается в настройке EIM как составной части среды с единым входом в систему, позволяющей сократить затраты на управление паролями пользователей предприятия или организации. Применение предоставляемых EIM возможностей преобразования идентификаторов в сочетании с идентификацией Kerberos позволяет сократить количество вводимых пользователями паролей и тем самым упростить жизнь как пользователям, так и администраторам. Выигрыш достигается за счет меньшего числа обращений, связанных с устранением неполадок идентификаторов пользователей, например, просьб сбросить забытые пользователями пароли. Однако правила стратегии управления паролями по-прежнему остаются в силе и вам по-прежнему нужно будет обслуживать пользовательские профайлы при истечении срока действия паролей.

Для реализации дополнительных преимуществ в среде с единым входом в систему вы можете изменить пароли для пользовательских профайлов, указанных в целевых связях. Если профайл является целевым идентификатором связи, то соответствующему пользователю не нужно указывать пароль при обращении к

платформе System i или к ресурсам приложений i5/OS с поддержкой EIM. Обычно для таких профайлов можно указать пароль *NONE, запрещающий непосредственный вход в систему с помощью таких пользовательских профайлов. Благодаря применению EIM и среды с единым входом в систему, владельцу этого пользовательского система больше не нужно применять пароль. Присвоив паролю значение *NONE, можно избежать в дальнейшем необходимости помнить об истечении срока действия пароля; кроме того, никто не сможет использовать профайл для непосредственного входа на платформу System i или для обращения к ресурсам i5/OS с поддержкой EIM. Тем не менее, в такой конфигурации можно сохранить пароли пользовательских профайлов администраторов на тот случай, если им придется непосредственно входить на платформу System i. Например, в случае сбоя контроллера домена и невозможности обращения к службе преобразования идентификаторов администратор сможет непосредственно входить на платформу System i до тех пор, пока не будут устранены неполадки контроллера домена.

Понятия, связанные с данным

“Управление доступом EIM” на стр. 39
Пользователь EIM - это пользователь, обладающий правами доступа EIM в соответствии с членством в предопределенных группах пользователей LDAP выбранного домена.

Информация, связанная с данной

Создать пользовательский профайл (CRTUSRPRF), команда

Контроль i5/OS и EIM

При составлении общего плана защиты важно учитывать применяемые средства контроля.

При настройке и применении EIM вы можете настроить поддержку контроля сервера каталогов, обеспечив тем самым уровень контроля, соответствующий требованиям стратегии защиты. Например, поддержка контроля может потребоваться при определении того, какие пользователи, определенные путем связи стратегии, выполнили в вашей системе ту или иную операцию или изменили объект.

Информация, связанная с данной

Контроль сервера каталогов

Приложения для i5/OS с поддержкой EIM

EIM может использовать различные приложения i5/OS.

Применение EIM можно настроить в следующих приложениях i5/OS:

- Серверы хоста i5/OS (в настоящее время используемые System i Access for Windows
- и System i Navigator)
- Сервер Telnet (в настоящее время применяется эмулятором PC5250 и продуктом IBM Websphere host on demand)
- QFileSrv.400 ODBC (позволяет организовать единый вход в систему с помощью SQL)
- JDBC (позволяет использовать EIM с помощью SQL)
- Distributed Relational Database Architecture (DRDA) (позволяет использовать EIM с помощью SQL)
- IBM WebSphere Host On-Demand версии 8, (функция Web Express Logon)
- i5/OS NetServer
- QFileSvr.400

Сценарии: Преобразования идентификаторов в рамках предприятия

Сведения об управлении пользовательскими профайлами в различных системах в среде с единым входом в систему.

Технология преобразования идентификаторов в рамках предприятия (EIM) - это технология инфраструктуры IBM, позволяющая управлять идентификаторами пользователей в масштабах предприятия.

Обычно EIM применяется совместно с технологией идентификации, например, со службой сетевой идентификации, для настройки среды с единым входом в систему.

Информация, связанная с данной

Сценарии единого входа в систему

Планирование EIM

Перед настройкой EIM необходимо разработать план реализации EIM, гарантирующий успешную настройку EIM в среде System i или в многоплатформенной среде.

Для успешной настройки и эксплуатации технологии EIM на предприятии следует обязательно составить план реализации EIM. Для разработки плана реализации необходимо собрать данные о системах, приложениях и пользователях, которые будут работать с EIM. На основании собранной информации вы сможете выбрать оптимальный способ настройки EIM.

Поскольку EIM представляет собой технологию инфраструктуры IBM eServer, поддерживаемую всеми платформами IBM, то конкретный план реализации определяется применяемыми платформами. Несмотря на то, что существует множество операций, специфичных для отдельных платформ, многие операции планирования EIM относятся ко всем платформам IBM. Вам понадобится выполнить общие операции планирования EIM и создать собственный план реализации. Дополнительные сведения о планировании конкретной реализации EIM приведены в следующих разделах:

Планирование EIM для eServer

Для успешной настройки и эксплуатации технологии EIM на предприятии с широким набором платформ следует обязательно составить план реализации EIM. Для разработки плана реализации необходимо собрать данные о системах, приложениях и пользователях, которые будут работать с EIM. На основании собранной информации вы сможете выбрать оптимальный способ настройки EIM в среде с различными платформами.

Ниже приведен справочный список задач планирования, которые необходимо выполнить перед началом настройки и использования EIM в среде с различными платформами. Эта информация поможет вам составить эффективный план настройки EIM, включая выбор необходимой информации для сбора, выявление необходимых навыков сотрудников и ознакомление с перечнем принимаемых решений. Вы можете распечатать справочные таблицы планирования EIM (номер 8 в списке) и заполнить их в ходе планирования.

Требования для поддержки EIM на серверах eServer

Для успешной реализации EIM на предприятии существует три обязательных набора требований: уровень сети или предприятия, система и приложение.

Требования уровня сети или предприятия

Одну из систем вашего предприятия или сети необходимо настроить в качестве контроллера домена EIM, который представляет собой особым образом настроенный сервер LDAP, хранящий и предоставляющий данные домена EIM. Существует множество факторов, которые следует учитывать при выборе сервера каталогов в качестве контроллера домена, включая тот факт, что не все серверы LDAP обеспечивают поддержку контроллера домена EIM.

Еще одним важным фактором является наличие средств администрирования. Одним из вариантов является применение API EIM в ваших собственных административных приложениях. Если в качестве контроллера домена EIM вы планируете использовать IBM Tivoli для i5/OS то для управления EIM можно применять System i Navigator. Если вы планируете воспользоваться продуктам IBM Directory, то вы сможете использовать утилиту eimadmin, входящую в состав LDAP SPE V1R4.

Ниже приведена общая информация о том, какие платформы IBM предоставляют серверы каталогов с поддержкой EIM. Информацию о выборе сервера каталогов с поддержкой контроллера домена EIM вы можете найти в разделе Планирование контроллера домена EIM.

Требования к системе и приложениям

Каждая система, входящая в состав домена EIM, должна отвечать ряду требований:

- На ней должен быть установлен клиент LDAP.
- На ней должны быть реализованы API EIM.

Каждое приложение в домене EIM должно иметь возможность применения API EIM для поиска соответствий и выполнения других операций.

Примечание: В случае распределенного приложения применение API EIM одновременно на сервере и клиенте может быть необязательным. Как правило, API EIM необходимы только серверному компоненту приложения.

Следующая таблица содержит информацию о поддержке EIM, предоставляемой платформами eServer. Информация упорядочена по платформам и включает следующие сведения:

- Клиент EIM, необходимый для поддержки API EIM платформой.
- Тип конфигурации EIM и средств администрирования для данной платформы.
- Сервер каталогов, который можно установить на данной платформе для применения в качестве контроллера домена EIM.

Для работы в домене EIM платформа может не отвечать требованиям, обязательным для контроллера домена EIM.

Таблица 9. Поддержка EIM платформами eServer

Платформа	Клиент EIM (поддержка API)	Контроллер домена	Средства администрирования EIM
AIX на System p	AIX R5.2	IBM Directory V5.1	Нет
Linux • SLES8 на PPC64 • Red Hat 7.3 на i386 • SLES7 на System z	Загрузите один из следующих продуктов: • Клиент IBM Directory V4.1 • Клиент IBM Directory V5.1 • Открытый клиент LDAP v2.0.23	IBM Directory V5.1	Нет
i5/OS на System i	i5/OS V5R3 или выше	IBM Tivoli Directory Server for i5/OS	System i Navigator
Windows 2000 на System x	Загрузите один из следующих продуктов: • Клиент IBM Directory V4.1 • Клиент IBM Directory V5.1	Клиент IBM Directory V5.1	Нет
z/OS на System z	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

Если платформа обеспечивает поддержку клиента EIM (API), то данная система может работать в домене EIM. Если вы не планируете использовать систему в качестве контроллера домена EIM на предприятии, то поддержка контроллера домена EIM этой платформой необязательна.

Информация, связанная с данной

Сервер каталогов IBM Tivoli

Выявление требуемых навыков и ролей

Технология преобразования идентификаторов в рамках предприятия (EIM) устроена таким образом, что в небольшой организации отвечать за настройку и администрирование может один человек. В более крупных организациях эти обязанности можно распределить между несколькими сотрудниками.

Необходимое количество сотрудников зависит от навыков, которыми обладает каждый член коллектива, от платформ, включенных в состав реализации EIM, а также от того, как в вашей организации принято распределять роли и обязанности, связанные с обеспечением безопасности.

Правильная реализация EIM требует настройки и взаимодействия нескольких различных программных продуктов. Поскольку для работы с каждым из этих продуктов требуются определенные навыки и роли, то в коллектив, обеспечивающий реализацию EIM, вы можете включить сотрудников, специализирующихся в различных областях, особенно при работе в большой организации.

Приведенная ниже информация содержит список навыков и прав доступа, необходимых для успешной реализации EIM. Необходимые навыки представлены названиями должностей тех сотрудников, которые специализируются в данной области. Например, задача, требующая навыков работы с протоколом LDAP, указана как задача для администратора сервера каталогов.

Члены коллектива и их роли

В этом разделе описаны обязанности и необходимые права доступа для ролей, применяемых для управления EIM. Этот список ролей позволит вам определить членов коллектива, которым можно будет поручить установку и настройку обязательных продуктов, а также настройку EIM и одного или нескольких доменов EIM.

Один из первых наборов ролей, которые вам потребуется определить - это количество и тип администраторов домена EIM. Все сотрудники, на которых будут возложены обязанности по администрированию EIM, и которым будут предоставлены соответствующие права доступа, обязательно должны участвовать в процессе планирования EIM.

Примечание: Администраторы EIM играют важную роль в организации и именно они имеют возможность создавать идентификаторы пользователей в ваших системах. При создании связей EIM для идентификаторов пользователей они определяют, кто может обращаться к компьютерным системам, и какие права доступа при этом предоставляются пользователям. IBM рекомендует предоставлять такой уровень доступа лишь тем сотрудникам, которым вы полностью доверяете.

В следующей таблице перечислены возможные роли членов коллектива, а также задачи и навыки, необходимые для настройки и обслуживания EIM.

Примечание: Если за выполнение всех задач настройки и администрирования EIM в вашей организации будет отвечать один сотрудник, то для этого сотрудника необходимо выбрать роль администратора EIM и предоставить соответствующие права доступа.

Таблица 10. Роли, задачи и навыки для настройки EIM

Роль	Задачи, к которым есть доступ	Необходимые навыки
Администратор EIM	• Координация операций, выполняемых в домене • Добавление, удаление и изменение определений реестров, идентификаторов EIM и связей идентификаторов пользователей • Доступ для управления данными в домене EIM	Знакомство с инструментами администрирования EIM
Администратор ИД EIM	• Создание и изменение идентификаторов EIM • Добавление и удаление административных и исходных связей (добавление и удаление целевых связей запрещено)	Знакомство с инструментами администрирования EIM
Администратор реестров EIM	Управление всеми определениями реестров EIM: • Добавление и удаление целевых связей (добавление и удаление исходных и административных связей запрещено) • Обновление определений реестров EIM	Необходимы следующие знания и навыки: • Знакомство со всеми реестрами пользователей, определенными в домене EIM (например, с информацией об идентификаторах пользователей) • Знакомство с инструментами администрирования EIM
Администратор конкретного реестра EIM	Управление конкретным определением реестра EIM: • Добавление и удаление целевых связей для конкретного реестра пользователей (например, реестра X) • Обновление определения конкретного реестра EIM	Необходимы следующие знания и навыки: • Знакомство с обслуживаемым реестром пользователей, определенным в домене EIM (например, с информацией об идентификаторах пользователей) • Знакомство с инструментами администрирования EIM
Администратор сервера каталогов (LDAP)	• Установка и настройка сервера каталогов (при необходимости) • Изменение конфигурации сервера каталогов для взаимодействия с EIM • Создание домена EIM (см. примечание) • Определение пользователей, имеющих доступ к контроллеру домена EIM • Необязательно: Определение первого администратора EIM **Примечание:** Администратор сервера каталогов может выполнять все операции, которые разрешены администратору EIM.	Необходимы следующие знания и навыки: • Установка и настройка сервера каталогов • Средства администрирования EIM

Таблица 10. Роли, задачи и навыки для настройки EIM (продолжение)

Роль	Задачи, к которым есть доступ	Необходимые навыки
Администратор реестра пользователей	• Настройка пользовательских профайлов или идентификаторов в конкретном реестре пользователей • Необязательно: Выполнение функций администратора обслуживаемого реестра пользователей EIM	Необходимы следующие знания и навыки: • Инструменты администрирования реестра пользователей • Средства администрирования EIM
Системный программист или системный администратор	Установка необходимых программных продуктов (может включать установку EIM)	Необходимы следующие знания и навыки: • Навыки системного программирования и администрирования • Знакомство с процедурами установки для применяемых платформ
Прикладной программист	Написание приложений, использующих API EIM	Необходимы следующие знания и навыки: • Знакомство с платформой • Навыки программирования • Навыки компиляции программ

Понятия, связанные с данным

“Управление доступом EIM” на стр. 39
Пользователь EIM - это пользователь, обладающий правами доступа EIM в соответствии с членством в предопределенных группах пользователей LDAP выбранного домена.

Планирование домена EIM

Одним из компонентов процесса первоначального планирования EIM является определение домена EIM. Для наиболее эффективной эксплуатации централизованного хранилища информации о соответствии идентификаторов необходимо составить план, позволяющий использовать этот домен множеству приложений и систем.

В процессе планирования EIM вы соберете информацию, необходимую для определения домена, и запишете ее в справочные таблицы планирования. Примеры справочных таблиц помогут вам собрать и записать всю необходимую на каждом этапе информацию в удобной форме.

В следующей таблице перечислена информация, которую необходимо собрать при планировании домена, а также дан ряд рекомендаций по распределении ролей в коллективе, осуществляющем реализацию EIM, или в коллективе сотрудников, отвечающих за различные области информации.

Примечание: Несмотря на то, что в таблице даны рекомендации по назначению ролей для сбора описанной информации, на самом деле роли следует распределять в соответствии с требованиями и стратегией защиты вашего предприятия. Например, в небольших организациях за все аспекты планирования, настройки и управления EIM может отвечать один человек, являющийся администратором EIM.

Таблица 11. Информация, необходимая для планирования домена EIM

Необходимая информация	Роль
1. Есть ли уже существующий домен, отвечающий вашим требованиям, или необходимо создать новый.	Администратор EIM

Таблица 11. Информация, необходимая для планирования домена EIM (продолжение)

Необходимая информация	Роль
2. Какой сервер каталогов будет выполнять роль контроллера домена EIM. (Подробная информация о выборе контроллера домена приведена в разделе “Планирование контроллера домена EIM”.)	Администратор сервера каталогов LDAP или администратор EIM
3. Имя домена. (Можно также указать необязательное описание.)	Администратор EIM
4. В каком месте каталога будут храниться данные домена EIM. **Примечание:** В зависимости от системы, выбранной для размещения сервера каталогов, а также в зависимости от каталога, применяемого для хранения данных домена EIM, перед созданием домена может потребоваться дополнительная настройка служб каталогов.	Администратор сервера каталогов LDAP и администратор EIM
5. Какие приложения и операционные системы будут входить в состав домена. При настройке первого домена это набор может включать в себя одну единственную систему. (Для получения более детальной информации обратитесь к разделу “Разработка плана присвоения имен определениям реестра EIM” на стр. 61.)	Коллектив реализации EIM
6. Какие пользователи и объекты будут входить в состав домена. **Примечание:** Для упрощения первоначального тестирования можно ограничить число пользователей одним или двумя.	Коллектив реализации EIM

Планирование контроллера домена EIM

В процессе сбора информации, определяющей конфигурацию домена EIM, вы должны решить, какой продукт сервера каталогов вы будете применять в качестве контроллера домена EIM.

EIM требует размещения контроллера домена на сервере каталогов, поддерживающем простой протокол доступа к каталогам (LDAP) версии 3. Кроме того, сервер каталогов должен поддерживать схему LDAP, отвечать другим требованиям EIM, а также поддерживать определенные атрибуты и классы объектов.

При наличии на предприятии нескольких серверов каталогов, каждый их которых может применяться в качестве контроллера домена EIM, вы также можете настроить дополнительные копии контроллера домена. Например, если вы ожидаете, что в сети будет выполняться множество операций поиска соответствий EIM, то создание копий позволит повысить производительность выполнения таких операций.

Кроме того, следует решить, будет ли контроллер домена *локальным* или *удаленным* по отношению к системе, которая будет выполнять наибольшее количество операций поиска соответствий. Разместив локальный контроллер домена в мощной системе, вы можете существенно повысить скорость выполнения поиска в этой системе. Запишите все принятые решения в справочных таблицах планирования.

После выбора сервера каталогов, который будет применяться в качестве контроллера домена EIM, вы должны будете принять ряд решений о доступе к контроллеру домена.

Планирование доступа к контроллеру домена

Вы должны составить план обращения администратора и приложений с поддержкой EIM к серверу каталогов, выполняющему роль контроллера домена EIM. Для обращения к домену EIM вы должны иметь возможность выполнять следующие операции:

1. Подключаться к контроллеру домена EIM

2. Включить ИД субъекта подключения в группу управления доступом EIM или сделать его администратором LDAP. Дополнительная информация приведена в разделе Управление доступом EIM.

Выберите тип привязки EIM

API EIM поддерживают различные механизмы подключения к контроллеру домена EIM. Каждый тип механизма подключения обеспечивает свой уровень идентификации и шифрования данных. Возможны следующие варианты:

Простое подключение
Простое подключение - это подключение к серверу LDAP, при котором клиент LDAP предоставляет серверу LDAP отличительное имя и пароль для идентификации. Отличительное имя и пароль определяются администратором LDAP в каталоге LDAP. Это наименее надежная форма идентификации, поскольку отличительное имя и пароль передаются по сети без шифрования и без защиты от перехвата. Для повышения уровня защиты паролей можно воспользоваться механизмом идентификации CRAM-MD5. При использовании протокола CRAM-MD5 клиент отправляет серверу для идентификации вместо текстового пароля хэшированное значение.

Идентификация сервера с помощью SSL - идентификация на сервере
На сервере LDAP можно настроить поддержку соединений с помощью защищенного протокола SSL или TLS. Сервер LDAP с помощью цифрового сертификата идентифицирует себя перед клиентом LDAP и устанавливает защищенный сеанс связи с клиентом. Сертификат применяется только для идентификации сервера LDAP. Идентификация конечного пользователя выполняется с помощью отличительного имени и пароля. Этот механизм идентификации обеспечивает те же возможности, что и простое подключение, но все данные, включая отличительное имя и пароль, передаются в зашифрованном виде.

Идентификация клиентов с помощью SSL
На сервере LDAP можно настроить идентификацию конечных пользователей, подключающихся к серверу с помощью SSL или TLS, посредством их цифровых сертификатов, применяемых в данном случае вместо отличительного имени и пароля. В этом случае выполняется идентификация клиента и сервера, а также обеспечивается шифрование всех данных сеанса. Этот вариант обеспечивает наиболее надежную идентификацию пользователей и гарантирует защиту всех передаваемых данных.

Идентификация Kerberos
Идентификация клиента LDAP на сервере может выполняться с помощью паспорта Kerberos, заменяющего в этом случае отличительное имя и пароль. Kerberos - это популярная и очень надежная система сетевой идентификации, позволяющая субъекту (пользователю или службе) подтвердить свои идентификационные данные при обращении к другой службе в незащищенной сети. Идентификация субъектов осуществляется с помощью централизованного сервера, называемого центром рассылки ключей (KDC). KDC идентифицирует пользователя с помощью паспорта Kerberos. Эти паспорта подтверждают сведения о субъекте при обращении к другим службам сети. После идентификации субъекта с помощью паспорта субъект и служба могут начать обмен зашифрованными данными. Этот вариант обеспечивает надежную идентификацию пользователей и гарантирует защиту идентификационных данных.

Выбор механизма подключения должен основываться на требованиях приложения EIM к уровню защиты, а также на наборе механизмов идентификации поддерживаемых сервером LDAP, выполняющим роль контроллера домена EIM.

Для включения на сервере LDAP поддержки выбранного механизма идентификации может потребоваться дополнительная настройка. Просмотрите документацию по серверу LDAP, выполняющему функции контроллера домена, и определите, нужно ли выполнять дополнительные задачи настройки.

Пример справочной таблицы планирования: Информация о контроллере домена

После принятия решений о контроллере домена EIM запишите в справочных таблицах планирования всю информацию о контроллере домена EIM, необходимую для операционных систем и приложений с поддержкой EIM. Собранная при этом информация позволит администратору LDAP создать идентификатор для подключения приложения или операционной системы к серверу каталогов LDAP, выполняющему роль контроллера домена EIM.

В следующем примере справочных таблиц планирования показана информация, которую вы должны собрать. Приведены также примеры значений, используемых при настройке контроллера домена EIM.

Таблица 12. Справочная таблица информации о домене и контроллере домена

Информация, необходимая для настройки домена EIM и контроллера домена	**Примеры ответов**
Описательное имя домена. Это может быть название компании, отдела или приложения, использующего этот домен.	`MyDomain`
Необязательно: При настройке домена EIM в уже существующем каталоге LDAP укажите родительское отличительное имя домена. Это отличительное имя записи, потомком которой в иерархии информации каталога является запись имени домена, например, `o=ibm,c=us`.	`o=ibm,c=us`
Полное отличительное имя домена EIM. Это полное имя домена EIM, описывающее размещение в каталоге данных домена EIM. Полное отличительное имя домена состоит, как минимум, из DN домена (`ibm-eimDomainName=`) и указанного вами имени домена. Если вы решили указать родительское DN домена, то полное имя домена DN будет включать относительное DN домена (`ibm-eimDomainName=`), имя домена (MyDomain) и родительское DN (`o=ibm,c=us`). **Примечание:**	Любое из следующих значений, в зависимости от выбранного родительского DN: • `ibm-eimDomainName=MyDomain` • `ibm-eimDomainName=MyDomain,o=ibm,c=us`
Адрес для подключения к контроллеру домена. Включает в себя тип соединения (обычное или защищенное соединение ldap, например, `ldap://` или `ldaps://`) плюс следующая информация:	`ldap://`
• Необязательно: Имя или IP-адрес хоста • Необязательно: Номер порта	• `some.ldap.host` • `389`
Полный адрес для подключения к контроллеру домена.	`ldap://some.ldap.host:389`
Способ подключения, который должен применяться приложениями или системами. Возможные варианты: • Простое подключение • CRAM MD5 • Идентификация сервера • Идентификация клиента • Kerberos	Kerberos

Если в состав группы настройки и администрирования EIM входит несколько сотрудников, то для каждого из них необходимо определить идентификатор и механизм, которые будут применяться этими сотрудниками для подключения к домену EIM в соответствии с их обязанностями. Кроме того, необходимо определить идентификатор и механизм для конечных пользователей приложений EIM. При сборе этой информации в качестве примера вы можете воспользоваться следующей справочной таблицей.

Таблица 13. Пример справочной таблицы планирования идентификаторов

Права доступа EIM или роль	Идентификатор для подключения	Способ подключения	Причина
Администратор EIM	eimadmin@krbrealm1.com	kerberos	Настройка и управление EIM
Администратор LDAP	cn=administrator	Простое подключение	Настройка контроллера домена EIM
Администратор конкретного реестра EIM	cn=admin2	CRAM MD5	Управление конкретным определением реестра
Поиск в EIM	cn=MyApp,c=US	Простое подключение	Выполнение операций поиска соответствий приложением

Разработка плана присвоения имен определениям реестра EIM

Для преобразования с помощью EIM идентификаторов пользователей из одного реестра в соответствующие идентификаторы из другого реестра оба этих реестра должны быть определены в EIM.

Определение реестра EIM необходимо создать для каждого реестра пользователей приложения или операционной системы, которые входят в состав домена EIM. Реестры пользователей могут представлять собой реестры операционных систем, такие как RACF, i5/OS, распределенные реестры типа Kerberos или фрагменты системных реестров, используемые исключительно приложениями.

В состав домена EIM могут входить определения реестров пользователей любых платформ. Например, домен, которым управляет контроллер домена i5/OS, может содержать определения реестров для других платформ (например, AIX). Несмотря на то, что в домене EIM можно определить любой реестр пользователей, следует создавать определения реестров пользователей только для тех приложений и операционных систем, которые поддерживают EIM.

Определению реестра EIM можно присвоить любое имя, уникальное в пределах домена EIM. Например, определению реестра EIM можно присвоить имя на основании имени системы, в которой размещается реестр пользователей. Если этого недостаточно для того, чтобы различать схожие определения реестров, то вы можете, например, добавить точку (.) или знак подчеркивания (_), а затем указать тип определяемого реестра пользователей. Независимо от применяемого способа обязательное следует разработать соглашение о присвоении имен определениям реестров EIM. Тем самым можно гарантировать согласованность имен определений в домене, адекватное описание типов и экземпляров реестров, а также способ применения каждого определенного реестра. Например, имя определения реестра может включать в себя сочетание имени операционной системы или приложения, использующего этот реестр, а также физическое размещение реестра на предприятии.

Приложение, созданное для работы с EIM, может указать псевдоним исходного реестра, псевдоним целевого реестра, либо оба псевдонима. При создании определений реестров EIM обязательно просмотрите документацию по приложению и выясните, нужно ли определять для идентификатора псевдонимы. Когда вы присваиваете псевдонимы соответствующим определениям реестров, приложение может выполнять поиск псевдонимов и находить определения реестров EIM, соответствующие псевдонимам в приложении.

Приведенный ниже пример справочной таблицы планирования поможет вам записать информацию о применяемых реестрах пользователей. В своей справочной таблице вы можете задать имя определения каждого реестра пользователей, указать, применяются ли в нем псевдонимы, а также описать размещение и способ применения этого реестра. Часть информации, которая должна указываться в справочной таблице, приведена в документации по установке и настройке приложения.

Таблица 14. Пример справочной таблицы планирования определения реестра EIM

Имя определения реестра	Тип реестра пользователей	Псевдоним определения реестра	Описание реестра
System_C	Системный реестр пользователей i5/OS	См. документацию по приложению	Главный реестр пользователей системы i5/OS C
System_A_WAS	WebSphere LTPA	app_23_alias_source	Реестр пользователей WebSphere LTPA в системе A
System_B	Linux	См. документацию по приложению	Реестр пользователей Linux в системе B
System_A	Системный реестр пользователей i5/OS	app_23_alias_target app_xx_alias_target	Главный реестр пользователей i5/OS системы A
System_D	Реестр пользователей Kerberos	app_xx_alias_source	Область Kerberos legal.mydomain.com
System_4	Реестр пользователей Windows 2000	См. документацию по приложению	Реестр пользователей приложения отдела кадров в системе 4

Примечание: Типы связей для каждого реестра будут определены на последующих этапах процедуры планирования.

После заполнения этого раздела справочной таблицы необходимо разработать план преобразования идентификаторов, указывающий, должны ли при определении соответствия между идентификаторами пользователей в определенных реестрах пользователей применяться связи идентификаторов, связи стратегий, или оба этих типа связей.

Разработка плана преобразования идентификаторов

Критически важным компонентом процесса первоначального планирования EIM является определения способа применения технологии преобразования идентификаторов на вашем предприятии.

Существует два способа применения преобразования идентификаторов в EIM:

- **Связи идентификаторов** описывают взаимосвязь между идентификаторами EIM и идентификаторами пользователей в различных реестрах. Связь идентификаторов задает прямое однозначное соответствие между идентификатором EIM и конкретным идентификатором пользователей. Связи идентификаторов можно применять для косвенного определения взаимосвязей между идентификаторами пользователей с помощью идентификаторов EIM.

  Если ваша стратегия защиты требует ведения подробных протоколов контроля, то связи идентификаторов могут применяться практически исключительно для реализации преобразования идентификаторов. Поскольку связи идентификаторов применяются для создания однозначного соответствия между принадлежащими пользователям идентификаторами, то вы всегда сможете определить, кто именно выполнил операцию над объектом или системой.
- **Связи стратегий** описывают взаимосвязь между несколькими идентификаторами пользователей и одним идентификатором пользователя в реестре пользователей. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM.

  Связи стратегий могут оказаться полезными в том случае, когда есть одна или несколько больших групп пользователей, которым необходим доступ к системам или приложениям предприятия в ситуации, когда применение отдельных идентификаторов пользователей для предоставления такого доступа нежелательно. Допустим, например, что вы поддерживаете Web-приложение, обращающееся к какому-либо определенному внутреннему приложению. Естественно, что вы не хотите настраивать несколько сотен или тысяч идентификаторов пользователей для этого внутреннего приложения. В таком случае можно настроить преобразование идентификаторов, связывающее всех пользователей этого

Web-приложения с одним идентификатором пользователя с минимальным уровнем доступа, необходимым для запуска приложения. Такой способ преобразования идентификаторов может применяться с помощью связей стратегий.

Вы можете воспользоваться связями идентификаторов для обеспечения наилучших условий управления идентификаторами пользователей на предприятии при сохранении простоты управления паролями. Вы также можете воспользоваться смесью связей стратегий и связей идентификаторов, что позволит применять единый вход в систему, где это возможно, а также сохранить возможность управления идентификаторами пользователей для администраторов. Независимо от того, какой тип преобразования идентификаторов по вашему мнению наилучшим образом отвечает требованиям предприятия и стратегии защиты, вам нужно будет создать план преобразования идентификаторов, гарантирующий правильную реализацию этой функции.

Для создания плана преобразования идентификаторов необходимо выполнить следующие действия:

Понятия, связанные с данным

“Создание связей EIM” на стр. 105
Существует два типа связей EIM, которые вы можете создавать. Вы можете создавать связь идентификаторов или связь стратегий.

“Создание связи стратегий” на стр. 106
Связь стратегий непосредственно определяет взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре.

Планирование связей EIM:

Связи - это записи, создаваемые в домене EIM и определяющие взаимосвязь между идентификаторами пользователей в разных реестрах пользователей.

В EIM можно создавать два типа связей: связи идентификаторов, определяющие однозначное соответствие, и связи стратегий, определяющие множественное соответствие, когда несколько записей преобразуются в одну. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

В каждом конкретном случае создаваемые типы связей определяются тем, как именно пользователь применяет тот или иной идентификатор, а также вашим общим планом соответствия идентификаторов.

Вы можете создавать любые из следующих типов связей идентификаторов:

- **Целевые связи**

  Целевые связи определяются для тех пользователей, которые обычно обращаются к данной системе с какой-либо другой клиентской системы как к серверу. Этот тип связей используется приложениями при поиске соответствий.
- **Исходные связи**

  Исходные связи определяются для идентификаторов, которые пользователь первоначально указывает для входа в систему или сеть. Этот тип связей используется приложениями при поиске соответствий.
- **Административные связи**

  Административные связи определяются в тех случаях, когда необходимо, чтобы была возможность отслеживать факт принадлежности идентификатора определенному пользователю, но сам этот идентификатор не должен возвращаться операциями поиска соответствия. Такой тип связей позволяет отслеживать все идентификаторы, применяемые каждым из сотрудников предприятия.

Связи стратегий всегда задают целевые связи.

В отдельном определении реестра может быть задано несколько связей различных типов, в зависимости от того, как применяется соответствующий реестр пользователей. Несмотря на то, что никаких формальных

ограничений на количество или сочетания связей не существует, для упрощения администрирования домена EIM рекомендуется поддерживать минимальное число связей.

Обычно в документации по приложению приводится информация о том, какие определения реестров это приложение использует в качестве исходных или целевых реестров, но тип связей не указывается. Для каждого конечного пользователя приложения должна быть задана по крайней мере одна связь. Это может быть однозначная связь между уникальным идентификатором EIM и идентификатором пользователя в требуемом целевом реестре, либо многозначная связь между исходным реестром, в котором зарегистрирован идентификатор пользователя и требуемым целевым реестром. Тип применяемых связей определяется требованиями преобразования идентификаторов и требованиями приложения.

Ранее, в ходе планирования, вы заполнили две справочные таблицы идентификаторов пользователей предприятия с информацией о требуемых идентификаторах EIM и определениях реестров EIM. Теперь эту информацию необходимо свести воедино, задав типы связей, которые должны применяться для установления соответствия между идентификаторами пользователей вашего предприятия. Вы должны решить, какой тип связи будете применять: связь стратегий для конкретного приложения и его реестра пользователей, или связи между отдельными идентификаторами (целевые, исходные и административные) пользователей системы или реестра приложения. Для этого вы можете указать требуемые типы связей и в таблице определения реестра и в соответствующих строках каждой таблицы связей.

Для завершения процедуры планирования связей идентификаторов вы можете воспользоваться следующим примером справочных таблиц. Эти примеры помогут вам указать информацию о связях, необходимую для получения полной картины планируемой схемы преобразования идентификаторов.

Таблица 15. Пример информации для справочной таблицы определения реестра EIM

Имя определения реестра	**Тип реестра пользователей**	**Псевдоним определения реестра**	**Описание реестра**	**Типы связей**
System_C	Системный реестр пользователей i5/OS	См. документацию по приложению	Главный реестр пользователей системы i5/OS C	Целевые связи
System_A_WAS	WebSphere LTPA	app_23_alias_source	Реестр пользователей WebSphere LTPA в системе A	Первоначальные исходные связи
System_B	Linux	См. документацию по приложению	Реестр пользователей Linux в системе B	Исходные и целевые связи
System_A	Системный реестр пользователей i5/OS	app_23_alias_target app_xx_alias_target	Главный реестр пользователей i5/OS системы A	Целевые связи
System_D	Реестр пользователей Kerberos	app_xx_alias_source	Область Kerberos legal.mydomain.com	Исходные связи
System_4	Реестр пользователей Windows 2000	См. документацию по приложению	Реестр пользователей приложения отдела кадров в системе 4	Административные связи
order.mydomain.com	Реестр пользователей Windows 2000		Основной реестр входа в систему для сотрудников отдела заказов	Стратегия реестра по умолчанию (исходный реестр)
System_A_order_app	Приложение отдела заказов		Реестр приложения для обновления заказов	Стратегия реестра по умолчанию (целевой реестр)
System_C_order_app	Приложение отдела заказов		Реестр приложения для обновления заказов	Стратегия реестра по умолчанию (целевой реестр)

Таблица 16. Пример справочной таблицы планирования идентификаторов EIM

Имя уникального идентификатора	Описание идентификатора пользователя	Псевдоним идентификатора
John S Day	Менеджер отдела кадров	app_23_admin
John J Day	Юридический отдел	app_xx_admin
Sharon A. Jones	Администратор отдела заказов	

Таблица 17. Пример справочной таблицы планирования связей идентификаторов

Уникальное имя идентификатора: _____John S Day_____		
Реестр пользователей	**Идентификатор пользователей**	**Типы связей**
WAS системы A в системе A	johnday	Исходные связи
Linux в системе B	jsd1	Исходные и целевые связи
i5/OS в системе C	JOHND	Целевые связи
Реестр 4 в системе Windows 2000 отдела кадров	JDAY	Административные связи

Таблица 18. Пример справочной таблицы планирования связей стратегий

Тип связей стратегий	Исходный реестр пользователей	Целевой реестр пользователей	Идентификатор пользователей	Описание
Реестр по умолчанию	order.mydomain.com	System_A_order_app	SYSUSERA	Преобразует ИД идентифицированных пользователей отдела заказов Windows в соответствующие ИД пользователей приложения
Реестр по умолчанию	order.mydomain.com	System_C_order_app	SYSUSERB	Преобразует ИД идентифицированных пользователей отдела заказов Windows в соответствующие ИД пользователей приложения

Разработка плана присвоения имен идентификаторам EIM:

При планировании соответствия идентификаторов EIM вы можете создать уникальные идентификаторы EIM для пользователей приложений с поддержкой EIM и операционных систем вашего предприятия, что позволит создать однозначное соответствие между идентификаторами каждого пользователя. Путем организации соответствия идентификаторов и создания однозначных соответствий вы можете наиболее эффективно использовать предлагаемые EIM возможности управления паролями.

Разрабатываемый план присвоения имен будет зависеть от требований предприятия и ваших предпочтений; единственным обязательным условием при создании идентификаторов EIM является их уникальность. Некоторые организации предпочитают использовать полные официальные имена сотрудников; другие могут использовать иные типы данных, например, личные идентификационные номера сотрудников. Если вы хотите создавать имена идентификаторов EIM на основе традиционных полных имен, то необходимо учесть возможность совпадения имен. Способ обработки таких совпадений определяется только вашими предпочтениями. Вы можете, например, исправлять каждое совпадение вручную, добавляя к каждому идентификатору определенную строку для обеспечения его уникальности, например, можно добавлять номер отдела, в котором работает данный сотрудник.

В ходе разработки плана присвоения имен идентификаторам EIM вы должны выбрать общий план соответствия идентификаторов. Это поможет вам выбрать случаи, когда на предприятии для преобразования идентификаторов следует применять идентификаторы и их связи, а когда - связи стратегий. Для разработки плана присвоения имен идентификаторам EIM вы можете воспользоваться приведенной ниже справочной таблицей. Она поможет вам собрать информацию об идентификаторах пользователей вашей организации и выработать план присвоения идентификаторов EIM всем пользователям. Справочная таблица содержит информацию, которую администратор EIM должен учитывать при создании идентификаторов EIM или связей стратегий для пользователей приложений.

Таблица 19. Пример справочной таблицы планирования идентификаторов EIM

Имя уникального идентификатора	**Описание идентификатора пользователя**	**Псевдоним идентификатора**
John S Day	Менеджер отдела кадров	app_23_admin
John J Day	Юридический отдел	app_xx_admin
Sharon A. Jones	Администратор отдела заказов	

Приложение, созданное для работы с EIM, может указать псевдоним, позволяющий найти идентификатор EIM для этого приложения. По этому идентификатору EIM приложение в свою очередь сможет определить требуемый идентификатор пользователя. Просмотрите документацию по приложению и выясните, нужно ли определять для идентификатора псевдонимы. Идентификатор EIM или поля описания идентификатора пользователя задаются в свободной форме и могут содержать сведения, описывающие пользователя.

Совсем необязательно создавать идентификаторы EIM сразу для всех сотрудников предприятия. После создания первоначального идентификатора EIM и тестирования конфигурации EIM вы сможете создать дополнительные идентификаторы EIM в соответствии с целями, поставленными в вашей организации для применения EIM. Например, идентификаторы EIM могут добавляться по организационному или по территориальному принципу. Идентификаторы EIM могут также добавляться при развертывании новых приложений EIM.

После сбора информации, необходимой для разработки плана присвоения имен идентификаторам EIM вы можете составить план соответствия идентификаторов пользователей.

Справочная таблица по планированию реализации EIM

Следующие таблицы могут оказаться полезными в процессе планирования EIM для сбора информации, необходимой для настройки и применения EIM на вашем предприятии. Где это возможно, приведены также примеры заполненных разделов справочных таблиц.

Эти таблицы представляют собой примеры различных типов справочных таблиц, необходимых при создании плана реализации EIM. Число записей в них обычно меньше, чем реально необходимо информации о EIM. Вы можете видоизменить эти таблицы в соответствии со своей ситуацией.

Таблица 20. Справочная таблица информации о домене и контроллере домена

Информация, необходимая для настройки домена EIM и контроллера домена	**Ответы**
Описательное имя домена. Это может быть название компании, отдела или приложения, использующего этот домен.	
Необязательно: Родительское отличительное имя домена. Это отличительное имя записи, потомком которой в иерархии информации каталога является запись имени домена, например, `o=ibm,c=us`.	

Таблица 20. Справочная таблица информации о домене и контроллере домена (продолжение)

Полное отличительное имя домена EIM. Это полное имя домена EIM, описывающее размещение в каталоге данных домена EIM. Полное отличительное имя домена состоит, как минимум, из DN домена (`ibm-eimDomainName=`) и указанного вами имени домена. Если вы решили указать родительское DN домена, то полное имя домена DN будет включать относительное DN домена (`ibm-eimDomainName=`), имя домена (MyDomain) и родительское DN (`o=ibm,c=us`).	
Адрес для подключения к контроллеру домена. Включает в себя тип соединения (обычное или защищенное соединение ldap, например, `ldap://` или `ldaps://`) плюс следующая информация:	
• Необязательно: Имя или IP-адрес хоста • Необязательно: Номер порта	
Полный адрес для подключения к контроллеру домена.	
Способ подключения, который должен применяться приложениями или системами. Возможные варианты: • Простое подключение • CRAM MD5 • Идентификация сервера • Идентификация клиента • Kerberos	

Пример применения этой таблицы приведен в разделе Планирование контроллера домена EIM.

Таблица 21. Справочная таблица идентификаторов подключения

Права доступа EIM или роль	**Идентификатор для подключения**	**Способ подключения**	**Причина**

Пример применения этой таблицы приведен в разделе Планирование контроллера домена EIM.

Таблица 22. Справочная таблица планирования информации определения реестра EIM

Имя определения реестра	**Тип реестра пользователей**	**Псевдоним определения реестра**	**Описание реестра**	**Тип связей**

Таблица 22. Справочная таблица планирования информации определения реестра EIM (продолжение)

Пример применения этой таблицы приведен в разделе Разработка плана присвоения имен определениям реестра EIM.

Таблица 23. Справочная таблица планирования идентификаторов EIM

Имя уникального идентификатора	**Описание идентификатора пользователя**	**Псевдоним идентификатора**

Пример применения этой таблицы приведен в разделе Разработка плана присвоения имен идентификаторам EIM.

Таблица 24. Справочная таблица планирования связей идентификаторов

Уникальное имя идентификатора: _____John S Day_____		
Реестр пользователей	Идентификатор пользователей	Типы связей

Пример применения этой таблицы приведен в разделе План связей EIM.

Таблица 25. Справочная таблица планирования связей стратегий

Тип связей стратегий	Исходный реестр пользователей	Целевой реестр пользователей	Идентификатор пользователей	Описание

Пример применения этой таблицы приведен в разделе План связей EIM.

План разработки приложений EIM

Для того чтобы приложение могло применять технологию EIM и входить в состав домена, это приложение должно иметь возможность использоваться API EIM.

Обязательно просмотрите документацию по EIM API, а также документацию, относящуюся к реализации EIM на вашей конкретной платформе и выясните, нет ли каких-либо особенностей планирования, которые нужно учитывать при создании или переработке приложений для применения API EIM. Например, могут быть оговорены какие-либо особенности компиляции приложений C и C++, использующих API EIM. В зависимости от платформы приложения, могут также действовать другие ограничения и особенности.

Задачи, связанные с данной

“API EIM” на стр. 129
Технология EIM предоставляет механизмы кросс-платформенного управления идентификаторами пользователей. Существует несколько интерфейсов прикладных программ (API) EIM, с помощью которых приложения могут выполнять операции EIM от своего имени или от имени пользователя приложения.

Планирование EIM для i5/OS

Технология EIM объединяет большое количество функций и служб на платформе System i platform. Перед началом настройки EIM на сервере рекомендуется определить, какие возможности EIM и единого входа в систему нужны в вашей среде.

Сначала нужно определить общие требования к защите сети и настроить соответствующие средства защиты. Технология EIM в значительной степени упрощает идентификацию пользователей в рамках предприятия. Совместно со службой сетевой идентификации технология EIM позволяет организовать единую среду входа в сеть в масштабах всей организации.

Если в среде с единым входом в систему для идентификации пользователей вы планируете применять протокол Kerberos, то потребуется установить службу сетевой идентификации.

Дополнительная информация о планировании конфигурации EIM приведена в следующих разделах:

Информация, связанная с данной

Планирование службы сетевой идентификации

Предварительные требования для установки EIM в i5/OS

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

Таблица 26. Справочная таблица планирования установки EIM

Справочная таблица планирования предварительных требований EIM	**Ответы**
Установлена ли в системе операционная система i5/OS V5R4 или более поздняя версия?	

Таблица 26. Справочная таблица планирования установки EIM (продолжение)

Установлены ли в вашей системе следующие компоненты и лицензионные продукты? • i5/OS Host Servers (5761-SS1, компонент 12) • System i Access for Windows (5761-XE1) • Qshell Interpreter (5761-SS1, компонент 30) Необходим в том случае, если вместе с EIM вы планируете настроить службу сетевой идентификации. **Примечание:** 5722 - это код компонентов и продуктов версий i5/OS, предшествующих V6R1.	
Установлен ли на PC администратора System i Navigator со следующими компонентами? • Сеть • Защита (необходим в том случае, если вместе с EIM вы планируете настроить службу сетевой идентификации	
Установили ли вы последний пакет обслуживания System i Access for Windows? Сведения о последнем пакете обслуживания приведены на Web-сайте System i Access	
Если сервер каталогов, например, Сервер каталогов IBM Tivoli для i5/OS настроен и вы планируете применять его в качестве контроллера EIM, то знаете ли вы отличительное имя (DN) и пароль администратора LDAP?	
Если сервер каталогов в настоящее время настроен, то 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?	

Компоненты System i Navigator, требующие установки

Для настройки среды единого входа в систему с помощью EIM и службы сетевой идентификации необходимо установить такие компоненты System i Navigator, как **Сеть** и **Защита**.

EIM входит в состав компонента **Сеть**, а служба сетевой идентификации - в состав компонента **Защита**. Если вы не планируете применять службу сетевой идентификации, то устанавливать компонент **Защита** в System i Navigator не нужно.

Для того чтобы установить компонент Сеть продукта System i Navigator или проверить его наличие, убедитесь в том, что продукт System i Access for Windows установлен на PC, применяемом для управления моделью System i.

Для установки компонента **Сеть** выполните следующие действия:

1. Нажмите на кнопку **Пуск > Программы > System i Access for Windows > Выборочная настройка**.
2. Следуйте инструкциям, приведенным в окне. В окне **Выбор компонентов** разверните значок **System i Navigator** и выберите компонент **Сеть**. Для применения службы сетевой идентификации дополнительно требуется установить компонент **Защита**.
3. Выполните все остальные этапы **Выборочной установки**.

Информация, связанная с данной

Служба сетевой идентификации

Особенности резервного копирования и восстановления при использовании EIM

Для того чтобы обеспечить надежную защиту и возможность восстановления данных EIM на случай сбоя сервера каталогов, на котором находится контроллер домена EIM, необходимо разработать план резервного копирования и восстановления данных EIM. Кроме того, следует обязательно познакомиться со способами восстановления важной информации о конфигурации EIM.

Информация, связанная с данной

Копирование сервера каталогов

Задачи копирования

Замечания по сохранению и восстановлению сервера каталогов

Резервное копирование и восстановление данных домена EIM:

Способ сохранения данных EIM зависит от того, как вы решили управлять этим аспектом работы сервера каталогов, выполняющего функции контроллера домена для данных EIM.

Одним из способов резервного копирования данных, особенно удобным для восстановления в случае серьезной аварии, является сохранение библиотеки базы данных. По умолчанию это библиотека QUSRDIRDB. Если включена поддержка протокола изменений (changelog), то следует также сохранять библиотеку QUSRDIRCL. Сервер каталогов в системе, в которой вы планируете восстановить библиотеку, должен применять ту же конфигурацию и схему LDAP, что и исходный сервер каталогов. Эта информация хранится в файлах /QIBM/UserData/OS400/DirSrv. Дополнительные сведения о конфигурации хранятся в библиотеке QUSRSYS/QGLDCFG (объект *USRSPC) и в QUSRSYS/QGLDVLDL (объект *VLDL). Для получения полной резервной копии всех объектов сервера каталогов необходимо сохранить обе библиотеки, файлы интегрированной файловой системы, а также объекты QUSRSYS.

Например, для полного или частичного сохранения содержимого сервера каталогов можно воспользоваться файлом LDIF. Для сохранения информации о домене для контроллера домена Сервер каталогов IBM Tivoli для i5/OS выполните следующие действия:

1. В System i Navigator разверните **Сеть > Серверы > TCP/IP**.
2. Щелкните правой кнопкой мыши на значке **Сервер каталогов**, выберите опцию **Инструменты**, а затем - **Экспортировать файл**. Будет показано окно, в котором вы сможете указать, какую часть информации сервера каталогов необходимо экспортировать в файл.
3. Передайте экспортированный файл на платформу System i, которая будет применяться в качестве резервного сервера каталогов.
4. В System i Navigator на резервном сервере разверните **Сеть > Серверы > TCP/IP**.
5. Щелкните правой кнопкой мыши на значке **Сервер каталогов** выберите опцию **Инструменты**, а затем - опцию **Импорт** для загрузки содержимого полученного файла на новый сервер каталогов.

Еще один способ сохранения данных домена EIM заключается в настройке и применении копии сервера каталогов. Все изменения, вносимые в данные домена EIM, будут автоматически передаваться серверу-копии, поэтому в случае сбоя сервера каталогов, на котором находится контроллер домена, или в случае потери данных EIM вы сможете получить данные с сервера-копии.

Способ настройки и применения сервера-копии зависит от выбранной модели копирования.

Резервное копирование и восстановление информации о конфигурации EIM:

В случае сбоя системы вам может потребоваться восстановить информацию о конфигурации EIM этой системы. Такую информацию нельзя сохранять и восстанавливать в разных системах.

Существуют следующие способы сохранения и восстановления конфигурации EIM:

- Сохраните EIM и другую важную информацию о конфигурации в каждой системе с помощью команды Сохранить данные защиты (SAVSECDTA). После восстановите в каждой системе объект пользовательского профайла QSYS.

  Примечание: Запускать команду SAVSECDTA и восстанавливать объект пользовательского профайла QSYS необходимо отдельно в каждой системе с конфигурацией EIM. В случае, если вы сохраните объект пользовательского профайла QSYS в одной системе, а затем попытаетесь восстановить его в другой системе, могут возникнуть ошибки.

- Запустите мастер настройки EIM или вручную обновите свойства папки конфигурации EIM. Для упрощения этой процедуры следует сохранять рабочие таблицы планирования реализации EIM или записывать информацию о конфигурации EIM в каждой системе.

Кроме того, в случае, если при реализации среды единого входа в систему вы настроили службу сетевой идентификации, необходимо составить план резервного копирования и восстановления данных этой службы.

Настройка преобразований идентификаторов в рамках предприятия

Мастер настройки EIM позволяет быстро и легко выполнить базовую настройку EIM в вашей системе. Мастер предлагает три способа настройки EIM.

Способ применения мастера настройки EIM в конкретной системе зависит от ваших общих планов по применению EIM на предприятии и от требований, предъявляемых в вашей среде EIM. Например, многие администраторы используют EIM вместе со службой сетевой идентификации для создания среды с единым входом в систему, позволяющей использовать множество различных систем и платформ, не изменяя базовые стратегии защиты. В связи с этим мастер настройки EIM позволяет в процессе настройки EIM настроить также службы сетевой идентификации. Однако настройка службы сетевой идентификации не является предварительным требованием для настройки и применения EIM.

Перед началом настройки EIM в одной или в нескольких системах составьте план реализации EIM и соберите всю требуемую информацию. Например, вам потребуется принять следующие решения:

- Какую платформу System i необходимо настроить в качестве контроллера домена EIM? С помощью мастера настройки EIM сначала создайте в этой системе новый домен, а затем настройте все дополнительные системы.
- Будете ли вы настраивать службы сетевой идентификации в каждой системе, в которой настроена поддержка EIM? Если это так, то с помощью мастера настройки EIM вы сможете создать базовую конфигурацию служб сетевой идентификации в каждой модели System i. Однако для завершения настройки служб сетевой идентификации вам потребуется выполнить ряд дополнительных задач.

После создания с помощью мастера EIM базовой конфигурации на каждой платформе System i вам нужно будет выполнить ряд дополнительных задач настройки EIM, без выполнения которых конфигурация EIM будет неполной. Пример настройки среды единого входа в сеть в вымышленной компании с помощью службы сетевой идентификации и EIM приведен в разделе Сценарий: Настройка единого входа в систему.

Для настройки EIM необходимы следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)
- Права доступа на настройку системы (*IOSYSCFG)

Перед началом работы с мастером настройки EIM необходимо завершить все шаги планирования “Планирование EIM” на стр. 53 и определить, как именно будет применяться EIM. Если вы настраиваете EIM в ходе создания среды с единым входом в систему, то вам потребуется также выполнить все шаги планирования среды с единым входом в систему.

Для запуска мастера настройки EIM выполните следующие действия:

1. Запустите System i Navigator.
2. Войдите в систему, на которой необходимо настроить EIM. Если EIM нужно настроить в нескольких системах, начните с системы, в которой будет настроен контроллер домена EIM.
3. Разверните узлы **Сеть → EIM**.
4. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите опцию **Настроить**, чтобы запустить мастер настройки EIM.

5. Выберите вариант конфигурации EIM и следуйте инструкциям мастера.
6. Описание информации, указываемой в каждом поле мастера, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.

После завершения планирования вы сможете создать с помощью мастера EIM одну из трех базовых конфигураций EIM. Например, вы можете воспользоваться мастером для включения системы в уже существующий домен или для создания нового домена и включения системы в ее состав. Если вы создаете новый домен и добавляете в него систему с помощью мастера EIM, то в ходе создания конфигурации EIM вы можете также создать контроллер домена EIM в локальной или в удаленной системе. Ниже приведены инструкции по настройке EIM в зависимости от требуемой базовой конфигурации:

Информация, связанная с данной

Служба сетевой идентификации

Единый вход в систему

Создание нового локального домена и добавление системы в него

Если вы создаете новый домен и добавляете в него систему с помощью мастера настройки EIM, то в ходе создания конфигурации EIM вы можете также создать в локальной системе контроллер домена EIM.

При необходимости мастер настройки EIM предлагает пользователю задать базовую конфигурацию сервера каталогов. Кроме того, если на платформе System i не настроены функции Kerberos, то мастер предлагает запустить мастер настройки службы сетевой идентификации.

Работая с мастером настройки EIM, вы можете выполнить следующие задачи:

- Создание нового домена EIM
- Настройка локального сервера каталогов в качестве контроллера домена EIM
- Настройка службы сетевой идентификации для системы
- Создание определений реестра EIM для локального реестра i5/OS и реестра Kerberos.
- Настройка системы для работы в новом домене EIM

Для создания нового домена EIM и включения системы в его состав необходимы следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)
- Права доступа на настройку системы (*IOSYSCFG)

Для того чтобы запустить мастер настройки EIM, создать с его помощью новый домен EIM и добавить систему в этот домен, выполните следующие действия:

1. В System i Navigator выберите систему, в которой настроены EIM, и разверните пункты **Сеть > Преобразование идентификаторов в рамках предприятия**.
2. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите **Настроить**, чтобы запустить мастер настройки EIM.

   Примечание: Если EIM уже был настроен в данной системе, то эта опция называется **Изменить настройку**.
3. На странице мастера **Приветствие** выберите **Создать и добавить в новый домен**, после чего нажмите **Далее**.
4. На странице **Задать расположение домена EIM** выберите опцию **На локальном сервере каталогов** и нажмите кнопку **Далее**.

Примечание: Эта опция позволяет настроить локальный сервер каталогов в качестве контроллера домена EIM. Поскольку на этом сервере каталогов хранятся все данные EIM для домена, то он для поддержки операций поиска соответствий EIM и других операций он должен быть активен.

Если служба сетевой идентификации на платформе System i не настроена или для настройки среды с единым входом в систему необходима дополнительная настройка этой службы, то будет показана страница **Настройка служб сетевой идентификации**. С помощью этой страницы вы можете запустить мастера и настроить службу сетевой идентификации. Вы также можете выполнить эту настройку позже, запустив мастера с помощью System i Navigator. По завершении настройки службы сетевой идентификации продолжит работу мастер настройки EIM.

5. Для настройки службы сетевой идентификации выполните следующие действия:
   a. На странице **Настройка служб сетевой идентификации** выберите опцию **Да** для запуска мастера настройки служб сетевой идентификации. С помощью этого мастера вы можете настроить несколько служб и интерфейсов i5/OS для работы в составе области Kerberos, а также настроить среду единого входа в систему, в которой применяется как EIM, так и служба сетевой идентификации.
   b. На странице **Задать информацию об области** укажите в поле **Область по умолчанию** имя области по умолчанию. Если для идентификации Kerberos вы применяете Microsoft Active Directory, то выберите опцию **Применять Microsoft Active Directory для идентификации Kerberos** и нажмите кнопку **Далее**.
   c. На странице **Указать информацию о KDC** укажите в поле **KDC** полное имя сервера Kerberos для данной области, в поле **Порт** укажите значение 88 и нажмите кнопку **Далее**.
   d. На странице **Указать информацию о сервере паролей** выберите опцию **Да** или **Нет** для настройки сервера паролей. Сервер паролей позволяет субъектам изменять свои пароли на сервере Kerberos. При выборе ответа **Да** укажите в поле **Сервер паролей** имя сервера паролей. В поле **Порт** оставьте значение по умолчанию 464 и нажмите кнопку Далее.
   e. На странице **Выбрать записи файла ключей** выберите опцию **Идентификация Kerberos i5/OS** и нажмите кнопку **Далее**.

      Примечание: Если вы хотите, чтобы соответствующие службы также применяли идентификацию Kerberos, то можете также создать записи файла ключей для сервера каталогов IBM Tivoli для i5/OS, i5/OS NetServer и IBM HTTP Server for i5/OS. Для применения этими службами идентификации Kerberos может потребоваться их дополнительная настройка.

   f. На странице **Создать запись файла ключей i5/OS** введите и подтвердите пароль, а затем нажмите кнопку **Далее**. Этот тот же пароль, который вы будете применять при добавлении субъектов i5/OS на сервер Kerberos.
   g. Необязательно: На странице **Создать пакетный файл** выберите ответ **Да**, укажите следующую информацию и нажмите кнопку **Далее**:
      - В поле **Пакетный файл** укажите требуемый каталог. Вы можете нажать кнопку **Обзор** и найти требуемый каталог, либо вручную указать нужное значение в поле **Пакетный файл**.
      - В поле **Включить пароль** выберите ответ **Да**. Тем самым вы гарантируете включение в пакетный файл всех паролей, связанных с субъектами служб i5/OS. Следует помнить, что пароли отображаются в текстовом формате и их может просмотреть любой пользователь, имеющий права доступа на чтение пакетного файла. Таким образом, пакетный файл необходимо удалить с сервера Kerberos и с PC сразу же после использования. Если вы не включите пароли, то при запуске пакетного файла вам будет предложено указать пароль.

        Примечание: Вы также можете вручную добавить созданных мастером субъектов служб в каталог Microsoft Active Directory. Необходимые инструкции приведены в разделе Добавление субъектов i5/OS на сервер Kerberos

      - На странице обзорной информации просмотрите сведения о конфигурации службы сетевой идентификации и нажмите кнопку **Готово** для возврата к мастеру настройки EIM.

6. Если локальный сервер каталогов еще не настроен, то после возобновления работы мастера настройки EIM появится страница **Настроить сервер каталогов**. Для настройки локального сервера каталогов укажите следующую информацию:

   Примечание: Если вы настроили локальный сервер каталогов до запуска мастера настройки EIM, то появится страница **Укажите пользователя для подключения**. Эта страница позволяет указать отличительное имя и пароль администратора LDAP, предоставляющие мастеру права доступа, достаточные для администрирования домена EIM и настройки различных объектов, что необходимо для успешного выполнения последующих шагов данной процедуры. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.

   a. В поле **Порт** оставьте номер порта по умолчанию 389 или введите другой номер порта для незащищенного обмена данными EIM с сервером каталогов.

   b. В поле **Отличительное имя** укажите отличительное имя администратора сервера каталогов. Мастер настройки EIM создает это DN администратора LDAP и применяет его для настройки сервера каталогов, выполняющего функции контроллера создаваемого домена.

   c. В поле **Пароль** введите пароль администратора LDAP.

   d. В поле **Подтверждение пароля** введите этот пароль еще раз.

   e. Нажмите кнопку **Далее**.

7. На странице **Укажите домен** введите следующие данные:

   a. В поле **Домен** укажите имя создаваемого домена EIM. Оставьте имя EIM, указанное по умолчанию, или введите другое имя. Имя не должно содержать такие специальные символы, как **= + < > , # ;** \ и *****.

   b. В поле **Описание** введите описание этого домена.

   c. Нажмите кнопку **Далее**.

8. На странице **Указать родительское DN домена** выберите опцию **Да** для указания родительского DN создаваемого домена или опцию **Нет** для сохранения данных EIM в поддереве сервера каталогов, суффикс которого определяется именем домена EIM.

   Примечание: При создании домена в локальном сервере каталогов родительское DN указывать не обязательно. С помощью родительского DN можно указать расположение данных EIM домена в локальном пространстве имен LDAP. Если родительское DN указано не будет, то данные EIM будут храниться в отдельном суффиксе. Для того чтобы задать родительское DN, выберите в списке локальный суффикс LDAP или введите текст для создания другого родительского DN. Указывать родительское DN для создаваемого домена не обязательно. Для просмотра дополнительной информации о родительском DN нажмите кнопку **Справка**.

9. На странице **Информация о реестре** укажите, следует ли добавлять локальные реестры пользователей в домен EIM в качестве определений реестров. Можно выбрать один из указанных ниже типов реестров пользователей или оба типа:

   Примечание: Сейчас создавать определения реестров не нужно. Если в дальнейшем вы решите создать определения реестров, то вам нужно будет добавить определения системных реестров и обновить свойства конфигурации EIM.

   a. Для добавления определения локального реестра выберите опцию **Локальный реестр i5/OS**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя реестра EIM - произвольная строка, задающая тип реестра и отдельный экземпляр этого реестра.

   b. Для добавления определения реестра Kerberos выберите опцию **Kerberos**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя определения реестра по умолчанию совпадает с именем области. Оставив значение по умолчанию и воспользовавшись именем реестра Kerberos, совпадающим с именем области, вы можете повысить производительность получения информации из реестра. При необходимости выберите опцию **Идентификаторы пользователей Kerberos с учетом регистра символов**.

c. Нажмите кнопку **Далее**.

10. На странице **Указать системного пользователя для EIM** выберите тип пользователя, с помощью которого система будет выполнять операции EIM от имени функций операционной системы. Эти операции включают поиск соответствий и удаление связей при удалении локального пользовательского профайла i5/OS. Предусмотрены следующие типы пользователей: **Отличительное имя и пароль**, **Файл ключей и субъект Kerberos** или **Субъект и пароль Kerberos**. Список доступных типов пользователя зависит от конфигурации текущей системы. Например, если в системе не настроена служба сетевой идентификации, то вы не сможете выбрать тип пользователя Kerberos. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях:

    Примечание: Вы должны указать пользователя, определенного на сервере каталогов, выполняющем функции контроллера домена EIM. Указанному пользователю должны быть предоставлены права на поиск соответствий и на управление реестрами локальных пользователей. Если указанный пользователь не имеет этих прав, определенные функции операционной системы, связанные с единым входом в систему и удалением пользовательских профайлов могут не выполняться.

    Если перед запуском этого мастера вы не настроили сервер каталогов, то единственным доступным типом пользователя будет **Отличительное имя и пароль**, а в качестве значения можно будет указать только DN администратора LDAP.

    - Если была выбрана опция **Отличительное имя и пароль**, то введите следующие данные:
      - В поле **Отличительное имя** укажите отличительное имя LDAP, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
      - В поле **Пароль** введите пароль, соответствующий заданному отличительному имени.
      - В поле **Подтверждение пароля** введите этот пароль еще раз.
    - Если была выбрана опция **Субъект Kerberos и пароль**, то введите следующие данные:
      - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
      - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
      - В поле **Пароль** введите пароль пользователя.
      - В поле **Подтверждение пароля** введите этот пароль еще раз.
    - Если была выбрана опция **Файл ключей и субъект Kerberos**, то введите следующие данные:
      - В поле **Файл ключей** укажите полное имя файла ключей, содержащего сведения о субъекте Kerberos, который должен применяться системой при выполнении операций EIM. Вы также можете нажать кнопку **Обзор** и выбрать требуемый файл в структуре каталогов интегрированной файловой системы System i.
      - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
      - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
    - Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации о пользователе мастер может успешно подключиться к контроллеру домена EIM.
    - Нажмите кнопку **Далее**.

11. На странице сводной информации проверьте правильность указанной информации о конфигурации. Если все данные указаны верно, нажмите кнопку **Готово**.

Завершение конфигурации EIM для домена

После завершения работы мастер добавит новый домен в папку **Управление доменами** и создаст для данного сервера базовую конфигурацию EIM. Для завершения настройки EIM в домене необходимо выполнить следующие задачи:

1. Запустить мастера настройки EIM на каждом дополнительном сервере, который вы планируете включить в состав домена.
2. Добавить в домен EIM определения реестров EIM для других платформ и приложений, которые также будут входить в домен EIM. Эти определения реестров соответствуют реальным реестрам пользователей, которые также должны применяться в домене. В зависимости от предъявляемых требований вы можете Добавить определения системных реестров или Добавить определения реестров приложений.
3. В зависимости от требований конфигурации EIM выберите один из следующих вариантов:
   - Создать идентификаторы EIM для каждого уникального пользователя или объекта в домене, а затем создать для них связи идентификаторов.
   - Создать связи стратегий, задающие соответствие между группой пользователей и одним целевым идентификатором пользователя.
   - Воспользоваться сочетанием перечисленных опций.
4. С помощью функции проверки преобразования проверьте правильность преобразования идентификаторов в среде EIM.
5. Если в настоящее время в EIM определен только DN администратора LDAP, то у этого пользователя EIM есть очень высокий уровень доступа ко всем данным сервера каталогов. Рекомендуется создать несколько дополнительных DN пользователей с более адекватным и более ограниченным набором прав доступа к данным EIM. Дополнительная информация о создании DN сервера каталогов приведена в разделе Отличительные имена в главе i5/OS Information Center. Число создаваемых дополнительных пользователей EIM зависит от того, насколько тонко в применяемой стратегии защиты разделяются права доступа и обязанности пользователей. Обычно бывает необходимо создать по крайней мере два типа DN:
   - **Пользователь с правами доступа администратора EIM**

     DN администратора EIM обеспечивает необходимый уровень доступа для администратора, ответственного за управление доменом EIM. Этот DN администратора EIM может применяться для подключения к контроллеру домена EIM для управления всеми аспектами его работы с помощью System i Navigator.
   - **По крайней мере один пользователь, имеющий все права доступа из следующего набора:**
     - Администратор идентификаторов
     - Администратор реестра
     - Поиск соответствий EIM

     Этот пользователь имеет права доступа, необходимые для системного пользователя, выполняющего операции EIM от имени операционной системы.

     Примечание: Для применения в качестве системного пользователя этого нового DN вместо DN администратора LDAP необходимо изменить свойства конфигурации EIM для платформы System i platform. Изменение DN системного пользователя описано в разделе Управление свойствами конфигурации EIM.

Кроме того, вы можете настроить защиту подключения к контроллеру домена EIM с помощью протокола SSL или TLS. Если вы включили поддержку SSL для сервера каталогов, то необходимо обновить свойства конфигурации EIM, указав, что платформа System i применяет защищенные соединения SSL. При этом необходимо также обновить свойства домена, указав, что в EIM для управления доменом с помощью System i Navigator применяются соединения SSL.

Примечание: Если вы создали базовую конфигурацию службы сетевой идентификации, то может потребоваться дополнительная настройка, особенно в том случае, если вы реализуете среду с

единым входом в систему. Необходимую информацию вы можете найти в полном описании инструкций по настройке в разделе Включение поддержки единого входа в систему в i5/OS.

Создание нового удаленного домена и добавление системы в него

Если вы создаете новый домен и добавляете в него систему с помощью мастера настройки EIM, то в ходе создания конфигурации EIM вы можете также создать в удаленной системе сервер каталогов, выполняющий функции контроллера домена EIM.

Для настройки EIM вам потребуется указать информацию, необходимую для подключения к удаленному серверу каталогов. Кроме того, если на платформе System i не настроена поддержка Kerberos, то вам будет предложено запустить мастер настройки службы сетевой идентификации.

Примечание: Сервер каталогов в удаленной системе должен обеспечивать поддержку EIM. EIM требует размещения контроллера домена на сервере каталогов, поддерживающем простой протокол доступа к каталогам (LDAP) версии 3. Кроме того, сервер каталогов должен поддерживать применяемую схему EIM. Такая поддержка обеспечивается, например, продуктом IBM Directory Server V5.1. Более подробная информация о требованиях к контроллеру домена EIM приведена в разделе “Планирование контроллера домена EIM” на стр. 58.

Работая с мастером настройки EIM, вы можете выполнить следующие задачи:

- Создание нового домена EIM
- Настройка удаленного сервера каталогов в качестве контроллера домена EIM
- Настройка службы сетевой идентификации для системы
- Создание определений реестра EIM для локального реестра i5/OS и реестра Kerberos.
- Настройка системы для работы в новом домене EIM

Для создания нового домена EIM и включения системы в его состав необходимы следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)
- Права доступа на настройку системы (*IOSYSCFG)

Для того чтобы запустить мастер настройки EIM, создать с его помощью новый домен EIM и добавить удаленную систему в этот домен, выполните следующие действия:

1. Убедитесь, что сервер каталогов в удаленной системе активен.
2. В System i Navigator выберите систему, в которой настроены EIM, и разверните пункты **Сеть > Преобразование идентификаторов в рамках предприятия**.
3. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите **Настроить**, чтобы запустить мастер настройки EIM.

   Примечание: Если EIM уже был настроен в данной системе, то эта опция называется **Изменить настройку**.
4. На странице мастера **Приветствие** выберите **Создать и добавить в новый домен**, после чего нажмите **Далее**.
5. На странице **Задать расположение домена EIM** выберите опцию **На локальном сервере каталогов** и нажмите кнопку **Далее**.

   Примечание: Эта опция позволяет настроить локальный сервер каталогов в качестве контроллера домена EIM. Поскольку на этом сервере каталогов хранятся все данные EIM для домена, то он для поддержки операций поиска соответствий EIM и других операций он должен быть активен.

Если служба сетевой идентификации на платформе System i не настроена или для настройки среды с единым входом в систему необходима дополнительная настройка этой службы, то будет показана страница **Настройка служб сетевой идентификации**. С помощью этой страницы вы можете запустить мастера и настроить службу сетевой идентификации. Вы также можете выполнить эту настройку позже, запустив мастера с помощью System i Navigator. По завершении настройки службы сетевой идентификации продолжит работу мастер настройки EIM.

6. Для настройки службы сетевой идентификации выполните следующие действия:
   a. На странице **Настройка служб сетевой идентификации** выберите опцию **Да** для запуска мастера настройки служб сетевой идентификации. С помощью этого мастера вы можете настроить несколько служб и интерфейсов i5/OS для работы в составе области Kerberos, а также настроить среду единого входа в систему, в которой применяется как EIM, так и служба сетевой идентификации.
   b. На странице **Задать информацию об области** укажите в поле **Область по умолчанию** имя области по умолчанию. Если для идентификации Kerberos вы применяете Microsoft Active Directory, то выберите опцию **Применять Microsoft Active Directory для идентификации Kerberos** и нажмите кнопку **Далее**.
   c. На странице **Указать информацию о KDC** укажите в поле **KDC** полное имя сервера Kerberos для данной области, в поле **Порт** укажите значение 88 и нажмите кнопку **Далее**.
   d. На странице **Указать информацию о сервере паролей** выберите опцию **Да** или **Нет** для настройки сервера паролей. Сервер паролей позволяет субъектам изменять свои пароли на сервере Kerberos. При выборе ответа **Да** укажите в поле **Сервер паролей** имя сервера паролей. В поле **Порт** оставьте значение по умолчанию 464 и нажмите кнопку Далее.
   e. На странице **Выбрать записи файла ключей** выберите опцию **Идентификация Kerberos i5/OS** и нажмите кнопку **Далее**.

      Примечание: Если вы хотите, чтобы соответствующие службы также применяли идентификацию Kerberos, то можете также создать записи файла ключей для сервера каталогов IBM Tivoli для i5/OS, i5/OS NetServer и сервера IBM HTTP Server for i5/OS. Для применения этими службами идентификации Kerberos может потребоваться их дополнительная настройка.

   f. На странице **Создать запись файла ключей i5/OS** введите и подтвердите пароль, а затем нажмите кнопку **Далее**. Этот тот же пароль, который вы будете применять при добавлении субъектов i5/OS на сервер Kerberos.
   g. Необязательно: На странице **Создать пакетный файл** выберите ответ **Да**, укажите следующую информацию и нажмите кнопку **Далее**:
      - В поле **Пакетный файл** укажите требуемый каталог. Вы можете нажать кнопку **Обзор** и найти требуемый каталог, либо вручную указать нужное значение в поле **Пакетный файл**.
      - В поле **Включить пароль** выберите ответ **Да**. Тем самым вы гарантируете включение в пакетный файл всех паролей, связанных с субъектами служб i5/OS. Следует помнить, что пароли отображаются в текстовом формате и их может просмотреть любой пользователь, имеющий права доступа на чтение пакетного файла. Таким образом, пакетный файл необходимо удалить с сервера Kerberos и с PC сразу же после использования. Если вы не включите пароли, то при запуске пакетного файла вам будет предложено указать пароль.

        Примечание: Вы также можете вручную добавить созданных мастером субъектов служб в каталог Microsoft Active Directory. Необходимые инструкции приведены в разделе Добавление субъектов i5/OS на сервер Kerberos

      - На странице обзорной информации просмотрите сведения о конфигурации службы сетевой идентификации и нажмите кнопку **Готово** для возврата к мастеру настройки EIM.

7. Страница **Задать контроллер домена EIM** позволяет указать информацию о подключении к настраиваемому удаленному контроллеру домена EIM:
   a. В поле **Имя контроллера домена** укажите имя удаленного сервера каталогов, который будет выполнять функции контроллера создаваемого домена EIM. В качестве имени контроллера домена EIM можно указать имя хоста TCP/IP или IP-адрес сервера каталогов.

b. Укажите информацию о подключении к контроллеру домена:
   - Если для подключения к контроллеру домена EIM должно применяться защищенное соединение, то выберите опцию **Применять защищенное соединение (SSL или TLS)**. Если выбрана эта опция, то для защиты данных EIM, передаваемых по незащищенной сети, например, по Internet, будет применяться протокол SSL или TLS.

     Примечание: Предварительно следует убедиться, что на контроллере домена EIM настроена поддержка защищенных соединений. В противном случае подключение к контроллеру может оказаться невозможным.
   - В поле **Порт** укажите порт TCP/IP, применяемый сервером каталогов для приема запросов. Если выбрана опция **Применять защищенное соединение**, то по умолчанию применяется порт 636; в противном случае - порт 389.

c. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации мастер может успешно подключиться к удаленному контроллеру домена EIM.

d. Нажмите кнопку **Далее**.

8. На странице **Указать пользователя для подключения** выберите **Тип пользователя** для установления соединения. Предусмотрены следующие типы пользователей: **Отличительное имя и пароль**, **Файл ключей и субъект Kerberos**, **Субъект Kerberos и пароль** или **Пользовательский профайл**. Типы пользователей, связанные с Kerberos, можно выбрать только в том случае, если на локальной платформе System i установлена служба сетевой идентификации. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:

   Примечание: Для того чтобы мастер имел права доступа, достаточные для создания в каталоге необходимых объектов EIM, выберите тип пользователя **Отличительное имя и пароль** и укажите DN и пароль администратора LDAP.

   Вы можете указать и другого пользователя, однако заданный пользователь должен иметь права доступа, эквивалентные правам доступа администратора LDAP удаленного сервера каталогов.

   a. Если было выбрано значение **Отличительное имя и пароль**, то введите следующие данные:
      - В поле **Отличительное имя** укажите отличительное имя и пароль администратора LDAP, предоставляющие мастеру права доступа, достаточные для администрирования домена EIM и находящихся в нем объектов.
      - В поле **Пароль** введите пароль, соответствующий заданному отличительному имени.
      - В поле **Подтверждение пароля** введите этот пароль еще раз.

   b. Если была выбрана опция **Файл ключей и субъект Kerberos**, то введите следующие данные:
      - В поле **Файл ключей** укажите полное имя файла ключей, содержащего сведения о субъекте Kerberos, который должен применяться мастером для подключения к домену EIM. Вы также можете нажать кнопку **Обзор** и выбрать требуемый файл в структуре каталогов интегрированной файловой системы i5/OS.
      - В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
      - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.

   c. Если была выбрана опция **Субъект Kerberos и пароль**, то введите следующие данные:
      - В поле **Субъект** укажите имя субъекта Kerberos, который должен применяться мастером для подключения к домену EIM.
      - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект jsmith в области ordept.myco.com представлен в файле ключей записью jsmith@ordept.myco.com.

- В поле **Пароль** введите пароль, соответствующий заданному субъекту Kerberos.
- В поле **Подтверждение пароля** введите этот пароль еще раз.

d. Если была выбрана опция **Пользовательский профайл и пароль**, то введите следующие данные:
   - В поле **Пользовательский профайл** укажите пользовательский профайл, который должен применяться мастером для подключения к домену EIM.
   - В поле **Пароль** введите пароль, соответствующий заданному пользовательскому профайлу.
   - В поле **Подтверждение пароля** введите этот пароль еще раз.

e. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации о пользователе мастер может успешно подключиться к контроллеру домена EIM.

f. Нажмите кнопку **Далее**.

9. На странице **Укажите домен** введите следующие данные:
   a. В поле **Домен** укажите имя создаваемого домена EIM. Оставьте имя `EIM`, указанное по умолчанию, или введите другое имя. Имя не должно содержать такие специальные символы, как **= + < > , # ;** \ и *****.
   b. В поле **Описание** введите описание этого домена.
   c. Нажмите кнопку **Далее**.
10. В окне **Задать родительское DN для домена** выберите опцию **Да** чтобы задать родительское DN, в котором мастер должен разместить создаваемый домен EIM. Это отличительное имя записи, потомком которой в иерархии информации каталога является запись имени домен. Для сохранения данных EIM в поддереве сервера каталогов, суффикс которого определяется именем домена EIM, выберите ответ **Нет**.

    Примечание: При настройке с помощью мастера домена на удаленном контроллере следует указать родительское DN домена. Поскольку все необходимые объекты конфигурации с заданным родительским DN должны уже существовать (в противном случае настройка EIM выполнена не будет), то следует найти нужное DN, а не вводить его вручную. Для просмотра дополнительной информации о родительском DN нажмите кнопку **Справка**.
11. На странице **Информация о реестре** укажите, следует ли добавлять локальные реестры пользователей в домен EIM в качестве определений реестров. Можно выбрать один из указанных ниже типов реестров пользователей или оба типа:

    Примечание: Сейчас создавать определения реестров не нужно. Если в дальнейшем вы решите создать определения реестров, то вам нужно будет добавить определение системного реестра и обновить свойства конфигурации EIM.

    a. Для добавления определения локального реестра выберите опцию **Локальный реестр i5/OS**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя реестра EIM - произвольная строка, задающая тип реестра и отдельный экземпляр этого реестра.
    b. Для добавления определения реестра Kerberos выберите опцию **Kerberos**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя определения реестра по умолчанию совпадает с именем области. Оставив значение по умолчанию и воспользовавшись именем реестра Kerberos, совпадающим с именем области, вы можете повысить производительность получения информации из реестра. При необходимости выберите опцию **Идентификаторы пользователей Kerberos с учетом регистра символов**.
    c. Нажмите кнопку **Далее**.
12. На странице **Указать системного пользователя для EIM** выберите тип пользователя, с помощью которого система будет выполнять операции EIM от имени функций операционной системы. Эти операции включают поиск соответствий и удаление связей при удалении локального пользовательского профайла i5/OS. Предусмотрены следующие типы пользователей: **Отличительное имя и пароль**, **Файл ключей и субъект Kerberos** или **Субъект и пароль Kerberos**. Список доступных типов пользователя зависит от конфигурации текущей системы. Например, если в системе не настроена служба сетевой идентификации, то вы не сможете выбрать тип пользователя Kerberos. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях:

Примечание: Вы должны указать пользователя, определенного на сервере каталогов, выполняющем функции контроллера домена EIM. Указанному пользователю должны быть предоставлены права на поиск соответствий и на управление реестрами локальных пользователей. Если указанный пользователь не имеет таких прав, некоторые функции операционной системы, связанные с единым входом в систему и удалением пользовательских профайлов, могут не выполняться.

Если перед запуском этого мастера вы не настроили сервер каталогов, то единственным доступным типом пользователя будет **Отличительное имя и пароль**, а в качестве значения можно будет указать только DN администратора LDAP.

a. Если было выбрано значение **Отличительное имя и пароль**, то введите следующие данные:
   - В поле **Отличительное имя** укажите отличительное имя LDAP, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
   - В поле **Пароль** введите пароль, соответствующий заданному отличительному имени.
   - В поле **Подтверждение пароля** введите этот пароль еще раз.

b. Если была выбрана опция **Субъект Kerberos и пароль**, то введите следующие данные:
   - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
   - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
   - В поле **Пароль** введите пароль пользователя.
   - В поле **Подтверждение пароля** введите этот пароль еще раз.

c. Если была выбрана опция **Файл ключей и субъект Kerberos**, то введите следующие данные:
   - В поле **Файл ключей** укажите полное имя файла ключей, содержащего сведения о субъекте Kerberos, который должен применяться системой при выполнении операций EIM. Вы также можете нажать кнопку **Обзор** и выбрать требуемый файл в структуре каталогов интегрированной файловой системы System i.
   - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
   - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.

d. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации о пользователе мастер может успешно подключиться к контроллеру домена EIM.

e. Нажмите кнопку **Далее**.

13. На странице сводной информации проверьте правильность указанной информации о конфигурации. Если все данные указаны верно, нажмите кнопку **Готово**.

Завершение конфигурации EIM для домена

После завершения работы мастер добавит новый домен в папку **Управление доменами** и создаст для данного сервера базовую конфигурацию EIM. Для завершения настройки EIM в домене необходимо выполнить следующие задачи:

1. Запустить мастера настройки EIM на каждом дополнительном сервере, который вы планируете включить в состав домена. За дополнительной информацией обратитесь к разделу “Добавление в существующий домен” на стр. 83.
2. Добавить в домен EIM определения реестров EIM для других платформ и приложений, которые также будут входить в домен EIM. Эти определения реестров соответствуют реальным реестрам пользователей,

которые также должны применяться в домене. В зависимости от реализации EIM обратитесь к разделу “Добавление определения реестра систем” на стр. 95 или “Добавление определения реестра приложений” на стр. 95.

3. В зависимости от требований конфигурации EIM выберите один из следующих вариантов:
   a. “Создание идентификатора EIM” на стр. 102 для каждого уникального пользователя или объекта в домене, а затем “Создание связей идентификаторов EIM” на стр. 105 для них.
   b. “Создание связи стратегий” на стр. 106 задать соответствие между группой пользователей и одним целевым идентификатором пользователя.
   c. Выполнение перечисленных операций в различных сочетаниях.
4. С помощью функции “Тестирование связей EIM” на стр. 91 проверьте правильность преобразования идентификаторов в среде EIM.
5. Если в настоящее время в EIM определен только DN администратора LDAP, то у этого пользователя EIM есть очень высокий уровень доступа ко всем данным сервера каталогов. Рекомендуется создать несколько дополнительных DN пользователей с более адекватным и более ограниченным набором прав доступа к данным EIM. Дополнительная информация о создании DN сервера каталогов приведена в разделе Отличительные имена в главе i5/OS Information Center. Число создаваемых дополнительных пользователей EIM зависит от того, насколько тонко в применяемой стратегии защиты разделяются права доступа и обязанности пользователей. Обычно бывает необходимо создать по крайней мере два типа DN:
   - **Пользователь с правами доступа администратора EIM**

     DN администратора EIM обеспечивает необходимый уровень доступа для администратора, ответственного за управление доменом EIM. Этот DN администратора EIM может применяться для подключения к контроллеру домена EIM для управления всеми аспектами его работы с помощью System i Navigator.
   - **По крайней мере один пользователь, имеющий все права доступа из следующего набора:**
     – Администратор идентификаторов
     – Администратор реестра
     – Поиск соответствий EIM

     Этот пользователь имеет права доступа, необходимые для системного пользователя, выполняющего операции EIM от имени операционной системы.

   Примечание: Для применения в качестве системного пользователя этого нового DN вместо DN администратора LDAP необходимо изменить свойства конфигурации EIM для платформы System i platform. Изменение DN системного пользователя описано в разделе “Управление свойствами конфигурации EIM” на стр. 121.

Если вы создали базовую конфигурацию службы сетевой идентификации, то может потребоваться дополнительная настройка, особенно в том случае, если вы реализуете среду с единым входом в систему. Необходимую информацию вы можете найти в полном описании инструкций по настройке в разделе Включение поддержки единого входа в систему в i5/OS.

Добавление в существующий домен

Информация, касающаяся применения мастера настройки преобразования идентификаторов в рамках предприятия (EIM) на платформе System i для настройки контроллера домена и создания домена EIM и применения мастера настройки для настройки других систем в качестве доменов.

После создания домена EIM и настройки в одной из систем контроллера домена вы можете приступить к настройке дополнительных платформ System i, которые будут входить в состав уже созданного домена EIM. При работе с мастером вам потребуется указать информацию о домене, включая сведения о соединении с контроллером домена EIM. Если для добавления систем в существующий домен вы используете мастера настройки EIM, то в случае выбора Kerberos в качестве составного компонента конфигурации EIM вам будет предложено запустить мастера настройки службы сетевой идентификации.

Добавляя систему в существующий домен с помощью мастера настройки EIM вы можете выполнить следующие задачи:

- Настройка службы сетевой идентификации для системы
- Создание определений реестра EIM для локального реестра i5/OS и реестра Kerberos.
- Настройка системы для работы в составе существующего домена EIM

Для настройки конфигурации системы в составе существующего домена EIM необходимые следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)

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

1. Убедитесь, что сервер каталогов в удаленной системе активен.
2. В System i Navigator выберите систему, в которой настроены EIM, и разверните пункты **Сеть > Преобразование идентификаторов в рамках предприятия**.
3. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите **Настроить...**, чтобы запустить мастер настройки EIM.

   Примечание: Если EIM уже был настроен в данной системе, то эта опция называется **Изменить настройку...**.
4. На странице приветствия мастера выберите опцию **Добавить в существующий домен** и нажмите кнопку **Далее**.

   Примечание: Если служба сетевой идентификации в модели System i не настроена или для настройки среды с единым входом в систему необходима дополнительная настройка этой службы, то будет показана страница **Настройка служб сетевой идентификации**. С помощью этой страницы вы можете запустить мастера и настроить службу сетевой идентификации. Вы также можете выполнить эту настройку позже, запустив мастера с помощью System i Navigator. По завершении настройки службы сетевой идентификации продолжит работу мастер настройки EIM.
5. Для настройки службы сетевой идентификации выполните следующие действия:
   a. На странице **Настройка служб сетевой идентификации** выберите опцию **Да** для запуска мастера настройки служб сетевой идентификации. С помощью этого мастера вы можете настроить несколько служб и интерфейсов i5/OS для работы в составе области Kerberos, а также настроить среду единого входа в систему, в которой применяется как EIM, так и служба сетевой идентификации.
   b. На странице **Задать информацию об области** укажите в поле **Область по умолчанию** имя области по умолчанию. Если для идентификации Kerberos вы применяете Microsoft Active Directory, то выберите опцию **Применять Microsoft Active Directory для идентификации Kerberos** и нажмите кнопку **Далее**.
   c. На странице **Указать информацию о KDC** укажите в поле **KDC** полное имя сервера Kerberos для данной области, в поле **Порт** укажите значение 88 и нажмите кнопку **Далее**.
   d. На странице **Указать информацию о сервере паролей** выберите опцию **Да** или **Нет** для настройки сервера паролей. Сервер паролей позволяет субъектам изменять свои пароли на сервере Kerberos. При выборе ответа **Да** укажите в поле **Сервер паролей** имя сервера паролей. В поле **Порт** оставьте значение по умолчанию 464 и нажмите кнопку Далее.
   e. На странице **Выбрать записи файла ключей** выберите опцию **Идентификация Kerberos i5/OS** и нажмите кнопку **Далее**.

      Примечание: Если вы хотите, чтобы соответствующие службы также применяли идентификацию Kerberos, то можете также создать записи файла ключей для сервера каталогов IBM

Tivoli для i5/OS, i5/OS NetServer и IBM HTTP Server for i5/OS. Для применения этими службами идентификации Kerberos может потребоваться их дополнительная настройка.

f. На странице **Создать запись файла ключей i5/OS** введите и подтвердите пароль, а затем нажмите кнопку **Далее**. Этот тот же пароль, который вы будете применять при добавлении субъектов i5/OS на сервер Kerberos.

g. Необязательно: На странице **Создать пакетный файл** выберите ответ **Да**, укажите следующую информацию и нажмите кнопку **Далее**:

- В поле **Пакетный файл** укажите требуемый каталог. Вы можете нажать кнопку **Обзор** и найти требуемый каталог, либо вручную указать нужное значение в поле **Пакетный файл**.
- В поле **Включить пароль** выберите ответ **Да**. Тем самым вы гарантируете включение в пакетный файл всех паролей, связанных с субъектами служб i5/OS. Следует помнить, что пароли отображаются в текстовом формате и их может просмотреть любой пользователь, имеющий права доступа на чтение пакетного файла. Таким образом, пакетный файл необходимо удалить с сервера Kerberos и с PC сразу же после использования. Если вы не включите пароли, то при запуске пакетного файла вам будет предложено указать пароль.

  Примечание: Вы также можете вручную добавить созданных мастером субъектов служб в каталог Microsoft Active Directory. Необходимые инструкции приведены в разделе Добавление субъектов i5/OS на сервер Kerberos

- На странице обзорной информации просмотрите сведения о конфигурации службы сетевой идентификации и нажмите кнопку **Готово** для возврата к мастеру настройки EIM.

6. На странице **Укажите контроллер домена** введите следующие данные:

   Примечание: Для успешной настройки EIM сервер каталогов, выполняющий функции контроллера домена, должен быть активен.

   a. В поле **Имя контроллера домена** укажите имя системы, выполняющей функции контроллера домена EIM, в который вы включаете платформу System i.

   b. Если для подключения к контроллеру домена EIM должно применяться защищенное соединение, то выберите опцию **Применять защищенное соединение (SSL или TLS)**. Если выбрана эта опция, то для защиты данных EIM, передаваемых по незащищенной сети, например, по Internet, будет применяться протокол SSL или TLS.

      Примечание: Предварительно следует убедиться, что на контроллере домена EIM настроена поддержка защищенных соединений. В противном случае подключение к контроллеру может оказаться невозможным.

   c. В поле **Порт** укажите порт TCP/IP, применяемый сервером каталогов для приема запросов. Если выбрана опция **Применять защищенное соединение**, то по умолчанию применяется порт 636; в противном случае - порт 389.

   d. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации мастер может успешно подключиться к контроллеру домена EIM.

   e. Нажмите кнопку **Далее**.

7. На странице **Указать пользователя для подключения** выберите **Тип пользователя** для установления соединения. Предусмотрены следующие типы пользователей: **Отличительное имя и пароль**, **Файл ключей и субъект Kerberos**, **Субъект Kerberos и пароль** или **Пользовательский профайл**. Типы пользователей, связанные с Kerberos, можно выбрать только в том случае, если на локальной платформе System i установлена служба сетевой идентификации. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях окна:

   Примечание: Для того чтобы мастер имел права доступа, достаточные для создания в каталоге необходимых объектов EIM, выберите тип пользователя **Отличительное имя и пароль** и укажите DN и пароль администратора LDAP.

Вы можете указать и другого пользователя, однако заданный пользователь должен иметь права доступа, эквивалентные правам доступа администратора LDAP удаленного сервера каталогов.

- Если была выбрана опция **Отличительное имя и пароль**, то введите следующие данные:
  - В поле **Отличительное имя** укажите отличительное имя (DN) администратора сервера LDAP, которому предоставлены права 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, соответствующий заданному отличительному имени.
  - В поле **Подтверждение пароля** введите этот пароль еще раз.
- Если была выбрана опция **Файл ключей и субъект Kerberos**, то введите следующие данные:
  - В поле **Файл ключей** укажите полное имя файла ключей, содержащего сведения о субъекте Kerberos, который должен применяться мастером для подключения к домену EIM. Вы также можете нажать кнопку **Обзор...** и выбрать требуемый файл в структуре каталогов интегрированной файловой системы System i.
  - В поле **Субъект** введите имя субъекта Kerberos для данного пользователя.
  - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
- Если была выбрана опция **Субъект Kerberos и пароль**, то введите следующие данные:
  - В поле **Субъект** укажите имя субъекта Kerberos, который должен применяться мастером для подключения к домену EIM.
  - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
  - В поле **Пароль** введите пароль, соответствующий заданному субъекту Kerberos.
  - В поле **Подтверждение пароля** введите этот пароль еще раз.
- Если была выбрана опция **Пользовательский профайл и пароль**, то введите следующие данные:
  - В поле **Пользовательский профайл** укажите пользовательский профайл, который должен применяться мастером для подключения к домену EIM.
  - В поле **Пароль** введите пароль, соответствующий заданному пользовательскому профайлу.
  - В поле **Подтверждение пароля** введите этот пароль еще раз.
- Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации о пользователе мастер может успешно подключиться к контроллеру домена EIM.
- Нажмите кнопку **Далее**.

8. На странице **Указать домен** выберите имя домена, в который необходимо добавить сервер, и нажмите кнопку **Далее**.
9. На странице **Информация о реестре** укажите, следует ли добавлять локальные реестры пользователей в домен EIM в качестве определений реестров. Можно выбрать один из указанных ниже типов реестров пользователей или оба типа:
   - Для добавления определения локального реестра выберите опцию **Локальный реестр i5/OS**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя реестра EIM - произвольная строка, задающая тип реестра и отдельный экземпляр этого реестра.

     Примечание: Сейчас создавать определение локального реестра i5/OS не нужно. Если в дальнейшем вы решите создать определение реестра i5/OS, то вам нужно будет добавить определение системного реестра и обновить свойства конфигурации EIM.

- Для добавления определения реестра Kerberos выберите опцию **Kerberos**. Оставьте имя определения реестра по умолчанию или укажите собственное имя. Имя определения реестра по умолчанию совпадает с именем области. Оставив значение по умолчанию и воспользовавшись именем реестра Kerberos, совпадающим с именем области, вы можете повысить производительность получения информации из реестра. При необходимости выберите опцию **Идентификаторы пользователей Kerberos с учетом регистра символов**.

  Примечание: Если с помощью мастера настройки EIM вы уже добавляли в другую систему определение реестра, в котором у данной модели System i есть субъект службы, то при выполнении данной процедуры настройки добавлять определение реестра Kerberos не нужно. Однако после завершения работы с мастером вам нужно будет указать в свойствах конфигурации системы имя этого реестра Kerberos.
- Нажмите кнопку **Далее**.

10. На странице **Указать системного пользователя для EIM** выберите тип пользователя, с помощью которого система будет выполнять операции EIM от имени функций операционной системы. Эти операции включают поиск соответствий и удаление связей при удалении локального пользовательского профайла i5/OS. Предусмотрены следующие типы пользователей: **Отличительное имя и пароль**, **Файл ключей и субъект Kerberos** или **Субъект и пароль Kerberos**. Список доступных типов пользователя зависит от конфигурации текущей системы. Например, если в системе не настроена служба сетевой идентификации, то вы не сможете выбрать тип пользователя Kerberos. Выбранный тип пользователя влияет на другую информацию, которую следует указать в полях:

    Примечание: Вы должны указать пользователя, определенного на сервере каталогов, выполняющем функции контроллера домена EIM. Указанному пользователю должны быть предоставлены права на поиск соответствий и на управление реестрами локальных пользователей. Если указанный пользователь не имеет этих прав, определенные функции операционной системы, связанные с единым входом в систему и удалением пользовательских профайлов могут не выполняться.

    - Если была выбрана опция **Отличительное имя и пароль**, то введите следующие данные:
      - В поле **Отличительное имя** укажите отличительное имя LDAP, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
      - В поле **Пароль** введите пароль, соответствующий заданному отличительному имени.
      - В поле **Подтверждение пароля** введите этот пароль еще раз.
    - Если была выбрана опция **Субъект Kerberos и пароль**, то введите следующие данные:
      - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.
      - В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.
      - В поле **Пароль** введите пароль пользователя.
      - В поле **Подтверждение пароля** введите этот пароль еще раз.
    - Если была выбрана опция **Файл ключей и субъект Kerberos**, то введите следующие данные:
      - В поле **Файл ключей** укажите полное имя файла ключей, содержащего сведения о субъекте Kerberos, который должен применяться системой при выполнении операций EIM. Вы также можете нажать кнопку **Обзор...** и выбрать требуемый файл в структуре каталогов интегрированной файловой системы System i.
      - В поле **Субъект** укажите имя субъекта Kerberos, соответствующее тому пользователю, который должен применяться системой при выполнении операций EIM.

– В поле **Область** укажите полное имя области Kerberos, к которой относится данный субъект. Имя субъекта и имя области однозначно определяют пользователя Kerberos в файле ключей. Например, субъект `jsmith` в области `ordept.myco.com` представлен в файле ключей записью `jsmith@ordept.myco.com`.

- Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации о пользователе мастер может успешно подключиться к контроллеру домена EIM.
- Нажмите кнопку **Далее**.

11. На странице сводной информации проверьте правильность указанной информации о конфигурации. Если все данные указаны верно, нажмите кнопку **Готово**.

Завершение конфигурации EIM для домена

После завершения работы мастер добавит домен в папку **Управление доменами** и создаст для данного сервера базовую конфигурацию EIM. Однако для завершения настройки EIM на сервере может потребоваться выполнить следующие дополнительные задачи:

1. Добавить в домен EIM определения реестров EIM для других систем i5/OS и приложений, которые также будут входить в домен EIM. Эти определения реестров соответствуют реальным реестрам пользователей, которые также должны применяться в домене. В зависимости от предъявляемых требований вы можете Добавить определения системных реестров или Добавить определения реестров приложений.
2. В зависимости от требований конфигурации EIM выберите один из следующих вариантов:
   - Создать идентификаторы EIM для каждого уникального пользователя или объекта в домене, а затем создать для них связи идентификаторов.
   - Создать связи стратегий, задающие соответствие между группой пользователей и одним целевым идентификатором пользователя.
   - Воспользоваться сочетанием перечисленных опций.
3. С помощью функции проверки преобразования проверьте правильность преобразования идентификаторов в среде EIM.
4. Если в настоящее время в EIM определен только DN администратора LDAP, то у этого пользователя EIM есть очень высокий уровень доступа ко всем данным сервера каталогов. Рекомендуется создать несколько дополнительных DN пользователей с более адекватным и более ограниченным набором прав доступа к данным EIM. Дополнительная информация о создании DN сервера каталогов приведена в разделе Отличительные имена в главе i5/OS Information Center. Число создаваемых дополнительных пользователей EIM зависит от того, насколько тонко в применяемой стратегии защиты разделяются права доступа и обязанности пользователей. Обычно бывает необходимо создать по крайней мере два типа DN:
   - **Пользователь с правами доступа администратора EIM**

     DN администратора EIM обеспечивает необходимый уровень доступа для администратора, ответственного за управление доменом EIM. Этот DN администратора EIM может применяться для подключения к контроллеру домена EIM для управления всеми аспектами его работы с помощью System i Navigator.
   - **По крайней мере один пользователь, имеющий все права доступа из следующего набора:** :
     – Администратор идентификаторов
     – Администратор реестра
     – Поиск соответствий EIM

     Этот пользователь имеет права доступа, необходимые для системного пользователя, выполняющего операции EIM от имени операционной системы.

     Примечание: Для применения в качестве системного пользователя этого нового DN вместо DN администратора LDAP необходимо изменить свойства конфигурации EIM для платформы System i platform. Изменение DN системного пользователя описано в разделе Управление свойствами конфигурации EIM.

Если вы создали базовую конфигурацию службы сетевой идентификации, то может потребоваться дополнительная настройка, особенно в том случае, если вы реализуете среду с единым входом в систему. Необходимую информацию вы можете найти в полном описании инструкций по настройке в разделе Включение поддержки единого входа в систему в i5/OS.

Настройка защищенного соединения с контроллером домена EIM

Вы можете настроить применение протокола SSL или TLS для установления защищенного соединения с контроллером домена EIM и защиты передаваемых данных EIM.

Для того чтобы настроить поддержку SSL или TLS для EIM, необходимо выполнить следующие задачи:

1. При необходимости с помощью диспетчера цифровых сертификатов (DCM) создать сертификат сервера каталогов, который будет применяться средствами поддержки SSL.
2. Включить поддержку SSL на локальном сервере каталогов, который выполняет функции контроллера домена EIM.
3. Указать в свойствах EIM, что в модели System i применяется защищенное соединение SSL. Для обновления свойств конфигурации EIM выполните следующие действия:
   a. В System i Navigator выберите систему, в которой необходимо настроить EIM, и разверните пункты **Сеть → Преобразование идентификаторов в рамках предприятия**.
   b. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите **Свойства**.
   c. На странице **Домен** выберите опцию **Применять защищенное соединение (SSL или TLS)**, укажите номер защищенного порта сервера каталогов или оставьте значение по умолчанию 636 в поле **Порт** и нажмите кнопку **OK**.
4. Указать в свойствах всех доменов EIM, что для управления доменом с помощью System i Navigator применяется соединение SSL. Для обновления свойств домена EIM выполните следующие действия:
   a. В System i Navigator выберите систему, в которой необходимо настроить EIM, и разверните пункты **Сеть → Преобразование идентификаторов в рамках предприятия → Управление доменами**.
   b. Выберите домен EIM, с которым вы планируете работать.
      - Если необходимый домен EIM отсутствует в папке **Управление доменами**, то перейдите к разделу Добавление домена EIM в папку Управление доменами.
      - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
   c. Щелкните правой кнопкой мыши на домене EIM, с которым установлено соединение, и выберите пункт **Свойства**.
   d. На странице **Домен** выберите опцию **Применять защищенное соединение (SSL или TLS)**, укажите номер защищенного порта сервера каталогов или оставьте значение по умолчанию 636 в поле **Порт** и нажмите кнопку **OK**.

Управление преобразованием идентификаторов в рамках предприятия

Существует множество различных административных задач, которые вам придется выполнять для управления доменом EIM и данными этого домена после настройки EIM на платформе System i.

В этом разделе приведены дополнительные сведения, связанные с управлением EIM на вашем предприятии.

Управление доменами EIM

Используйте System i Navigator для управления всеми доменами EIM.

Для управления любым доменом EIM необходимо, чтобы этот домен был показан в папке **Управление доменами** в папке **Сеть** в System i Navigator. При создании и настройке нового домена EIM с помощью мастера настройки EIM домен добавляется в папку **Управление доменами** автоматически, поэтому вы можете управлять этим доменом и информацией в нем.

Для управления доменом EIM, находящимся в той же сети, что и система System i, можно использовать подключение к любой системе, даже если она сама не входит в состав домена.

Вы можете выполнять следующие задачи управления доменом:

Добавление домена EIM в папку управления доменами

Для добавления домена EIM в папку управления доменами необходимы специальные права доступа *SECADM, а домен, добавляемый в папку Управление доменами, должен уже существовать.

Для добавления существующего домена EIM в папку **Управление доменами** выполните следующие действия:

1. Разверните узлы **Сеть>EIM**.
2. Щелкните правой кнопкой мыши на папке **Управление доменами** и выберите **Добавить домен**.
3. В окне **Добавить домен** укажите необходимые сведения о домене и соединении. Вы также можете нажать кнопку **Обзор** и просмотреть список доменов, которыми управляет выбранный контроллер домена.

   Примечание: Если вы нажмете кнопку **Обзор**, то появится окно диалога **Подключение к контроллеру домена EIM**. Для просмотра списка доменов необходимо подключиться к контроллеру домена с правами доступа администратора LDAP или EIM. Содержимое списка доменов зависит от предоставленных вам прав доступа EIM. Если у вас есть права доступа администратора LDAP, то вы сможете просмотреть список всех доменов, которыми управляет контроллер домена. В противном случае в списке будут показаны только те домены, к которым у вас есть права доступа администратора EIM.
4. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
5. Нажмите **OK**, чтобы добавить домен.

Подключение к домену EIM

Для того чтобы вы могли работать с доменом EIM, необходимо сначала подключиться к контроллеру этого домена. Это можно сделать даже в том случае, если модель System i не входит в этот домен.

Для подключения к контроллеру домена EIM пользователь, под именем которого вы подключаетесь, должен входить в группу с правами доступа. Задачи, которые вы можете выполнять в домене EIM, а также данные EIM, которые вы можете просматривать и изменять, определяются вашим членством в группе управления доступом EIM.

Для подключения к домену EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Дважды щелкните на имени домена, с которым необходимо установить соединение.

   Примечание: Если нужный домен не указан в разделе **Управление доменами**, необходимо добавить домен EIM в папку управления доменами.
3. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Установить соединение**.
4. В окне **Подключение к домену EIM** укажите **Тип пользователя**, задайте необходимую идентификационную информацию и выберите опцию пароля для подключения к контроллеру домена.
5. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
6. Для подключения к контроллеру домена нажмите кнопку **OK**.

Включение связи стратегий для домена

Связи стратегий представляют собой средство создания соответствий между группой идентификаторов и одним идентификатором пользователя в том случае, когда идентификатор EIM не существует.

Связь стратегий позволяет преобразовать исходный набор из нескольких идентификаторов пользователей в отдельный целевой идентификатор пользователя, определенный в заданном целевом реестре. Для применения связей стратегий необходимо сначала разрешить применение в домене связей стратегий в операциях поиска соответствий.

Для включения поддержки стратегий преобразования необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для того чтобы разрешить применение связей стратегий в домене выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Стратегия преобразования**.
   - Если нужный домен не указан в разделе **Управление доменами**, необходимо добавить домен EIM в папку управления доменами.
   - Если соединение с необходимым доменом EIM не установлено, необходимо подключиться к контроллеру домена EIM. (Опция **Стратегия преобразования** становится доступной только после подключения к домену.)
3. На странице **Общие** выберите опцию **Разрешить операциям поиска применять связи стратегий в домене**.
4. Нажмите кнопку **OK**.

Примечание: Необходимо разрешить операции поиска и разрешить применение связей стратегий для каждого определения целевого реестра, для которого определены связи стратегий. Если вы не включите для определения целевого реестра поиск соответствий, то этот реестр не будет применяться в операциях поиска соответствий EIM. Если вы не укажете, что целевой реестр может применять связи стратегий, то операции поиска соответствий EIM будут игнорировать все определенные в этом реестре связи стратегий.

Понятия, связанные с данным

“Поддержка и активация стратегий преобразования EIM” на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

Тестирование связей EIM

При тестировании связей EIM в созданной конфигурации EIM выполняются операции поиска соответствий. Тестирование позволяет убедиться, что выбранный исходный идентификатор пользователя правильно преобразуется в целевой идентификатор. Проверка гарантирует возврат правильных результатов операциями поиска EIM на основе заданной информации.

Для того чтобы воспользоваться функцией тестирования преобразования в созданной конфигурации EIM необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа EIM одного из следующих уровней:

- Администратор EIM
- Администратор идентификаторов
- Администратор реестра
- Операции поиска соответствия EIM

Для тестирования конфигурации EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.

2. Выберите домен EIM, с которым вы планируете работать.
   - Если необходимый домен EIM отсутствует в папке **Управление доменами**, то перейдите к разделу Добавление домена EIM в папку Управление доменами.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Щелкните правой кнопкой мыши на домене EIM, с которым установлено соединение, и выберите пункт **Проверить преобразование**.
4. В окне **Проверить преобразование** укажите следующую информацию:
   a. В поле **Исходный реестр** укажите имя исходного определения реестра для операции поиска.
   b. В поле **Исходный пользователь** укажите исходный идентификатор пользователя для операции поиска.
   c. В поле **Целевой реестр** укажите имя целевого определения реестра для операции поиска.
   d. Необязательно: В поле **Информация для поиска** укажите определенную для целевого пользователя информацию для поиска.
5. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
6. Нажмите кнопку **Проверить** и просмотрите показанные результаты преобразования.

   Примечание: Если операция преобразования идентификатора/поиска связанного идентификатора возвращает неоднозначный результат, появится окно Проверить преобразование - Результат с сообщением об ошибке и списком целевых пользователей, обнаруженных операцией поиска.
   a. Для устранения неполадок, выберите целевого пользователя и нажмите кнопку **Подробные сведения**.
   b. В окне Проверить преобразование - Сведения приведена информация о результатах выполнения операции поиска идентификатора для указанного целевого пользователя. Нажмите кнопку Справка, чтобы получить дополнительную информацию о результатах операции преобразования идентификатора/поиска связанного идентификатора.
   c. Нажмите **Закрыть** для выхода из окна **Проверить преобразование - Результаты**.
7. Продолжите тестирование конфигурации или нажмите кнопку **Закрыть** для выхода.

Понятия, связанные с данным

“Устранение неполадок записей соответствия EIM” на стр. 126
Существует ряд типичных неполадок, которые могут привести к неправильной работе EIM или к тому, что преобразование совсем не будет выполняться. В следующей таблице приведена информация о неполадках, которые могут привести к ошибкам преобразования EIM, а также о возможных способах устранения этих неполадок. Для устранения ошибок преобразования EIM может потребоваться попробовать все перечисленные в таблице решения.

Работа с результатами проверки и устранение неполадок:

Если в процессе поиска соответствия будет найдена связь между исходным идентификатором пользователя и указанным целевым реестром пользователей, то в результате проверки будет возвращен целевой идентификатор пользователя. Указывается также тип связи, найденной между двумя идентификаторами пользователей. Если в ходе проверки не удастся найти связь на основании заданной информации, то в результате проверки будет возвращен целевой идентификатор пользователя `none`.

В процессе тестирования, как и в процессе обычной операции поиска соответствия EIM, выполняется поиск и возвращается первый соответствующий заданным параметрам целевой идентификатор пользователя. Поиск выполняется в следующем порядке:

1. Связь конкретных идентификаторов
2. Связь стратегии фильтра сертификатов
3. Связь стратегии реестра по умолчанию

4. Связь стратегии домена по умолчанию

В некоторых случаях целевой идентификатор пользователя не возвращается, несмотря на то, что в домене настроены необходимые связи. Проверьте правильность информации, указываемой при проверке. Если информация задана правильно, но результаты не возвращаются, то возможны следующие причины ошибки:

- На уровне домена не включена поддержка связей стратегий. Возможно, вам потребуется включить связи стратегий для домена.
- На уровне отдельного реестра не включена поддержка связей стратегий или поддержка поиска соответствий. Вам может потребоваться включить поддержку поиска соответствий и применение связей стратегий для целевого реестра.
- Неправильно настроены исходные или целевые связи идентификатора EIM. Например, у субъекта Kerberos (или пользователя Windows) может отсутствовать исходная связь или существовать неправильная исходная связь. Кроме того, в целевой связи может быть указан неправильный идентификатор пользователя. С помощью функции Показать все связи идентификаторов для идентификатора EIM проверьте связи выбранного идентификатора.
- Неправильно настроена связь стратегий. С помощью функции Показать все связи стратегий для домена проверьте информацию об определенных в домене исходных и целевых связях стратегий.
- Определение реестра и идентификаторы пользователей не совпадают из-за несоответствия регистра символов. Вы можете удалить, а затем заново создать реестр или связи, указав символы в правильном регистре.

В некоторых случаях могут быть получены неоднозначные результаты. В такой ситуации выдается сообщение об ошибке. Результаты считаются неоднозначными в том случае, если заданным условиям соответствует несколько целевых идентификаторов пользователей. Операция поиска соответствия может вернуть несколько целевых идентификаторов при выполнении следующих условий в любых сочетаниях:

- У идентификатора EIM есть несколько отдельных целевых связей с одним и тем же целевым реестром.
- Для идентификатора пользователя в исходной связи указано несколько идентификаторов EIM и каждый из этих идентификаторов EIM имеет целевую связь с одним и тем же целевым реестром, хотя в целевых связях каждого идентификатора может быть указан свой целевой идентификатор пользователя.
- Один и тот же целевой реестр указан в нескольких стратегиях домена по умолчанию.
- Один и тот же целевой реестр и один и тот же исходный реестр указаны в нескольких связях стратегий реестров по умолчанию.
- В нескольких связях стратегий фильтров сертификатов указан один и тот же исходный реестр X.509, фильтр сертификатов или целевой реестр.

Такая ситуация может привести к возникновению ошибок в приложениях с поддержкой EIM, в том числе в продуктах и приложениях i5/OS, которые не могут применять подобные неоднозначные результаты поиска. В подробной ситуации необходимо выявить причину получения неоднозначных результатов и предпринять необходимые действия для ее устранения. В зависимости от причины, можно выполнить одно или несколько следующих действий:

- При проверке получено несколько неправильных целевых идентификаторов. Это указывает на наличие одной из следующих ошибок в конфигурации связей в домене:
  - Неправильно настроены исходные или целевые связи идентификатора EIM. Например, у субъекта Kerberos (или пользователя Windows) может отсутствовать исходная связь или существовать неправильная исходная связь. Кроме того, в целевой связи может быть указан неправильный идентификатор пользователя. С помощью функции Показать все связи идентификаторов для идентификатора EIM проверьте связи выбранного идентификатора.
  - Неправильно настроена связь стратегий. С помощью функции Показать все связи стратегий для домена проверьте информацию об определенных в домене исходных и целевых связях стратегий.
- Если при проверке получено несколько целевых идентификаторов пользователей, каждый их которых соответствует настроенной конфигурации, то нужно указать для каждого целевого идентификатора пользователя информацию для поиска. Уникальную информацию для поиска необходимо задать для всех

целевых идентификаторов пользователей, имеющих один и тот же источник (т.е. идентификатор EIM в случае связей идентификаторов или исходный реестр пользователей в случае связей стратегий). Определение уникальной информации для поиска для каждого целевого идентификатора позволяет гарантировать возврат операцией поиска соответствия только одного целевого идентификатора пользователя, а не всех возможных целевых идентификаторов. См. раздел Добавление информации для поиска в целевой идентификатор пользователя. Эту информацию следует указывать в операциях поиска соответствий.

Примечание: Такой подход допустим лишь в том случае, если приложение поддерживает применение информации для поиска. Однако следует помнить, что базовые приложения i5/OS, такие как System i Access for Windows, не могут различать несколько возвращенных операцией поиска целевых идентификаторов пользователей с помощью информации для поиска. Следовательно, необходимо переопределить связи в домене, обеспечив возврат операциями поиска соответствий только одного идентификатора пользователя, что гарантирует приложениям i5/OS возможность успешного поиска соответствий и преобразования идентификаторов.

Удаление домена EIM из папки управления домена

Вы можете удалить домен EIM, которым больше не требуется управлять, из папки **Управление доменами**. Следует помнить, что удаление домена из папки **Управление доменами** - это **не** то же самое, что удаление самого домена. Данные домена при этом не удаляются с контроллера домена.

Для удаления домена из папки не требуются какие-либо особые права доступа.

Для удаления домена EIM из папки **Управление доменами** выполните следующие действия:

1. Разверните узлы **Сеть>EIM**.
2. Щелкните правой кнопкой мыши на папке **Управление доменами** и выберите **Удалить домен из папки**.
3. Выберите домен EIM, который необходимо удалить из папки **Управление доменами**.
4. Нажмите кнопку **OK**, чтобы удалить этот домен.

Задачи, связанные с данной

"Удаление домена EIM и всех объектов конфигурации"
Перед удалением домена EIM необходимо удалить из него все определения реестров и все идентификаторы EIM. Если вы не хотите удалять домен и все находящиеся в нем данные, но больше не планируете управлять этим доменом, то воспользуйтесь функцией удаления домена из папки.

Удаление домена EIM и всех объектов конфигурации

Перед удалением домена EIM необходимо удалить из него все определения реестров и все идентификаторы EIM. Если вы не хотите удалять домен и все находящиеся в нем данные, но больше не планируете управлять этим доменом, то воспользуйтесь функцией удаления домена из папки.

Для удаления домена EIM необходимо обладать правами доступа доступа к EIM на одном из следующих уровней:

- Администратор LDAP.
- Администратор EIM.

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Если это необходимо, удалите из домена EIM все определения реестров.
3. Если это необходимо, удалите из домена EIM все определения идентификаторов EIM.
4. Щелкните правой кнопкой мыши на удаляемом домене и выберите пункт **Удалить**.
5. В окне **Подтверждение удаления** нажмите кнопку **Да**.

Примечание: В окне Состояние удаления отображается состояние процесса удаления.

Задачи, связанные с данной

"Удаление домена EIM из папки управления домена" на стр. 94
Вы можете удалить домен EIM, которым больше не требуется управлять, из папки **Управление доменами**. Следует помнить, что удаление домена из папки **Управление доменами** - это **не** то же самое, что удаление самого домена. Данные домена при этом не удаляются с контроллера домена.

Управление определениями реестров EIM

Для применения в домене EIM реестров пользователей и находящихся в них идентификаторов пользователей необходимо создать определения реестров для этих реестров. После этого с помощью созданных определений реестров вы сможете управлять применением этих реестров пользователей и входящих в их состав идентификаторов пользователей EIM.

Вы можете выполнять следующие задачи управления определениями реестров:

Понятия, связанные с данным

"Создание связи стратегий" на стр. 106
Связь стратегий непосредственно определяет взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре.

Задачи, связанные с данной

"Удаление связи стратегии" на стр. 119
Для удаления связи стратегии необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора реестра или администратора EIM.

Добавление определения реестра систем

Для создания определения реестра систем необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для добавления определения системного реестра в домен EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе Управление доменами, обратитесь к разделу "Добавление домена EIM в папку управления доменами" на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу "Подключение к домену EIM" на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши на значке **Реестры пользователей**, выберите опцию **Добавить реестр**, а затем - опцию **Система**.
5. В окне **Добавить системный реестр** укажите информацию об определении реестра приложения:
   a. Имя определения системного реестра
   b. Тип определения реестра
   c. Описание определения системного реестра
   d. (Необязательно). URL реестра пользователей.
   e. Один или несколько псевдонимов для определения системного реестра, если это необходимо
6. Нажмите кнопку **OK**, чтобы сохранить указанную информацию и добавить определение реестра в домен EIM.

Добавление определения реестра приложений

Для создания определения реестра приложений необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для добавления определения реестра приложения в домен EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.

2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе Управление доменами, обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши на значке **Реестры пользователей**, выберите опцию **Добавить реестр**, а затем - опцию **Приложение**.
5. В окне **Добавить реестр приложения** укажите информацию об определении реестра приложения:
   a. Имя определения реестра приложения.
   b. Имя определения системного реестра, подмножеством которого является определяемый реестр пользователей приложения. Указанное определение системного реестра должно уже существовать в EIM. В противном случае определение реестра приложения создано не будет.
   c. Тип определения реестра
   d. Описание определения реестра приложения
   e. Один или несколько псевдонимов для определения реестра приложения, если это необходимо
6. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
7. Нажмите кнопку **OK**, чтобы сохранить указанную информацию и добавить определение реестра в домен EIM.

Понятия, связанные с данным

“Определения системных реестров” на стр. 13
Определение системного реестра - это запись, создаваемая в EIM для представления и описания отдельного реестра пользователей на рабочей станции или на сервере.

Добавление группового определения реестра

Для создания группового определения реестра необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для добавления группового определения реестра в домен EIM выполните следующие действия:

1. Разверните узлы **Сеть → EIM → Управление доменами.**
2. Выберите домен EIM, с которым вы планируете работать.
   a. Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу Добавление домена EIM в папку Управление доменами.
   b. Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой на значке **Реестры пользователей**, выберите опцию **Добавить реестр**, затем выберите **Group**
5. В окне Добавить групповой реестр укажите сведения о групповом определении реестра следующим образом:
   a. Имя группового определения реестра.
   b. Выберите опцию **Элементы группового реестра с учетом регистра** если все элементы группового определения реестра чувствительны к регистру.
   c. Описание группового определения реестра.
   d. Один или несколько псевдонимов для группового определения реестра, если это необходимо.
6. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.

7. Нажмите кнопку **OK**, чтобы сохранить указанную информацию и добавить определение реестра в домен EIM.

Добавление определения реестра псевдонимов

Пользователь или разработчик приложения может указать дополнительную отличительную информацию для определения реестра. Это можно сделать путем создания псевдонима для определения реестра. Такие псевдонимы позволяют более точно различать определения реестров пользователей.

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

Для добавления псевдонима для определения реестра необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа одного из следующих уровней:

- Администратор реестра.
- Администратор выбранных реестров (для изменяемого реестра)
- Администратор EIM

Для добавления псевдонима для определения реестра EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе Управление доменами, обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Реестры пользователей**, чтобы просмотреть список определений реестров в домене.

   Примечание: Если у вас есть права доступа администратора к выбранным реестрам, то список будет содержать только те определения реестров, к которым у вас есть явно заданные права доступа.
5. Щелкните правой кнопкой мыши на определении реестра, для которого вы хотите добавить псевдоним, и выберите пункт меню **Свойства**.
6. Перейдите на страницу **Псевдонимы** и укажите имя и тип добавляемого псевдонима.

   Примечание: Можно указать тип псевдонима, отсутствующий в списке типов.
7. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
8. Нажмите кнопку **Добавить**.
9. Для сохранения изменений, внесенных в определение реестра, нажмите **OK**.

Определение собственного типа реестра пользователей в EIM

При создании определения реестра EIM вы можете указать один из нескольких заранее определенных типов реестров пользователей, представляющий фактический реестр пользователей, существующий в сети вашего предприятия.

Заранее определенные определения реестров охватывают почти все реестры пользователей операционных систем, поэтому может возникнуть ситуация, когда необходимо будет создать определение реестра, для которого в EIM нет заранее определенного типа. Из этой ситуации есть два выхода. Вы можете либо воспользоваться существующим определением реестра, которое соответствует параметрам вашего реестра пользователей, либо определить собственный тип реестра пользователей.

Для того чтобы определить новый тип реестра пользователей, не распознаваемый EIM по умолчанию, необходимо воспользоваться идентификатором (OID) и указать тип реестра в формате **OID-нормализация**, где **OID** - это идентификатор объекта в десятичном формате с точками, например, 1.2.3.4.5.6.7, а параметр **нормализация** может принимать значение **caseExact** или **caseIgnore**. Например, идентификатор объекта (OID) для System i равен `1.3.18.0.2.33.2-caseIgnore`.

Для обеспечения уникальности создаваемых идентификаторов объектов (OID) эти OID следует получать в уполномоченных организациях по регистрации OID. Это исключит возможность возникновения конфликтов с OID, созданными другими организациями или приложениями.

OID можно получить двумя способами:

- **Зарегистрировать объект в уполномоченной организации**.Этот способ может применяться в случае, когда необходимо получить небольшое количество фиксированных OID. Например, эти OID могут представлять стратегии применения сертификатов пользователями предприятия.
- **Зарезервировать в уполномоченной официальной организации сегмент и назначить в нем собственные OID**. Такой способ резервирования диапазона идентификаторов объектов может применяться в том случае, если требуется создать большое количество OID или планируется изменять назначенные OID в будущем. Зарезервированный сегмент определяет первые цифры **идентификаторов объектов** в десятичном формате с точками. Примером зарезервированного сегмента является `1.2.3.4.5.`. На его основе можно создать отдельные OID. Например, можно создать OID вида `1.2.3.4.5.x.x.x)`.

Дополнительная информация о регистрации OID 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). Справочная информация о подаче заявления на регистрацию идентификатора поставщиков приложений (RID) в формате Microsoft Word опубликована на Web-сайте библиотеки общедоступной документации ANSI по адресу http://public.ansi.org/ansionline/Documents/ . Для поиска этой информации выберите ссылки **Other Services > Registration Programs**. Сегмент OID ANSI для организаций `2.16.840.1`. ANSI предоставляет сегменты OID на платной основе. На получение сегмента OID от ANSI уходит приблизительно две недели. ANSI создает новый сегмент OID путем добавления числа (NEWNUM) в конец идентификатора сегмента, например: `2.16.840.1.NEWNUM`.
- В большинстве стран и регионов за обслуживание реестра OID отвечают национальные ассоциации по стандартизации. Как и сегменты ANSI, сегменты, присваиваемые этими организациями, обычно начинаются с OID `2.16`. Иногда получить информацию, отвечающую за ведение реестра OID в конкретной стране, достаточно сложно. Адреса национальных организаций - членов ISO приведены на Web-сайте http://www.wssn.net/WSSN/listings/links_national.html . На этом сайте указаны почтовые адреса и адреса электронной почты. Во многих случаях дополнительно указан адрес Web-сайта.
- Комитет по предоставлению адресов Internet (IANA) регистрирует частные номера предприятий, являющиеся идентификаторами объектов, в сегменте `1.3.6.1.4.1`. К настоящему моменту IANA выделил сегменты более 7500 компаниям. Страница с заявлением 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), определяющий новый сегмент OID, который будет иметь вид `1.3.6.1.4.1.NEWNUM`.
- Федеральное правительство США ведет Реестр объектов защиты компьютеров (CSOR). CSOR - уполномоченный орган для присвоения идентификаторов в сегменте `2.16.840.1.101.3`, который в настоящее время отвечает за регистрацию объектов для меток защиты, алгоритмов шифрования и стратегий применения сертификатов. OID стратегий применения сертификатов регистрируются в сегменте `2.16.840.1.101.3.2.1`. CSOR предоставляет OID стратегий подразделениям федерального правительства США. Дополнительная информация о CSOR приведена на Web-сайте http://www.csrc.nist.gov/pki/CSOR/csor.html .

Понятия, связанные с данным

“Определения реестров EIM” на стр. 11
Определение реестра EIM - это созданная в EIM запись, которая содержит данные об отдельном реестре пользователей предприятия. Реестр пользователей - это каталог, в котором содержатся идентификаторы пользователей отдельной системы или приложения.

Включение поддержки поиска соответствий и связей стратегий для целевого реестра

Поддержка стратегий преобразования преобразования идентификаторов в рамках предприятия (EIM) позволяет применять связи стратегий для создания соответствий между группой идентификаторов и одним идентификатором пользователя в том случае, когда идентификатор EIM не существует. Связь стратегий позволяет преобразовать исходный набор из нескольких идентификаторов пользователей в отдельный целевой идентификатор пользователя, определенный в заданном целевом реестре.

Для применения связей стратегий необходимо сначала включить в домене поиск соответствий с помощью связей стратегий. Кроме того, необходимо также включить для каждого реестра следующие параметры:

- **Включить операции поиска соответствий для реестра.** Выберите эту опцию, чтобы реестр мог применяться в операциях поиска соответствий EIM, независимо от того, определены ли в нем связи стратегий или нет.
- **Применять связи стратегий.** Выберите эту опцию, чтобы реестр мог выполнять роль целевого реестра связи стратегий и мог применяться в операциях поиска соответствий EIM.

Если вы не включите для реестра поиск соответствий, то реестр не будет применяться в операциях поиска соответствий EIM. Если вы не укажете, что реестр должен применять связи стратегий, то операции поиска соответствий EIM будут игнорировать связи стратегий, определенные в целевом реестре операции поиска.

Для того чтобы разрешить применение связей стратегий в целевом реестре, необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор EIM
- Администратор реестра
- Администратор выбранных реестров (для изменяемого реестра)

Для включения в целевом реестре поддержки поиска соответствий в общем и для разрешения применения связей стратегий в частности выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Выберите **Реестры пользователей**, чтобы просмотреть список определений реестров в домене.

   Примечание: Если у вас есть права доступа администратора к выбранным реестрам, то список будет содержать только те определения реестров, к которым у вас есть явно заданные права доступа.
4. Щелкните правой кнопкой мыши на определении реестра, для которого вы хотите включить поддержку стратегий преобразования и выберите пункт меню **Стратегия преобразования**
5. На странице **Общие** выберите опцию **Включить для реестра поиск соответствий**. Выбор этой опции разрешает применение реестра в операциях поиска соответствий EIM. Если эта опция не выбрана, то операция поиска не сможет вернуть данные для этого реестра, независимо от того, является ли он целевым или исходным реестром в этой операции.

6. Выберите опцию **Применять связи стратегий**. Выбор этой опции разрешает операциям поиска применять связи стратегий в качестве основы для возврата данных в том случае, если реестр является целевым реестром в операции поиска.
7. Для сохранения внесенных изменений нажмите **OK**.

Примечание: Для применения в реестре связей стратегий необходимо также включить применение связей стратегий в домене.

Понятия, связанные с данным

“Поддержка и активация стратегий преобразования EIM” на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

Удаление определения реестра

Удаление из домена преобразования идентификаторов в рамках предприятия (EIM)определения реестра не оказывает никакого влияния на реестр пользователей, на который ссылается это определение реестра, однако данный реестр пользователей больше не будет применяться в домене EIM.

При удалении определения реестра следует также учесть следующие особенности:

- При удалении определения реестра будут утрачены все связи с этим реестром пользователей. Если вы заново определите этот реестр в домене, то придется заново создавать все требуемые связи.
- При удалении определения реестра X.509 будут утрачены все определенные для этого реестра фильтры сертификатов. Если вы заново определите этот реестр X.509 в домене, то придется заново создавать все фильтры сертификатов.
- Если существуют определения реестров приложений, использующие в качестве родительского реестра системный реестр, то вы не сможете удалить определение этого системного реестра.

Для удаления определения реестра необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для удаления определения реестра EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Реестры пользователей**, чтобы просмотреть список определений реестров в домене.

   Примечание: Если у вас есть права доступа администратора к выбранным реестрам, то список будет содержать только те определения реестров, к которым у вас есть явно заданные права доступа.
5. Щелкните правой кнопкой мыши на удаляемом реестре пользователей и выберите пункт **Удалить**.
6. В окне **Подтверждение** нажмите кнопку **Да**, чтобы удалить определение реестра.

Удаление псевдонима из определения реестра

Для удаления псевдонима из определения реестра EIM необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа Администратора реестра, Администратора выбранных реестров или Администратора EIM.

Для того, чтобы удалить псевдоним для определения реестра EIM, выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Реестры пользователей**, чтобы просмотреть список определений реестров в домене.

   Примечание: Если у вас есть права доступа администратора к выбранным реестрам, то список будет содержать только те определения реестров, к которым у вас есть явно заданные права доступа.
5. Щелкните правой кнопкой мыши на определении реестра и выберите опцию **Свойства**.
6. Выберите страницу **Псевдоним**.
7. Выберите псевдоним и нажмите кнопку **Удалить**.
8. Нажмите кнопку **OK** для сохранения внесенных изменений.

Добавление элемента в групповое определение реестра

Для добавления элемента в групповое определение реестра необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа Администратора EIM, Администратора реестра, Администратора выбранных реестров (для группового определения реестра, к которому необходимо добавить элемент, и отдельного элемента, который необходимо добавить).

Для добавления элемента в групповое определение реестра, выполните следующие действия:

1. **Разверните узлы Сеть → EIM → Управление доменами.**
2. Выберите домен EIM, с которым вы планируете работать.
   a. Если необходимый домен EIM отсутствует в папке Управление доменами, то перейдите к разделу Добавление домена EIM в папку Управление доменами.
   b. Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. 4. Выберите **Реестры пользователей**, чтобы просмотреть список определений реестров в домене.
5. 5. Щелкните правой кнопкой мыши на групповом определении реестра, в которому следует добавить элемент, и выберите **Свойства**
6. 6. Выберите страницу **Элементы** и нажмите кнопку **Add**.
7. 7. В окне **Добавить элемент группового реестра EIM** выберите одно или несколько определений реестра и нажмите кнопку **OK**. Содержимое списка зависит от предоставленных вам прав доступа EIM, и ограничено определением реестра с тем же учетом регистра, что и у других элементов группы.
8. 8. Нажмите кнопку **OK** для выхода.

Управление идентификаторами EIM

Сведения о создании и управлении идентификаторами EIM для домена.

Создание и применение идентификаторов EIM, представляющих пользователей сети, может быть очень полезным для отслеживания пользователей, которым принадлежат те или иные идентификаторы. Список пользователей на предприятии часто меняется, так как одни сотрудники приходят, другие - увольняются, а третьи - переезжают из одного офиса в другой. Подобные изменения добавляют к остальным задачам администрирования отслеживание идентификаторов и паролей пользователей в других системах и приложениях сети. Кроме того, управление паролями пользователей предприятия занимает очень много времени. Путем создания идентификаторов EIM и связывания их с идентификаторами отдельных

пользователей вы можете организовать процесс выявления владельца каждого выбранного идентификатора пользователя. Такой подход существенно упрощает управление паролями.

Реализация среды с единым входом в систему также упрощает процедуры управления идентификаторами пользователей, особенно при переходе пользователей в другой отдел или в другой филиал предприятия. Функция единого входа в сеть избавляет пользователей от необходимости запоминать множество имен пользователей и паролей для новых систем.

Примечание: Способ создания и применения идентификаторов EIM определяется потребностями предприятия. Дополнительные сведения приведены в разделе “Разработка плана присвоения имен идентификаторам EIM” на стр. 65.

Вы можете управлять идентификаторами EIM из любого домена EIM, указанного в папке **Управление доменами**. Для управления идентификаторами EIM в домене EIM вы можете выполнять следующие задачи:

Информация, связанная с данной

Единый вход в систему

Создание идентификатора EIM

Для создания идентификатора EIM необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора идентификатора или администратора EIM.

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

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните правой кнопкой мыши на пункте **Идентификаторы** и выберите **Создать идентификатор**.
5. В окне диалога **Создать идентификатор EIM** укажите следующую информацию об идентификаторе EIM:
   a. Имя идентификатора
   b. Должна ли система при необходимости создавать уникальное имя
   c. Описание идентификатора
   d. Один или несколько псевдонимов для идентификатора, если это необходимо
6. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
7. После указания необходимой информации нажмите кнопку **OK** для создания идентификатора EIM.

Примечание: При наличии большого числа идентификаторов EIM отображение списка в папке **Идентификаторы** занимает довольно много времени. Для повышения производительности при наличии большого количества идентификаторов EIM обратитесь к разделу “Настройка окна Консоли управления” на стр. 104.

Добавление псевдонима для идентификатора EIM

Пользователь может создать псевдоним, задающий дополнительную отличительную информацию об идентификаторе EIM. 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. Например, если в системе есть два пользователя с именем Иванов И.И., то для того чтобы различить этих пользователей, одному из них можно присвоить псевдоним Иванов Иван Иванович, а другому - Иванов Илья Ильич. В дополнительных псевдонимах можно указывать номера пользователей, номера отделов, должности и т.п.

Для добавления псевдонима для идентификатора EIM необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор EIM
- Администратор идентификатора

Для добавления псевдонима для идентификатора EIM выполните следующие действия.

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните на значке **Идентификаторы** для просмотра списка доступных в домене идентификаторов EIM.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM обратитесь к разделу “Настройка окна Консоли управления” на стр. 104.
5. Щелкните правой кнопкой мыши на идентификаторе EIM, для которого вы хотите добавить псевдоним, и выберите пункт меню **Свойства...**.
6. В поле **Псевдоним** укажите псевдоним, который необходимо добавить к идентификатору EIM, и нажмите кнопку **Добавить**.
7. Для сохранения изменений, внесенных в идентификатор EIM, нажмите **OK**.

Удаление псевдонима идентификатора EIM

Для удаления псевдонима из определения реестра EIM необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа Администратора идентификатора или Администратора EIM.

Для удаления псевдонима идентификатора EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Щелкните на значке **Идентификаторы** для просмотра списка доступных в домене идентификаторов EIM.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM обратитесь к разделу “Настройка окна Консоли управления” на стр. 104.

5. Щелкните правой кнопкой мыши на идентификаторе EIM, для которого вы хотите добавить псевдоним, и выберите пункт меню **Свойства...**.
6. Выберите псевдоним и нажмите кнопку **Удалить**.
7. Для сохранения внесенных изменений нажмите **OK**.

Удаление идентификатора EIM

Для удаления идентификатора EIM необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора EIM.

Для удаления идентификатора EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку “Настройка окна Консоли управления”.
5. Выберите идентификатор EIM для удаления. Для удаления нескольких идентификаторов выберите их, удерживая нажатой клавишу **Ctrl**.
6. Щелкните правой кнопкой мыши на удаляемых идентификаторах и выберите пункт **Удалить**.
7. В окне **Подтвердить удаление** нажмите кнопку **Да** для удаления выбранных идентификаторов EIM.

Настройка окна Консоли управления

Иногда при попытке открыть папку Идентификаторы отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку Идентификаторы, ограничив условия поиска отображаемых записей.

Для настройки представления папки **Идентификаторы** выполните следующие действия:

1. Разверните узлы **Сеть —> Преобразование идентификаторов в рамках предприятия —> Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Щелкните правой кнопкой мыши на папке **Идентификаторы** и выберите пункт меню **Настроить это представление**.
4. Укажите условия отображения идентификаторов EIM в домене. Для сокращения числа показанных идентификаторов EIM укажите символы, которые должны применяться для сортировки идентификаторов. В указанной строке может присутствовать один или несколько символов подстановки (*). Например, в поле **Идентификаторы** в качестве условия сортировки можно указать значение `*JOHNSON*`. В результате будут показаны все идентификаторы EIM, в которых в имени или псевдонима идентификатора EIM присутствует строка `JOHNSON`.
5. Для сохранения внесенных изменений нажмите **OK**.

Управление связями EIM

EIM позволяет создавать два вида связей, определяющих прямую или косвенную взаимосвязь между идентификаторами пользователей: связи идентификаторов и связи стратегий. EIM позволяет позволяет создавать и обслуживать связи идентификаторов между идентификаторами EIM идентификаторами пользователей, что позволяет определять косвенное, но точное соответствие между идентификаторами пользователей.

EIM также позволяет создавать связи стратегий, описывающие взаимозависимость между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM. Поскольку оба типа связей определяют взаимосвязь между идентификаторами пользователей предприятия, то управление связями является важным элементом управления EIM.

Создание и сохранение связей в домене значительно упрощает выполнение задач администрирования, предназначенных для отслеживания учетных записей пользователей в различных системах сети. Для применения функции единого защищенного входа в сеть необходимо поддерживать актуальное состояние связей стратегий и связей идентификаторов.

Вы можете выполнять следующие задачи управления связями:

Создание связей EIM

Существует два типа связей EIM, которые вы можете создавать. Вы можете создавать связь идентификаторов или связь стратегий.

Вы можете создать связь идентификаторов, косвенно определив взаимосвязь между двумя идентификаторами одного пользователя. Связь идентификаторов описывает связь между идентификатором EIM и идентификатором пользователя в реестре пользователей. Связи идентификаторов позволяют задавать однозначное соответствие между идентификатором EIM и всеми остальными идентификаторами того пользователя, которого представляет данный идентификатор EIM.

Вы можете создать связь стратегий, непосредственно определяющую взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM. Связи стратегий позволяют быстро создавать большое количество связей между идентификаторами пользователей из различных реестров.

Применение связей идентификаторов, связей стратегий или комбинации этих двух связей определяется требованиями к конкретной реализации EIM.

Понятия, связанные с данным

“Разработка плана преобразования идентификаторов” на стр. 62
Критически важным компонентом процесса первоначального планирования EIM является определения способа применения технологии преобразования идентификаторов на вашем предприятии.

Создание связей идентификаторов EIM:

Связь идентификаторов описывает связь между идентификатором преобразования идентификаторов в рамках предприятия EIM и идентификатором пользователя или объекта, которому соответствует этот идентификатор EIM.

Существует три типа связей идентификаторов: целевая, исходная и административная. Во избежание возникновение неполадок связей и преобразования идентификаторов обратитесь к разделу “Разработка плана преобразования идентификаторов” на стр. 62.

Для создания связи идентификаторов необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа, соответствующие типу создаваемой связи.

Для создания исходной или административной связи необходим один из следующих уровней прав доступа EIM:

- Администратор идентификатора
- Администратор EIM

Для создания целевой связи необходим один из следующих уровней прав доступа EIM:

- Администратор реестра
- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя).
- Администратор EIM

Для создания связи идентификаторов выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу “Подключение к домену EIM” на стр. 90.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**, чтобы просмотреть список идентификаторов EIM в домене.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM обратитесь к разделу “Настройка окна Консоли управления” на стр. 104.
5. Щелкните правой кнопкой мыши на идентификаторе EIM, для которого вы хотите создать связь, и выберите пункт меню **Свойства...**.
6. Перейдите на страницу **Связи** и нажмите кнопку **Добавить...**.
7. В окне **Добавить связь** укажите информацию, определяющую данную связь:
   - Имя реестра, в котором хранится идентификатор пользователя, связываемый с идентификатором EIM. Укажите точное имя существующего определения реестра или выберите нужное имя из списка.
   - Идентификатор пользователя, связываемый с идентификатором EIM.
   - Тип связи. Можно создавать связи следующих типов:
     – Административные связи
     – Исходные связи
     – Целевые связи
8. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
9. Необязательно. При определении целевой связи нажмите кнопку **Дополнительно...** Появится окно диалога **Добавить связь - Дополнительно**. Укажите для целевого идентификатора пользователя информацию для поиска и нажмите **OK** для возврата к окну **Добавить связь**.
10. После указания необходимой информации нажмите кнопку **OK** для создания связи.

Создание связи стратегий:

Связь стратегий непосредственно определяет взаимосвязь между несколькими идентификаторами пользователей в одном или нескольких реестрах, и отдельным целевым идентификатором пользователя в другом реестре.

Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM. Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед их созданием и применением необходимо внимательно изучить поддержку стратегий преобразования. Кроме того, во избежание возникновения неполадок связей и преобразования идентификаторов необходимо заранее, до начала создания связей, разработать для предприятия общий план преобразования идентификаторов.

Применение связей идентификаторов, связей стратегий или комбинации этих двух связей определяется требованиями к конкретной реализации EIM.

Способ создания связи стратегий зависит от типа связи. Дополнительные сведения о создании различных связей стратегий приведены в следующих разделах:

Понятия, связанные с данным

"Управление определениями реестров EIM" на стр. 95
Для применения в домене EIM реестров пользователей и находящихся в них идентификаторов пользователей необходимо создать определения реестров для этих реестров. После этого с помощью созданных определений реестров вы сможете управлять применением этих реестров пользователей и входящих в их состав идентификаторов пользователей EIM.

"Поддержка и активация стратегий преобразования EIM" на стр. 38
Поддержка стратегий соответствия EIM позволяет применять в домене EIM как связи стратегий, так и связи отдельных идентификаторов. Связи стратегий могут применяться как вместо связей идентификаторов, так и в сочетании с ними.

"Разработка плана преобразования идентификаторов" на стр. 62
Критически важным компонентом процесса первоначального планирования EIM является определения способа применения технологии преобразования идентификаторов на вашем предприятии.

Создание связи стратегии домена по умолчанию:

Для создания связи стратегии домена по умолчанию необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора реестра или администратора EIM.

Связь стратегий описывает взаимосвязь между несколькими идентификаторами пользователей и одним идентификатором пользователя в целевом реестре. Связи стратегий могут применяться для связывания исходного набора идентификаторов пользователей с одним-единственным целевым идентификатором пользователя, находящимся в заданном целевом реестре пользователей. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM.

Примечание: Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед их созданием и применением необходимо внимательно изучить поддержку стратегий преобразования. Кроме того, во избежание возникновение неполадок связей и преобразования идентификаторов необходимо заранее, до начала создания связей, разработать для предприятия общий план преобразования идентификаторов.

В связи стратегий домена по умолчанию все пользователи домена являются исходными записями для преобразования, которые соответствуют одному целевому реестру и целевому идентификатору пользователя. Связь стратегии домена по умолчанию можно определить для каждого реестра в домене. Если на один и тот же целевой реестр указывает несколько связей стратегий домена, то можно определить для каждой из таких связей уникальную информацию для поиска, позволяющую операциям поиска различать эти связи. В противном случае операция поиска может вернуть несколько целевых

идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.

Для создания связи стратегий домена по умолчанию выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Стратегия преобразования**
   - Если нужный домен EIM не указан в папке **Управление доменами**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Выберите опцию **Включить поиск соответствия с помощью связей стратегий для домена** на странице Общие.
4. Перейдите на страницу **Домен** и нажмите кнопку **Добавить**.
5. В окне **Добавить связь стратегии домена по умолчанию** укажите следующую обязательную информацию:
   - Имя определения **Целевого реестра** для создаваемой связи стратегий.
   - Идентификатор **Целевого пользователя** для создаваемой связи стратегий.
6. Для просмотра сведений о работе с этим и последующими окнами диалогов нажмите кнопку **Справка**.
7. Необязательно. Нажмите кнопку **Дополнительно**. Появится окно **Добавить связь - Дополнительно**. Укажите для связи стратегий **Информацию для поиска** и нажмите **OK** для возврата к окну **Добавить связь стратегий домена по умолчанию**.

   Примечание: Если на один и тот же целевой реестр указывает несколько связей с одним и тем же исходным реестром, то необходимо определить для каждого целевого идентификатора таких связей уникальную информацию для поиска. Тем самым вы сможете гарантировать, что операции поиска соответствий смогут различать требуемые целевые идентификаторы пользователей. В противном случае операция поиска может вернуть несколько целевых идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.
8. Для создания новой связи стратегий и возврата к странице **Домен** нажмите кнопку **OK**. Новая связь стратегий будет показана в таблице **Связи стратегий по умолчанию**.
9. Убедитесь, что новая связь стратегий включена в целевом реестре.
10. Нажмите **OK** для сохранения внесенных изменений и выхода из окна **Стратегия преобразования**.

Примечание: Убедитесь, что в целевом реестре пользователей включена поддержка стратегий преобразования и связей стратегий. Если соответствующие опции отключены, то связь стратегий применяться не будет.

Создание связи стратегии реестра по умолчанию:

Для создания связи стратегии реестра по умолчанию необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора реестра или администратора EIM.

Связь стратегий описывает взаимосвязь между несколькими идентификаторами пользователей и одним идентификатором пользователя в целевом реестре. Связи стратегий могут применяться для связывания исходного набора идентификаторов пользователей с одним-единственным целевым идентификатором пользователя, находящимся в заданном целевом реестре пользователей. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM.

Примечание: Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед их созданием и применением необходимо внимательно изучить поддержку стратегий преобразования. Кроме того, во избежание возникновения неполадок связей и преобразования идентификаторов необходимо заранее, до начала создания связей, разработать для предприятия общий план преобразования идентификаторов.

В связи стратегий реестра по умолчанию все пользователи реестра являются исходными записями для преобразования, которые соответствуют одному целевому реестру и целевому идентификатору пользователя. Включив для целевого реестра связь стратегий реестра по умолчанию, вы тем самым гарантируете возможность преобразования всех исходных идентификаторов пользователей в один заданный целевой идентификатор из целевого реестра.

Для создания связи стратегий реестра по умолчанию выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Выберите опцию **Включить поиск соответствия с помощью связей стратегий для домена** на странице Общие.
4. Выберите опцию **Включить поиск соответствия с помощью связей стратегий для домена** на странице Общие.
5. В окне **Добавить связь стратегии реестра по умолчанию** укажите следующую обязательную информацию:
   - Имя определения **Исходного реестра** для создаваемой связи стратегий.
   - Имя определения **Целевого реестра** для создаваемой связи стратегий.
   - Идентификатор **Целевого пользователя** для создаваемой связи стратегий.
6. Для просмотра сведений о работе с этим и последующими окнами диалогов нажмите кнопку **Справка**.
7. Необязательно. Нажмите кнопку **Дополнительно**. Появится окно **Добавить связь - Дополнительно**. Укажите для связи стратегий **Информацию для поиска** и нажмите **OK** для возврата к окну **Добавить связь стратегий реестра по умолчанию**. Если на один и тот же целевой реестр указывает несколько связей стратегий с одним и тем же исходным реестром, то необходимо определить для каждого целевого идентификатора таких связей уникальную информацию для поиска. Тем самым вы сможете гарантировать, что операции поиска соответствий смогут различать требуемые целевые идентификаторы пользователей. В противном случае операция поиска может вернуть несколько целевых идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.
8. Для создания новой связи стратегий и возврата к странице **Реестр** нажмите кнопку **OK**. Новая связь будет показана в окне **Связи стратегий по умолчанию**.
9. Убедитесь, что новая связь стратегий включена в целевом реестре.
10. Нажмите **OK** для сохранения внесенных изменений и выхода из окна **Стратегия преобразования**.

Примечание: Убедитесь, что в целевом реестре пользователей включена поддержка стратегий преобразования и связей стратегий. Если соответствующие опции отключены, то связь стратегий применяться не будет.

Создание связи стратегии фильтра сертификатов:

Для создания связи стратегии фильтра сертификатов необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора реестра или администратора EIM.

Связи стратегий позволяет установить соответствие между исходным набором идентификаторов пользователей и одним-единственным целевым идентификатором пользователя, находящимся в заданном целевом реестре пользователей. Связи стратегий используют поддержку стратегий преобразования EIM для установления многозначных (несколько с одним) соответствий между идентификаторами пользователей без применения идентификатора EIM.

Примечание: Поскольку связи стратегий могут применяться в самых разных сочетаниях, то перед их созданием и применением необходимо внимательно изучить поддержку стратегий преобразования. Кроме того, во избежание возникновения неполадок связей и преобразования идентификаторов необходимо заранее, до начала создания связей, разработать для предприятия общий план преобразования идентификаторов.

В связи стратегий фильтров сертификатов вы должны указать в качестве источника связи стратегий набор сертификатов из одного реестра X.509. Эти сертификаты связываются с единым указанным целевым реестром и целевым пользователем. В отличие от связи стратегий реестра по умолчанию, в которой источником связи стратегий являются все пользователи одного реестра, связи стратегий фильтров сертификатов характеризуются более гибкой областью применения. В качестве источника можно указать подмножество сертификатов из реестра. Область действия определяется заданным для связи стратегий фильтром сертификатов.

Примечание: Если необходимо связать все сертификаты, находящиеся в одном реестре пользователей X.509, с одним целевым идентификатором пользователя, то следует создать связь стратегии реестра по умолчанию.

Фильтр сертификатов задает способ установления соответствия между набором исходных идентификаторов пользователей (в данном случае - цифровых сертификатов) и заданным целевым идентификатором пользователя. Таким образом, применяемый фильтр сертификатов должен уже существовать к моменту создания связи стратегии фильтра сертификатов.

Перед созданием связи стратегии фильтра сертификатов необходимо сначала создать фильтр сертификатов, который будет применяться в качестве основного компонента этой связи.

Для создания связи стратегии фильтра сертификатов выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Стратегия преобразования**
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Выберите опцию **Включить поиск соответствия с помощью связей стратегий для домена** на странице Общие.
4. Перейдите на страницу **Фильтр сертификатов** и нажмите кнопку **Добавить** Будет показано окно **Добавить связь стратегии фильтра сертификатов**.
5. Для просмотра сведений о работе с этим и последующими окнами диалогов нажмите кнопку **Справка**.
6. Для определения связи стратегии необходимо указать следующую обязательную информацию:
   a. Укажите имя определения реестра пользователей X.509, которое будет применяться в данной связи в качестве **Исходного реестра X.509**. Вы также можете нажать кнопку **Обзор** и выбрать нужное имя из списка определений реестров домена
   b. Нажмите кнопку **Выбрать**. Будет показано окно диалога **Выбрать фильтр сертификатов**, в котором вы сможете выбрать существующий фильтр сертификатов для применения в качестве основы для новой связи стратегии фильтра сертификатов.

Примечание: **Обязательно** воспользуйтесь уже существующим фильтром сертификатов. Если фильтр сертификатов, который вы хотите использовать, не указан в списке, то нажмите кнопку **Добавить** и создайте новый фильтр сертификатов.

c. Укажите имя определения **Целевого реестра** или нажмите кнопку **Обзор** и выберите определение в списке существующих определений реестров домена.

d. Укажите имя **Целевого пользователя**, с которым должны быть связаны все сертификаты **Исходного реестра X.509**, соответствующие фильтру сертификатов. Вы также можете нажать кнопку **Обзор** и выбрать нужное имя из списка пользователей домена.

e. Необязательно. Нажмите кнопку **Дополнительно**. Появится окно **Добавить связь - Дополнительно**. Укажите для целевого идентификатора пользователя **Информацию для поиска** и нажмите **OK** для возврата к окну **Добавить связь стратегии фильтра сертификатов**.

Примечание: Если на один и тот же целевой реестр указывает несколько связей стратегий с одним и тем же исходным реестром X.509 и с одинаковыми условиями фильтрации сертификатов, то необходимо определить для каждого целевого идентификатора пользователя таких связей уникальную информацию для поиска. Тем самым вы сможете гарантировать, что операции поиска соответствий смогут различать требуемые целевые идентификаторы пользователей. В противном случае операция поиска может вернуть несколько целевых идентификаторов пользователей. Получив такой неоднозначный результат, использующее EIM приложение не сможет точно выбрать необходимый целевой идентификатор пользователя.

7. Для создания связи стратегии фильтра сертификатов и возврата к странице **Фильтр сертификатов** нажмите кнопку **OK**. Новая связь будет показана в списке.
8. Убедитесь, что новая связь стратегий включена в целевом реестре.
9. Нажмите **OK** для сохранения внесенных изменений и выхода из окна **Стратегия преобразования**.

Примечание: Убедитесь, что в целевом реестре пользователей включена поддержка стратегий преобразования и связей стратегий. Если соответствующие опции отключены, то связь стратегий применяться не будет.

Создание фильтра сертификатов:

Фильтр сертификатов определяет набор схожих атрибутов сертификатов отличительных имен для группы сертификатов пользователей из исходного реестра пользователей X.509. Фильтр сертификатов можно использовать в качестве основы для связи стратегий фильтров сертификатов.

Фильтр сертификатов в связи стратегий определяет, какие сертификаты из указанного исходного реестра X.509 должны быть связаны с заданным целевым пользователем. При выполнении операций поиска соответствия преобразования идентификаторов в рамках предприятия (EIM) сертификаты, в которых информация DN субъекта и DN издателя соответствует параметрам фильтра, связываются с указанным целевым пользователем.

Для создания фильтра сертификатов необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор EIM
- Администратор реестра
- Администратор выбранных реестров (для определения реестра, ссылающегося на реестр пользователей X.509, для которого вы создаете фильтр сертификатов)

Фильтр сертификатов создается на основе указанной в цифровом сертификате информации об отличительном имени (DN). Информация о DN может представлять собой либо отличительное имя

субъекта, обозначающее владельца сертификата, либо отличительное имя подписавшей организации, обозначающее организацию, выдавшую данный сертификат. В фильтре сертификатов может указываться как полная, так и частичная информация о DN.

Фильтр сертификатов, добавляемый к связи стратегии сертификатов, указывает, какие сертификаты из реестра X.509 преобразуются в целевой идентификатор пользователя, заданный в связи стратегии. Если в операции поиска соответствия EIM исходным идентификатором пользователя является цифровой сертификат (после вызова в приложении API EIM `eimFormatUserIdentity()` для форматирования идентификатора пользователя) и применяется связь стратегий фильтров сертификатов, то EIM сравнит информацию о DN из сертификата с полной или частичной информацией о DN, указанной в фильтре. Если информация о DN в сертификате соответствует фильтру, то EIM вернет целевой идентификатор пользователя, соответствующий связи стратегий фильтра сертификатов.

При создании фильтра сертификатов информацию об отличительном имени можно указать одним из следующих способов:

- Укажите в поле **DN субъекта** или **DN сертификатной компании** полное или частичное DN сертификата.
- Скопируйте в буфер обмена информацию из какого-либо сертификата и воспользуйтесь ей для создания списка возможных фильтров, основанного на содержащейся в сертификате информации об отличительном имени. После этого вы сможете выбрать DN для применения в фильтре сертификатов.

  Примечание: Если вы хотите создать фильтр сертификатов на основании сформированной обязательной информации об отличительном имени, то перед выполнением этой задачи скопируйте информацию из сертификата в буфер обмена. Сертификат должен быть в формате base64. Более подробная информация о способах получения сертификата в требуемом формате приведена в разделе Фильтр сертификатов.
- Сформируйте список возможных фильтров сертификатов на основании информации от отличительном имени из цифрового сертификата, для которого существует исходная связь с идентификатором EIM. После этого вы сможете выбрать DN для применения в фильтре сертификатов.

Для создания связи стратегии фильтра сертификатов, применяемого в качестве основы связи стратегии фильтра сертификатов, выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Стратегия преобразования**
   - Если нужный домен EIM не указан в папке **Управление доменами**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Перейдите на страницу **Фильтр сертификатов** и нажмите кнопку **Добавить** Будет показано окно **Фильтры сертификатов**.

   Примечание: Если вы перейдете на страницу **Фильтр сертификатов**, не выбрав связь стратегий, то появится окно **Просмотреть реестры EIM**. Это окно позволяет выбрать в списке определение реестра X.509, для которого необходимо просмотреть фильтры сертификатов. Содержимое списка зависит от предоставленных вам прав доступа EIM.
4. Нажмите кнопку **Добавить**. Будет показано окно **Добавить фильтр сертификатов**.
5. В окне **Добавить фильтр сертификатов** необходимо указать, будете ли вы добавлять один фильтр сертификатов или создавать фильтр на основе конкретных цифровых сертификатов. Для просмотра сведений о работе с этим и последующими окнами диалогов нажмите кнопку **Справка**.
   a. Если вы выбрали опцию **Добавить отдельный фильтр сертификатов**, то вы сможете указать полное или частичное **DN субъекта** и/или полное или частичное **DN сертификатной компании**. Для создания фильтра сертификатов и возврата к странице **Реестр** нажмите кнопку **OK**. Фильтр будет показан в списке.

b. Если вы выбрали опцию **Создать фильтр сертификата на основе сертификата**, то нажмите кнопку **OK** для перехода к окну **Генерировать фильтры сертификатов**.
   1) В поле **Информация о сертификате** вставьте из буфера обмена информацию о сертификате в формате base64.
   2) Нажмите кнопку **OK** для генерации списка возможных фильтров сертификатов на основании значений **DN субъекта** и **DN сертификатной компании**.
   3) В окне **Просмотр фильтров сертификатов** выберите один или несколько фильтров. Нажмите **OK** для возврата к окну **Выбрать фильтры сертификатов**, в котором теперь будут показаны выбранные фильтры сертификатов.

c. Если вы выбрали опцию **Создать фильтр сертификатов на основе исходной связи пользователя X.509**, то нажмите кнопку **OK** для перехода к окну **Генерировать фильтры сертификатов**. В этом окне показан список идентификаторов пользователей X.509, имеющих исходную связь с идентификатором EIM.
   1) Выберите идентификатор пользователя X.509, цифровым сертификатом которого вы хотите воспользоваться для генерации одного или нескольких возможных фильтров сертификатов и нажмите кнопку **OK**.
   2) Нажмите кнопку **OK** для генерации списка возможных фильтров сертификатов на основании значений **DN субъекта** и **DN сертификатной компании**.
   3) В окне **Просмотр фильтров сертификатов** выберите один или несколько предложенных фильтров. Нажмите **OK** для возврата к окну **Выбрать фильтры сертификатов**, в котором теперь будут показаны выбранные фильтры сертификатов.

Теперь вы можете воспользоваться новым фильтром сертификатов в качестве основы для создания связи стратегии фильтра сертификатов.

Добавление информации для поиска в целевой идентификатор пользователя

Информация для поиска - это необязательные уникальные идентификационные данные целевого идентификатора пользователя, определенного в связи. При этом может использоваться как целевая связь идентификатора, так и связь стратегий.

Информация для поиска необходима лишь в том случае, если операции поиска соответствий могут возвращать несколько целевых идентификаторов пользователей. Такая ситуация может привести к возникновению ошибок в приложениях с поддержкой EIM, в том числе в продуктах и приложениях i5/OS, которые не могут применять подобные неоднозначные результаты поиска.

При необходимости вы можете добавить уникальную информацию для поиска в каждый целевой идентификатор, обеспечив тем самым более точную идентификацию и подробное описание каждого целевого идентификатора пользователя. Если вы определили в целевом идентификаторе пользователя информацию для поиска, то эта информация обязательно должна указываться в операциях поиска соответствий, что позволит гарантировать возврат уникального целевого идентификатора пользователя. В противном случае приложение, использующее EIM, не сможет точно выбрать необходимый целевой идентификатор пользователя.

Примечание: Если вы не хотите, чтобы операции поиска EIM возвращали несколько целевых идентификаторов пользователей, то вместо поиска информации, позволяющей обойти эту ситуацию, можно изменить конфигурацию связей EIM. Подробная информация приведена в разделе “Устранение неполадок записей соответствия EIM” на стр. 126.

Способ добавления информации для поиска, позволяющей более точно определить целевой идентификатор, зависит от того, определен ли целевой идентификатор пользователя в связи идентификаторов или в целевой связи. Независимо от способа добавления информации для поиска, указываемая информация тесно связывается с целевым идентификатором пользователя, а не со связями идентификаторов или стратегий, в которых находится этот идентификатор.

Добавление информации для поиска в целевой идентификатор пользователя в связи идентификаторов:

Для выполнения этой задачи необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор реестра.
- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя).
- Администратор EIM.

Для того чтобы добавить информацию для поиска в целевой идентификатор пользователя в связи идентификаторов выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**, чтобы просмотреть список идентификаторов EIM в домене.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку **Идентификаторы**, ограничив условия поиска отображаемых записей. Щелкните правой кнопкой мыши на папке **Идентификаторы**, выберите опцию **Настроить это представление > Включить** и укажите условия поиска включаемых в представление идентификаторов EIM.
5. Щелкните правой кнопкой мыши на идентификаторе EIM и выберите **Свойства**.
6. Выберите страницу **Связи**, выберите целевую связь, в которую необходимо добавить информацию для поиска, и нажмите кнопку **Сведения**. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
7. В окне **Связь - Сведения** укажите **Информацию для поиска**, которая должна применяться для более точного указания целевого идентификатора пользователя в данной связи, а затем нажмите кнопку **Добавить**.
8. Повторите этот шаг для каждой записи информации для поиска, которую необходимо добавить в эту связь.
9. Для сохранения внесенных изменений и возврата к окну **Связи - Сведения** нажмите кнопку **OK**.
10. Нажмите кнопку **OK** для выхода.

Добавление информации для поиска в целевой идентификатор пользователя в связи стратегий:

Для выполнения этой задачи необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор реестра.
- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя).
- Администратор EIM.

Для того чтобы добавить информацию для поиска в целевой идентификатор пользователя в связи стратегий выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.

2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. В окне **Стратегия преобразования** вы можете просмотреть связи стратегий для домена.
4. Найдите и выберите связь стратегий для целевого реестра, содержащего целевой идентификатор пользователя, в который необходимо добавить информацию для поиска.
5. Нажмите кнопку **Сведения**. Будет показано окно **Связь стратегий - Сведения**, соответствующее выбранному типу связи стратегий. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
6. Укажите **Информацию для поиска**, которая должна применяться для более точного указания целевого идентификатора пользователя в данной связи стратегий, а затем нажмите кнопку **Добавить**. Повторите этот шаг для каждой записи информации для поиска, которую необходимо добавить в эту связь.
7. Для сохранения внесенных изменений и возврата к окну **Связи стратегий - Сведения** нажмите кнопку **OK**.
8. Нажмите кнопку **OK** для выхода.

Удаление информации для поиска из целевого идентификатора пользователя

Информация для поиска - это необязательные уникальные идентификационные данные целевого идентификатора пользователя, определенного в связи. При этом может использоваться как целевая связь идентификатора, так и связь стратегий.

Информация для поиска необходима лишь в том случае, если операции поиска соответствий могут возвращать несколько целевых идентификаторов пользователей. Такая ситуация может привести к возникновению ошибок в приложениях с поддержкой EIM, в том числе в продуктах и приложениях i5/OS, которые не могут применять подобные неоднозначные результаты поиска.

Информация для поиска обязательно должна указываться в операциях поиска соответствий для обеспечения возврата уникального целевого идентификатора пользователя. Однако, если определенная ранее информация для поиска больше не требуется, то вы можете удалить ее, после чего эту информацию больше не нужно будет указывать в операциях поиска соответствий.

Способ удаления информации для поиска, зависит от того, определен ли целевой идентификатор пользователя в связи идентификаторов или в целевой связи. Информация для поиска задается для целевого идентификатора пользователя, а не для связей идентификаторов и не для связей стратегий, в которых упоминается этот идентификатор пользователя. Таким образом, при удалении последней связи идентификаторов или связи стратегий, ссылающейся на этот целевой идентификатор пользователя, из домена EIM удаляется как сам идентификатор пользователя, так и заданная для него информация для поиска.

Удаление информации для поиска из целевого идентификатора пользователя в связи идентификаторов:

Для выполнения этой задачи необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор реестра
- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя)
- Администратор EIM

Для того чтобы удалить информацию для поиска из целевого идентификатора пользователя в связи идентификаторов выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.

2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**, чтобы просмотреть список идентификаторов EIM в домене.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку **Идентификаторы**, ограничив условия поиска отображаемых записей. Щелкните правой кнопкой мыши на папке **Идентификаторы**, выберите опцию **Настроить это представление > Включить** и укажите условия поиска включаемых в представление идентификаторов EIM.
5. Щелкните правой кнопкой мыши на идентификаторе EIM и выберите **Свойства**.
6. Выберите страницу **Связи**, выберите целевую связь, из которой необходимо удалить информацию для поиска, и нажмите кнопку **Сведения**.
7. В окне **Связь - Сведения** выберите информацию для поиска, которую необходимо удалить из целевого идентификатора пользователя, и нажмите кнопку **Удалить**.

   Примечание: При нажатии кнопки **Удалить** подтверждение не запрашивается.
8. Для сохранения внесенных изменений и возврата к окну **Связи - Сведения** нажмите кнопку **OK**.
9. Нажмите кнопку **OK** для выхода.

Удаление информации для поиска из целевого идентификатора пользователя в связи стратегий:

Для выполнения этой задачи необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть права доступа “Управление доступом EIM” на стр. 39 одного из следующих уровней:

- Администратор реестра
- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя).
- Администратор EIM

Для того чтобы удалить информацию для поиска из целевого идентификатора пользователя в связи стратегий выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. В окне **Стратегия преобразования** вы можете просмотреть связи стратегий для домена.
4. Найдите и выберите связь стратегий для целевого реестра, содержащего целевой идентификатор пользователя, из которого необходимо удалить информацию для поиска.
5. Нажмите кнопку **Сведения**. Будет показано окно **Связь стратегий - Сведения**, соответствующее выбранному типу связи стратегий.
6. Выберите информацию для поиска, которую необходимо удалить из целевого идентификатора пользователя, и нажмите кнопку **Удалить**.

   Примечание: При нажатии кнопки **Удалить** подтверждение не запрашивается.

7. Для сохранения внесенных изменений и возврата к окну **Связи стратегий - Сведения** нажмите кнопку **OK**.
8. Нажмите кнопку **OK** для выхода.

Просмотр всех связей идентификатора EIM

Для просмотра всех связей идентификатора EIM необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть необходимые права доступа.

Просматривать все связи можно с любым уровнем доступа, за исключением Администратора выбранных реестров. Такой уровень доступа позволяет просматривать только те связи реестров, к которым у вас есть явно заданные права доступа (если вам не предоставлены права доступа на управление операциями поиска соответствий EIM).

Для просмотра всех связей между идентификатором EIM и идентификаторами пользователей, для которых определены связи, выполните следующие действия:

Для просмотра связей идентификатора выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**, чтобы просмотреть список идентификаторов EIM в домене.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку **Идентификаторы**, ограничив условия поиска отображаемых записей. Щелкните правой кнопкой мыши на папке **Идентификаторы**, выберите опцию **Настроить это представление > Включить** и укажите условия поиска включаемых в представление идентификаторов EIM.
5. Выберите идентификатор EIM, щелкните на нем правой кнопкой мыши и нажмите кнопку **Свойства**.
6. Для просмотра списка идентификаторов пользователей, связанных с идентификатором EIM, выберите страницу **Связи**.
7. Для завершения нажмите кнопку **Готово**.

Просмотр всех связей стратегии для домена

Для просмотра всех связей стратегий какого-либо конкретного домена необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть необходимые права доступа.

Просматривать все связи стратегий можно с любым уровнем доступа, за исключением Администратора выбранных реестров. Такой уровень доступа позволяет просматривать только те связи реестров, к которым у вас есть явно заданные права доступа. В результате, имея такой уровень доступа, вы не можете просматривать связи стратегий домена по умолчанию (если у вас нет также прав доступа на управление операциями поиска соответствий EIM).

Для просмотра всех связей стратегий домена выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Стратегия преобразования**.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.

- Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.

3. Выберите страницу связей стратегий домена:
   a. Для просмотра определенных в домене связей стратегий домена по умолчанию и сведений о том, включены ли эти связи на уровне реестра, выберите страницу **Домен**.
   b. Для просмотра определенных в домене связей стратегий реестров по умолчанию выберите страницу **Реестр**. Вы также можете просматривать исходные и целевые реестры, на которые влияют эти связи.
   c. Для просмотра определенных и включенных на уровне реестра связей стратегий фильтров сертификатов выберите страницу **Фильтр сертификата**.
4. Для завершения нажмите кнопку **Готово**.

Просмотр всех связей стратегий для определения реестра

Для просмотра всех связей стратегий какого-либо конкретного реестра необходимо наличие соединения с доменом EIM, в котором вы планируете работать, а у вас должны быть необходимые права доступа.

Просматривать все связи стратегий можно с любым уровнем доступа, за исключением Администратора выбранных реестров. Такой уровень доступа позволяет просматривать только те связи реестров, к которым у вас есть явно заданные права доступа. В результате, имея такой уровень доступа, вы не можете просматривать связи стратегий домена по умолчанию (если у вас нет также прав доступа на управление операциями поиска соответствий EIM).

Для просмотра всех связей стратегий для определения реестра выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Щелкните правой кнопкой мыши на нужном определении реестра и выберите пункт **Стратегия преобразования**.
4. Выберите страницу связей стратегий для выбранного определения реестра:
   - Для просмотра определенных в реестре связей стратегий домена по умолчанию выберите страницу **Домен**.
   - Для просмотра определенных и включенных в реестре связей реестров по умолчанию выберите страницу **Реестр**.
   - Для просмотра определенных и включенных в реестре связей стратегий фильтров сертификатов выберите страницу **Фильтр сертификата**.
5. Для завершения нажмите кнопку **Готово**.

Удаление связи идентификатора

Для удаления связи идентификатора необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа, соответствующие типу удаляемой связи.

Для удаления исходной или административной связи необходим один из следующих уровней прав доступа EIM:

- Администратор идентификатора
- Администратор EIM

Для удаления целевой связи необходим один из следующих уровней прав доступа EIM:

- Администратор реестра

- Администратор выбранных реестров (для определения реестра, который ссылается на реестр пользователей, содержащий целевой идентификатор пользователя)
- Администратор EIM

Для удаления связи идентификатора выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Разверните домен EIM, с которым было установлено соединение.
4. Выберите **Идентификаторы**, чтобы просмотреть список идентификаторов EIM в домене.

   Примечание: Иногда при попытке открыть папку **Идентификаторы** отображение списка идентификаторов может занять довольно продолжительное время. Для повышения производительности при наличии в домене большого количества идентификаторов EIM можно настроить папку **Идентификаторы**, ограничив условия поиска отображаемых записей. Щелкните правой кнопкой мыши на папке **Идентификаторы**, выберите опцию **Настроить это представление > Включить** и укажите условия поиска включаемых в представление идентификаторов EIM.
5. Выберите идентификатор EIM, щелкните на нем правой кнопкой мыши и нажмите кнопку **Свойства**.
6. Для просмотра списка идентификаторов пользователей, связанных с идентификатором EIM, выберите страницу **Связи**.
7. Выберите связь для удаления.

   Примечание: При нажатии кнопки **Удалить** подтверждение не запрашивается.
8. Для сохранения внесенных изменений нажмите **OK**.

Примечание: При отсутствии в целевом реестре других связей (связей стратегий или идентификаторов) все операции поиска соответствия в целевом реестре, использующие удаленную связь, будут возвращать пустой набор результатов.

Единственный способ создания в идентификатора пользователя в EIM заключается в его создании в процессе создания связи идентификатора или связи стратегий. Таким образом, при удалении последней целевой связи идентификатора пользователя (как путем удаления отдельных целевых связей, так и путем удаления связи стратегий) этот идентификатор пользователя больше не будет определен в EIM. В результате идентификатор пользователя и вся его информация для поиска будут утрачены.

Удаление связи стратегии

Для удаления связи стратегии необходимо наличие соединения с доменом EIM, с которым вы планируете работать, а у вас должны быть права доступа администратора реестра или администратора EIM.

Для удаления связи стратегии выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.
3. Выберите страницу, соответствующую типу удаляемой связи стратегии.
4. На этой странице выберите удаляемую связь стратегий и нажмите кнопку **Удалить**.

Примечание: При нажатии кнопки **Удалить** подтверждение не запрашивается.

5. Для выхода из окна **Управление стратегиями** и сохранения внесенных изменений нажмите кнопку **OK**.

Примечание: При отсутствии в целевом реестре других связей (связей стратегий или идентификаторов) все операции поиска соответствия в целевом реестре, использующие удаленную связь стратегий, будут возвращать пустой набор результатов.

Единственный способ создания в идентификатора пользователя в EIM заключается в его создании в процессе создания связи идентификатора или связи стратегий. Таким образом, при удалении последней целевой связи идентификатора пользователя (как путем удаления отдельных целевых связей, так и путем удаления связи стратегий) этот идентификатор пользователя больше не будет определен в EIM. В результате идентификатор пользователя и вся его информация для поиска будут утрачены.

Понятия, связанные с данным

“Управление определениями реестров EIM” на стр. 95
Для применения в домене EIM реестров пользователей и находящихся в них идентификаторов пользователей необходимо создать определения реестров для этих реестров. После этого с помощью созданных определений реестров вы сможете управлять применением этих реестров пользователей и входящих в их состав идентификаторов пользователей EIM.

Управление правами доступа пользователей EIM

Пользователь EIM - это пользователь, обладающий правами доступа в соответствии с членством в предопределенных группах пользователей LDAP. При настройке доступа EIM пользователь добавляется в соответствующую группу пользователей LDAP.

Каждая группа LDAP имеет права доступа на выполнение различных административных задач EIM в домене. Тип задач (включая операции поиска соответствий EIM), выполнение которых разрешено пользователю EIM, определяется группой управления доступом, в состав которой входит пользователь EIM.

Добавлять пользователей в группу управления доступом EIM и изменять права доступа пользователей могут только пользователи с правами доступа администратора EIM или администратора LDAP. Для того чтобы пользователя можно было добавить в группу управления доступом EIM, этому пользователю должна соответствовать запись на сервере каталогов, выполняющем функции контроллера домена EIM. Кроме того, следует помнить, что в группу управления поиском EIM могут входить лишь отдельные категории пользователей: субъекты Kerberos, отличительные имена и пользовательские профайлы i5/OS.

Примечание: Для того чтобы в EIM в качестве типа пользователя был доступен субъект Kerberos, необходимо настроить в системе службу сетевой идентификации. Для того чтобы в EIM в качестве типа пользователя был доступен пользовательский профайл i5/OS, необходимо настроить на сервере каталогов суффикс системных объектов. Тем самым вы предоставите серверу каталогов возможность обращения к системным объектам i5/OS, в том числе к пользовательским профайлам i5/OS.

Для управления правами доступа существующего пользователя сервера каталогов или для добавления существующего пользователя сервера каталогов в группу управления доступом EIM выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Выберите домен EIM, с которым вы планируете работать.
   - Если нужный домен EIM не указан в разделе **Управление доменом**, то обратитесь к разделу “Добавление домена EIM в папку управления доменами” на стр. 90.
   - Если соединение с необходимым доменом EIM не установлено, то перейдите к разделу Подключение к контроллеру домена EIM.

3. Щелкните правой кнопкой мыши на домене EIM, с которым установлено соединение, и выберите пункт **Управление доступом**.
4. В окне **Изменить права доступа EIM** выберите **Тип пользователя**. Будут показаны поля ввода, позволяющие указать идентификационную информацию пользователя.
5. Введите информацию о пользователе, права доступа которого необходимо изменить, и нажмите кнопку **OK** для перехода к окну **Изменить права доступа EIM**. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
6. Выберите одну или несколько **групп управления доступом** и нажмите кнопку **OK** для добавления пользователя в выбранные группы. Для просмотра сведений о правах доступа, предоставляемых каждой группой, а также о предъявляемых специальных требованиях нажмите кнопку **Справка**.
7. После указания всей необходимой информации нажмите кнопку **OK** для сохранения внесенных изменений.

Понятия, связанные с данным

“Управление доступом EIM” на стр. 39
Пользователь EIM - это пользователь, обладающий правами доступа EIM в соответствии с членством в предопределенных группах пользователей LDAP выбранного домена.

Информация, связанная с данной

Служба сетевой идентификации

Управление свойствами конфигурации EIM

Вы можете управлять различными свойствами конфигурации EIM сервера. Как правило, необходимость такого управления возникает нечасто.

Однако, существует ряд ситуаций, в которых вам может потребоваться внесение изменений в свойства конфигурации. Например, если вам необходимо восстановить свойства конфигурации EIM после сбоя системы, то можно либо полностью повторить все шаги настройки с помощью мастера EIM, либо изменить свойства с помощью приведенных ниже инструкций. Другим примером может служить ситуация, в которой вы решили не создавать определения локальных реестров при работе с мастером настройки EIM, а настроить требуемую информацию непосредственно в свойствах конфигурации.

Вы можете изменять следующие свойства:

- Домен EIM, в состав которого входит сервер.
- Информация о подключении к контроллеру домена EIM.
- Идентификатор пользователя, применяемый системой для выполнения операций EIM от имени операционной системы.
- Имена определений реестров, ссылающиеся на фактические реестры пользователей, применяемые системой при выполнении операций EIM от имени операционной системы. Эти имена определений реестров ссылаются на локальные реестры пользователей, которые вы можете создать с помощью мастера настройки EIM.

  Примечание: Если вы решили не создавать имена локальных определений реестров с помощью мастера настройки EIM (из-за того, что реестры уже были определены в домене EIM или из-за того, чтобы решили определить их позже), то вам необходимо будет обновить свойства конфигурации системы, указав нужные имена определений реестров. Информация об определениях реестров необходима системе для выполнения операций EIM от имени операционной системы.

Для изменения свойств конфигурации EIM необходимы следующие специальные права доступа:

- Права доступа системного администратора (*SECADM)
- Права доступа ко всем объектам (*ALLOBJ)

Для изменения свойств конфигурации EIM на платформе System i выполните следующие действия:

1. Разверните узлы **Сеть>EIM**.
2. Щелкните правой кнопкой мыши на пункте **Конфигурация** и выберите **Свойства**.
3. Измените информацию о конфигурации EIM.
4. Описание информации, указываемой в каждом поле, приведено в электронной справке. Для ее просмотра нажмите кнопку **Справка**.
5. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации можно успешно подключиться к контроллеру домена EIM.
6. Для сохранения внесенных изменений нажмите **OK**.

Примечание: Если вы не использовали мастер настройки EIM для создания домена или для включения системы в уже существующий домен, то не пытайтесь создать конфигурацию EIM путем задания свойств конфигурации вручную. Выполнив базовую настройку EIM с помощью мастера, вы можете избежать возникновения неполадок, поскольку помимо изменения свойств конфигурации, мастер выполняет также ряд других операций.

Устранение неполадок преобразований идентификаторов в рамках предприятия

Следующие методы устранения неполадок используются для решения некоторых основных проблем, возникающих при настройке и использовании преобразований идентификаторов в рамках предприятия (EIM).

EIM объединяет несколько технологий и состоит из нескольких приложений и функций. Наличие большого числа компонентов может привести к возникновению различных неполадок. Ниже описаны некоторые типичные ошибки и неполадки, которые могут возникнуть при работе с EIM, а также даны рекомендации по устранению этих неполадок.

Информация, связанная с данной

Устранение неполадок в конфигурации единого входа в систему

Устранение неполадок подключения к контроллеру домена

Сбои при попытках подключиться к контроллеру домена могут быть вызваны разными причинами. Следующая таблица поможет вам выявить и устранить возможные неполадки подключения

Таблица 27. Типичные неполадки подключения к контроллеру домена EIM

Возможная неполадка	Способы исправления
Невозможно подключиться к контроллеру домена при управлении EIM с помощью System i Navigator.	Может быть неправильно указана информация о подключении к контроллеру домена, которым вы хотите управлять. Для проверки информации о подключении к контроллеру домена выполните следующие действия: • Разверните узлы **Сеть-->Преобразования идентификаторов в рамках предприятия-->Сеть->Управление доменами**. Щелкните правой кнопкой мыши на интересующем вас домене и выберите пункт **Свойства**. • Проверьте правильность значений, указанных в полях **Контроллер домена** и **Родительское DN**. • Проверьте правильность информации о **Подключении** к контроллеру домена. Проверьте правильность указанного номера **Порта**. Если выбран переключатель **Применять защищенное соединение (SSL или TLS)**, то на сервере каталогов должна быть настроена поддержка SSL. Нажмите кнопку **Проверить соединение**, чтобы убедиться, что с помощью указанной информации можно успешно подключиться к контроллеру домена EIM. • Проверьте правильность информации о пользователе, указанной на панели **Подключение к контроллеру домена**.

Таблица 27. Типичные неполадки подключения к контроллеру домена EIM (продолжение)

Возможная неполадка	Способы исправления
Операционная система или приложения не могут подключиться к контроллеру домена для работы с данными EIM. Например, при выполнении операций поиска соответствия EIM от имени системы возникают ошибки. Причина может заключаться в неправильной конфигурации EIM в одной или нескольких системах.	Запишите параметры конфигурации функции публикации. В системе, в которой вы пытаетесь выполнить идентификацию, разверните категории **Сеть-->Преобразования идентификаторов в рамках предприятия-->Конфигурация**. Щелкните правой кнопкой мыши на папке **Конфигурация**, выберите пункт меню **Свойства** и проверьте следующие значения: • На странице **Домен**: – Проверьте правильность указания имени и номеров портов контроллера домена. – Нажмите кнопку **Проверить конфигурацию** и убедитесь, что контроллер домена активен. – Проверьте правильность указания имени локального реестра. – Проверьте правильность указания имени реестра Kerberos. – Убедитесь, что выбран переключатель **Включить операции EIM на этой системе**. • На странице **Система**: – Убедитесь, что права доступа EIM применяемого пользователя допускают выполнение операций поиска соответствий. Проверьте правильность пароля пользователя. Дополнительная информация о различных типах идентификационных данных пользователей приведена в электронной справке. **Примечание:** Если вы изменяли пароль данного системного пользователя на сервере каталогов, то необходимо изменить пароль и в локальной системе. Если пароли не совпадают, то системный пользователь не сможет выполнять функции EIM для операционной системы и операции поиска соответствия выполняться не будут. – Нажмите кнопку **Проверить соединение** и убедитесь, что информация о пользователе указана правильно.
Информация о конфигурации указана правильно, но подключиться к контроллеру домена невозможно.	• Убедитесь, что запущен сервер каталогов, выполняющий функции контроллера домена EIM. Если контроллер домена расположен на платформе System i, то для проверки воспользуйтесь System i Navigator и выполните следующие действия: 1. Разверните узлы **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**.

После проверки информации о подключении и запуска сервера каталогов попытайтесь подключиться к контроллеру домена. Для этого выполните следующие действия:

1. Разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**.
2. Щелкните правой кнопкой мыши на домене EIM, с которым необходимо установить соединение, и выберите пункт **Установить соединение**.

3. Укажите тип пользователя и обязательные сведения о пользователе для подключения к контроллеру домена EIM.
4. Нажмите кнопку **OK**.

Устранение типичных неполадок конфигурации и домена EIM

Существует ряд типичных неполадок, с которыми вы можете столкнуться при настройке EIM в своей системе или при обращении к домену EIM. В следующей таблице перечислены такие неполадки и возможные способы их устранения.

Таблица 28. Типичные неполадки конфигурации и домена EIM

Возможная неполадка	Способы исправления
Зависание мастера настройки EIM после нажатия кнопки **Готово**.	Мастер может ожидать запуска контроллера домена. Убедитесь, что запуск сервера каталогов прошел без ошибок. В случае платформ System i просмотрите записи протокола задания `QDIRSRV` в подсистеме `QSYSWRK`. Для просмотра протокола задания выполните следующие действия: 1. В System i Navigator разверните список **Управление потоком операций > Подсистемы > Qsyswrk**. 2. Щелкните правой кнопкой мыши на **Qdirsrv** и выберите **Протокол задания**.
При создании с помощью мастера настройки EIM домена в удаленной системе появляется сообщение об ошибке ″Введенное родительское отличительное имя (DN) недопустимо. DN должно существовать на удаленном сервере каталогов. Укажите или выберите новое или существующее родительское DN.’	Указанное для удаленного домена родительское DN не существует. Ознакомьтесь с инструкциями по работе с мастером настройки EIM из раздела “Создание нового удаленного домена и добавление системы в него” на стр. 78. Кроме того, вы можете ознакомиться со сведениями об указании родительского DN, приведенными в электронной справке.
Сообщение об ошибке, указывающее, что домен EIM не существует.	Если еще вы не создали домен EIM, воспользуйтесь мастером настройки EIM. Этот мастер создаст домен EIM или поможет вам настроить существующий домен EIM. Если вы уже создали домен EIM, то убедитесь, что указанный пользователь входит в состав группы “Управление доступом EIM” на стр. 39, имеющей необходимые права доступа.
Сообщение об ошибке, указывающее, что объект EIM (идентификатор, реестр, связь, связь стратегий или фильтр сертификатов) не найден или у вас нет прав доступа к данным EIM.	Убедитесь, что объект EIM существует, а указанный пользователь входит в состав группы “Управление доступом EIM” на стр. 39, имеющей необходимые права доступа к этому объекту.

Таблица 28. Типичные неполадки конфигурации и домена EIM (продолжение)

Возможная неполадка	Способы исправления
При разворачивании папки **Идентификаторы** отображение списка идентификаторов занимает очень много времени.	Причина может заключаться в наличии очень большого числа идентификаторов в домене EIM. Для того чтобы список отображался быстрей, вы можете настроить представление папки **Идентификаторы**, задав более строгие условия поиска, применяемые для выбора отображаемых идентификаторов. Для настройки представления списка идентификаторов EIM выполните следующие действия: 1. В System i Navigator разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > 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**. 4. Укажите условия поиска идентификаторов EIM, включаемых в показанный список. **Примечание:** В качестве символа подстановки можно указать звездочку (*****). 5. Нажмите кнопку **OK**. Если после этого вы выберете пункт **Идентификаторы**, то будут показаны только те идентификаторы EIM, которые отвечают указанным условиям.
При управлении EIM с помощью System i Navigator появляется сообщение об ошибке, указывающее, что описатель EIM больше не действителен.	Утеряно соединение с контроллером домена. Для повторного подключения к контроллеру домена выполните следующие действия: 1. В System i Navigator разверните узлы **Сеть > Преобразование идентификаторов в рамках предприятия > Управление доменами**. 2. Щелкните правой кнопкой мыши на нужном домене и выберите пункт **Подключиться заново**. 3. Укажите сведения о соединении. 4. Нажмите кнопку **OK**.
При использовании для идентификации EIM протокола Kerberos в протокол задания заносится диагностическое сообщение `CPD3E3F`.	Это сообщение выдается сбое идентификации или при общем сбое операций преобразования идентификаторов. Это диагностическое сообщение содержит основной и дополнительный код состояния, указывающий, где возникла неполадка. Для наиболее распространенных ошибок в сообщениях приводятся инструкции по их исправлению. Для устранения неполадки обратитесь к справочной информации, связанной с полученным диагностическим сообщением. Вы также можете ознакомиться с разделом Устранение неполадок конфигурации единого входа в систему.

Устранение неполадок записей соответствия EIM

Существует ряд типичных неполадок, которые могут привести к неправильной работе EIM или к тому, что преобразование совсем не будет выполняться. В следующей таблице приведена информация о неполадках, которые могут привести к ошибкам преобразования EIM, а также о возможных способах устранения этих неполадок. Для устранения ошибок преобразования EIM может потребоваться попробовать все перечисленные в таблице решения.

Таблица 29. Типичные неполадки преобразования EIM и способы их устранения

Возможная неполадка	Способы исправления
Неправильно задана информация о подключении к контроллеру домена или контроллер домена неактивен.	Сведения о том, как проверить информацию о подключении к контроллеру домена, а также о том, как убедиться в активности контроллера, приведены в разделе Неполадки подключения к контроллеру домена.
При выполнении операций поиска соответствия EIM от имени системы возникают ошибки. Причина может заключаться в неправильной конфигурации EIM в одной или нескольких системах.	Запишите параметры конфигурации функции публикации. В системе, в которой вы пытаетесь выполнить идентификацию, разверните категории **Сеть-->Преобразования идентификаторов в рамках предприятия-->Конфигурация**. Щелкните правой кнопкой мыши на папке **Конфигурация**, выберите пункт меню **Свойства** и проверьте следующие значения: • На странице **Домен**: – Проверьте правильность указания имени и номеров портов контроллера домена. – Нажмите кнопку **Проверить конфигурацию** и убедитесь, что контроллер домена активен. – Проверьте правильность указания имени локального реестра. – Проверьте правильность указания имени реестра Kerberos. – Убедитесь, что выбран переключатель **Включить операции EIM на этой системе**. • На странице **Система**: – Убедитесь, что права доступа EIM применяемого пользователя допускают выполнение операций поиска соответствий. Проверьте правильность пароля пользователя. Дополнительная информация о различных типах идентификационных данных пользователей приведена в электронной справке. **Примечание:** Если вы изменяли пароль данного системного пользователя на сервере каталогов, то необходимо изменить пароль и в локальной системе. Если пароли не совпадают, то системный пользователь не сможет выполнять функции EIM для операционной системы и операции поиска соответствия выполняться не будут. – Нажмите кнопку **Проверить соединение** и убедитесь, что информация о пользователе указана правильно.

Таблица 29. Типичные неполадки преобразования EIM и способы их устранения (продолжение)

Возможная неполадка	Способы исправления
Операция поиска соответствий возвращает несколько целевых идентификаторов пользователей. Такая ошибка может возникать в следующих ситуациях: • У идентификатора EIM есть несколько отдельных целевых связей с одним и тем же целевым реестром. • Для идентификатора пользователя в исходной связи указано несколько идентификаторов EIM и каждый из этих идентификаторов EIM имеет целевую связь с одним и тем же целевым реестром, хотя в целевых связях каждого идентификатора может быть указан свой целевой идентификатор пользователя. • Один и тот же целевой реестр указан в нескольких стратегиях домена по умолчанию. • Один и тот же целевой реестр и один и тот же исходный реестр указаны в нескольких связях стратегий реестров по умолчанию. • В нескольких связях стратегий фильтров сертификатов указан один и тот же исходный реестр X.509, фильтр сертификатов или целевой реестр.	С помощью функции Проверить преобразование EIM убедитесь, что конкретный исходный идентификатор пользователя правильно преобразуется в соответствующий целевой идентификатор пользователя. Способ исправления ошибки зависит от результатов проверки: • При проверке получено несколько неправильных целевых идентификаторов, по одной из следующих причин: – Это может указывать на наличие одной из следующих ошибок в конфигурации связей в домене: - Неправильно настроены исходные или целевые связи идентификатора EIM. Например, у субъекта Kerberos (или пользователя Windows) может отсутствовать исходная связь или существовать неправильная исходная связь. Кроме того, в целевой связи может быть указан неправильный идентификатор пользователя. С помощью функции Показать все связи идентификаторов для идентификатора EIM проверьте связи выбранного идентификатора. - Неправильно настроена связь стратегий. С помощью функции Показать все связи стратегий для домена проверьте информацию об определенных в домене исходных и целевых связях стратегий. – Это может указывать на то, что групповые определения реестра, содержащие общие элементы, являются исходными или целевыми реестрами для связи идентификатора EIM или связи стратегии. С помощью сведений, предоставленных операцией проверки поиска идентификатора, определите, являются ли целевой или исходный реестр групповым определением реестра. Если это так, проверьте свойства группового определения реестра чтобы установить, не содержат ли групповые определения реестра общие элементы. – При проверке получено несколько целевых идентификаторов, соответствующих настроенной конфигурации. В этом случае необходимо указать для каждого целевого идентификатора пользователя информацию для поиска, позволяющую гарантировать возврат операцией поиска соответствия только одного целевого идентификатора пользователя, а не всех возможных целевых идентификаторов. См. раздел Добавление информации для поиска в целевой идентификатор пользователя. **Примечание:** Такой подход допустим лишь в том случае, если приложение поддерживает применение информации для поиска. Однако следует помнить, что базовые приложения i5/OS, такие как System i Access for Windows, не могут различать несколько возвращенных операцией поиска целевых идентификаторов пользователей с помощью информации для поиска. Следовательно, необходимо переопределить связи в домене, обеспечив возврат операциями поиска соответствий только одного идентификатора пользователя, что гарантирует приложениям i5/OS

Таблица 29. Типичные неполадки преобразования EIM и способы их устранения (продолжение)

Возможная неполадка	Способы исправления
В домене настроены связи, но операции поиска EIM не возвращают результаты.	С помощью функции Проверить преобразование EIM убедитесь, что конкретный исходный идентификатор пользователя правильно преобразуется в соответствующий целевой идентификатор пользователя. Проверьте правильность информации, указываемой при проверке. Если информация задана правильно, но результаты не возвращаются, то возможны следующие причины ошибки: • Неправильно настроена связь. Проверьте конфигурацию связи с помощью информации об устранении неполадки из предыдущего сообщения. • На уровне домена не включена поддержка связей стратегий. Возможно, вам потребуется включить связи стратегий для домена. • На уровне отдельного реестра не включена поддержка связей стратегий или поддержка поиска соответствий. Вам может потребоваться включить поддержку поиска соответствий и применение связей стратегий для целевого реестра. • Определение реестра и идентификаторы пользователей не совпадают из-за несоответствия регистра символов. Вы можете удалить, а затем заново создать реестр или связи, указав символы в правильном регистре.

Задачи, связанные с данной

“Тестирование связей EIM” на стр. 91
При тестировании связей EIM в созданной конфигурации EIM выполняются операции поиска соответствий. Тестирование позволяет убедиться, что выбранный исходный идентификатор пользователя правильно преобразуется в целевой идентификатор. Проверка гарантирует возврат правильных результатов операциями поиска EIM на основе заданной информации.

API EIM

Технология EIM предоставляет механизмы кросс-платформенного управления идентификаторами пользователей. 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. Все эти API поддерживаются платформами IBM.

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

Для изменения или получения данных EIM из домена EIM с помощью API в приложениях обычно применяется следующая схема:

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

Понятия, связанные с данным

“План разработки приложений EIM” на стр. 69
Для того чтобы приложение могло применять технологию EIM и входить в состав домена, это приложение должно иметь возможность использоваться API EIM.

Информация, связанная с данной

API преобразования идентификаторов предприятия (EIM)

Дополнительная информация о EIM

Такие публикации как IBM Руководства по выполнению задач и другие сборники разделов информационного центра содержат информацию, связанную со сборником разделов, посвященных преобразованию идентификаторов в рамках предприятия (EIM). Документы в формате PDF можно просмотреть или распечатать.

Руководства по выполнению задач IBM

- Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server 
- iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos 

Другая информация

- Единый вход в систему
- Служба сетевой идентификации
- Сервер каталогов IBM Tivoli для i5/OS (LDAP)

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, а в некоторых случаях - и за дополнительную плату.

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Соглашения о лицензии на машинный код или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Все приведенные цены представляют собой рекомендованные IBM в данный момент розничные цены. Эти цены могут быть изменены без предварительного уведомления. Цены у дилеров могут отличаться от указанных.

Данная информация предназначена исключительно для планирования. К моменту выхода продукта приведенная информация может быть изменена.

Данная информация содержит примеры данных и отчетов, применяемых в повседневных бизнес-операциях. Для более полной иллюстрации эти примеры содержат имена людей, названия компаний, продуктов и товаров. Все эти имена являются вымышленными и любое сходство с фактическими именами и адресами абсолютно случайно.

Лицензия на авторские права:

Эта публикация содержит исходные тексты примеров программ, демонстрирующих способы создания программ для различных операционных платформ. Вы можете копировать, изменять и распространять эти примеры в любой форме без выплат в адрес IBM с целью разработки, применения, распространения и продажи прикладных программ, поддерживающих интерфейс прикладных программ операционных платформ, для которых создавались примеры. Работа примеров не была проверена во всех возможных условиях. В связи с этим, фирма IBM не гарантирует и не подразумевает, что эти программы правильно работают и не содержат ошибок.

Каждая полная или частичная копия этих примеров, а также любых программ, созданных на их основе, должна включать следующее примечание:

© (ваша компания) (год). Часть данного кода заимствована из примеров IBM Corp. © Copyright IBM Corp. _год или годы_. Все права защищены.

При просмотре этого документа в электронном виде фотографии и цветные иллюстрации могут отсутствовать.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

AIX
Distributed Relational Database Architecture
Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
System i
Tivoli
WebSphere
xSeries
z/OS

Adobe, логотип Adobe, PostScript и логотип PostScript являются товарными знаками Adobe Systems Incorporated, зарегистрированными в США и/или других странах.

Linux является зарегистрированным товарным знаком Линуса Торвальдса (Linus Torvalds) в США и других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками корпорации Microsoft в США и/или других странах.

UNIX - зарегистрированный знак The Open Group в США и других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.

Напечатано в Дании