



@server

iSeries

Secure Sockets Layer (SSL)

Версия 5, выпуск 3





@server

iSeries

Secure Sockets Layer (SSL)

Версия 5, выпуск 3

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 19.

Пятое издание (август 2005 г.)

Это издание относится к версии 5, выпуску 3, модификации 0 IBM Operating System/400 (код продукта 5722–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).

© Copyright International Business Machines Corporation 2002, 2005. Все права защищены.

Содержание

| | |
|--|----------|
| Secure Sockets Layer (SSL) | 1 |
| Что нового в V5R3 | 1 |
| Как напечатать этот раздел | 1 |
| Сценарии: | 2 |
| Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL | 2 |
| Сценарий: Защита всех соединений с сервером централизованного управления с помощью SSL | 6 |
| Принципы работы | 13 |
| История появления SSL | 13 |
| Принципы работы SSL | 13 |
| Поддержка протоколов SSL и Transport Layer Security (TLS) | 14 |

| | |
|---|----|
| Идентификация сервера | 15 |
| Идентификация клиента | 15 |
| Планирование настройки SSL | 16 |
| Защита приложений с помощью SSL | 16 |
| Устранение неполадок SSL | 17 |
| Связанная информация | 18 |

| | |
|--|-----------|
| Приложение. Примечания | 19 |
| Товарные знаки | 20 |
| Условия загрузки и печати публикаций | 21 |

Secure Sockets Layer (SSL)


Протокол Secure Sockets Layer (SSL) стал отраслевым стандартом, который применяется приложениями для установления защищенных соединений в незащищенной сети, например, в Internet. Ниже приведены ссылки на страницы с дополнительной информацией об SSL и приложениях сервера iSeries:

- **Что нового в V5R3**
Обзор новых функций и новой информации по SSL
- **Сценарии применения SSL**
- новый раздел с информацией об SSL, в котором описаны различные примеры применения SSL на сервере iSeries.
- **Принципы работы SSL**
Содержит дополнительную информацию, в том числе некоторые базовые сведения о протоколах SSL.
- **Планирование настройки SSL**
содержит список предварительных требований, которые должны быть выполнены на сервере iSeries для применения SSL, а также некоторые полезные советы и рекомендации.
- **Защита приложений с помощью SSL**
содержит список приложений, для защиты которых на сервере iSeries может применяться SSL.
- **Устранение неполадок SSL**
- краткая информация об устранении неполадок SSL на сервере iSeries.
- **Связанная информация об SSL**
содержит ссылки на дополнительные источники информации.

Что нового в V5R3



В этом выпуске следует обратить внимание на две особенности, связанные с Secure Sockets Layer (SSL):

1. **Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL**
Это новый сценарий, который описывает применение SSL для защиты соединения между удаленным клиентом и сервером централизованного управления на сервере iSeries, выбранном в качестве центральной системы в локальной сети.
2. **Версия API GSKit 6B**
Начиная с выпуска V5R3, API GSKit базируются на версии GSKit 6B. В предыдущем выпуске они базировались на версии GSKit 4D. Здесь вы можете найти дополнительную информацию об API GSKit.

Другую информацию об измененных и новых возможностях, появившихся в этом выпуске, вы можете найти в документе [Информация для пользователей](#) 

Обозначение новой и измененной информации:

Внесенные в данный документ технические изменения обозначены следующим образом:

- Начало нового или измененного раздела информации помечается значком 
- Конец нового или измененного раздела информации помечается значком 

Как напечатать этот раздел

Вы можете просмотреть этот документ или загрузить его версию в формате PDF. Для того чтобы сделать это, выберите ссылку [выберите Secure Sockets Layer \(SSL\)](#) (около 243 Кб).

Другая информация:


При необходимости вы можете просмотреть или напечатать информацию, связанную с данным разделом.

Сохранение файла PDF:

Для сохранения файла в формате PDF на рабочей станции с целью последующего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой мыши на имени файла PDF в окне браузера.
2. Выберите пункт **Сохранить как**.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Щелкните на **Сохранить**.

Загрузка программы Adobe Acrobat Reader:

Для просмотра и печати этого документа можно воспользоваться программой Adobe Acrobat Reader. Ее можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html) .

Сценарии:

Следующие сценарии помогут вам с максимальной эффективностью SSL на сервере iSeries:

- Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL
Этот сценарий описывает применение SSL для защиты соединения между удаленным клиентом и сервером централизованного управления на сервере iSeries, играющем роль центральной системы функции централизованного управления Навигатора iSeries.
- Сценарий: Защита всех соединений с сервером централизованного управления с помощью SSL
Этот сценарий описывает применение SSL для защиты **всех** соединений с сервером централизованного управления на сервере iSeries, играющем роль центральной системы функции централизованного управления Навигатора iSeries.
- Сценарий: Защита FTP с помощью SSL
В этом сценарии описывается применение SSL в приложении FTP.
- Сценарий: Защита Telnet с помощью SSL
В этом сценарии описывается применение SSL в приложении Telnet.
- Сценарий: Повышение эффективности работы SSL в iSeries
В этом сценарии описано применение криптографического аппаратного обеспечения для более эффективного шифрования данных на сервере iSeries.
- Сценарий: Защита личных ключей с помощью аппаратного обеспечения для шифрования
В этом сценарии описывается применение криптографического аппаратное обеспечение для защиты личных ключей, связанных с транзакциями SSL на сервере iSeries.

Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL



Ситуация:

В состав локальной сети, развернутой в офисе компании, входит несколько серверов iSeries. Системный администратор этой компании выбрал один из серверов iSeries в качестве центральной системы сети (далее мы будем называть этот сервер системой А). Он использует запущенный в этой системе сервер централизованного управления для управления всеми остальными конечными системами сети.

Администратор хочет обеспечить возможность подключения к серверу централизованного управления в системе А из внешней сети. Он часто бывает в командировках и ему требуется безопасное соединение с сервером централизованного управления во время отсутствия. Он хочет, чтобы соединение между его компьютером и сервером централизованного управления было надежно защищено, даже когда его нет в

офисе. Администратор решает использовать SSL на своем компьютере и на сервере централизованного управления системы А. Настроив поддержку SSL, он может быть уверен, что сервер централизованного управления надежно защищен.

Цели:

Администратор хочет защитить только соединение между своим компьютером и сервером централизованного управления. Ему не требуется дополнительная защита для соединений между этим сервером и конечными системами сети. Другие сотрудники компании также не нуждаются в дополнительной защите своих подключений к серверу централизованного управления. Администратору предстоит настроить свой компьютер и сервер централизованного управления так, чтобы его клиентское подключение использовало идентификацию сервера. При этом подключения других компьютеров-клиентов и других серверов iSeries к серверу централизованного управления не будут защищены с помощью SSL.

Подробности:

Следующая таблица иллюстрирует типы идентификации, применяемые в зависимости от того, включена ли поддержка SSL на компьютере-клиенте:

Таблица 1. Необходимые элементы для защищенного соединения SSL между клиентом и сервером централизованного управления

| Состояние SSL на компьютере администратора | Выбранный уровень идентификации для сервера централизованного управления в системе А. | Применяется ли соединение SSL? |
|--|---|--------------------------------|
| Поддержка SSL выключена | Безразлично | Нет |
| Включена поддержка SSL | Безразлично | Да (идентификация сервера) |

Идентификация сервера означает, что компьютер администратора идентифицирует сертификат сервера централизованного управления. Компьютер администратора в соединении с сервером играет роль клиента SSL. Сервер централизованного управления играет роль сервера SSL и должен подтвердить свою идентификацию. Для этого он предоставляет сертификат, выданный сертификатной компанией (CA), которой доверяет компьютер администратора.

Предварительные требования и предположения:

Для того чтобы защитить соединение между своим компьютером и сервером централизованного управления в системе А, администратор должен выполнить ряд задач по настройке:

1. В системе А должны быть выполнены все предварительные требования, предъявляемые средствами поддержки SSL (дополнительная информация приведена в разделе Предварительные требования SSL).
2. В системе должна быть установлена OS/400 версии V5R3 или более поздняя. Если в системе А применяется версия OS/400 V5R1, то установите следующие исправления (PTF) для OS/400 (5722-SS1):
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. На компьютере клиента должен применяться Навигатор iSeries, входящий в состав продукта iSeries Access для Windows V5R3 или более поздней версии.
4. Выберите сертификатную компанию (CA) для серверов iSeries.
5. Создайте для системы А сертификат, подписанный CA.
6. Отправьте сертификаты сервера и сертификатной компании в систему А и импортируйте их в базу данных ключей.
7. Свяжите сертификат с идентификационными данными сервера централизованного управления.

- a. В системе А Запустите Диспетчер цифровых сертификатов IBM. Теперь администратор может получить или создать сертификаты, а также внести другие изменения в систему сертификатов. Необходимые инструкции вы можете найти в разделе Работа с Диспетчером цифровых сертификатов.
 - b. Нажмите кнопку **Выбрать хранилище сертификатов**.
 - c. Выберите ***SYSTEM** и нажмите кнопку **Далее**.
 - d. Введите **пароль хранилища сертификатов *SYSTEM** и нажмите кнопку **Далее**. После обновления меню разверните папку **Управление приложениями**.
 - e. Нажмите **Обновить присвоение сертификата**.
 - f. Выберите **Сервер** и нажмите кнопку **Далее**.
 - g. Выберите **Сервер Централизованного управления** и нажмите **Обновить присвоение сертификата**. Теперь серверу централизованного управления присвоен сертификат, который будет применяться для идентификации клиентов iSeries Access для Windows.
 - h. Нажмите **Назначить новый сертификат**. DCM снова откроет страницу **Обновить присвоение сертификата** с подтверждающим сообщением.
 - i. Нажмите кнопку **Готово**.
8. Настройте Навигатор iSeries:
- a. Установите компонент SSL программы Навигатор iSeries. Для этого выполните процедуру выборочной установки.
 - b. Загрузите CA на компьютер-клиент.

Действия по настройке

Для защиты соединения с сервером с помощью SSL, необходимо выполнить следующие действия:

1. Шаг 1: Отключите поддержку SSL в Навигаторе iSeries на клиенте
2. Шаг 2: Задайте уровень идентификации для сервера централизованного управления.
3. Шаг 3: Перезапустите сервер централизованного управления в системе А
4. Шаг 4: Включите SSL в Навигаторе iSeries на клиенте:
5. Необязательный шаг: Отключите поддержку SSL в Навигаторе iSeries на клиенте

Подробные инструкции по настройке приведены в разделе Защита соединения клиента с сервером централизованного управления с помощью SSL.

Подробные сведения о настройке: Защита соединения клиента с сервером централизованного управления с помощью SSL

Эта информация предполагает, что вы ознакомились с разделом Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL. В этом сценарии, сервер iSeries выбран в качестве центральной системы локальной сети компании. Администратор использует сервер централизованного управления, работающий в центральной системе (до этого момента называвшейся системой А), для управления конечными системами сети. Ниже приведены инструкции по настройке защищенного подключения внешнего клиента к этому серверу. Вы можете вслед за администратором нашей гипотетической сети выполнить все необходимые операции.

Перед применением SSL в функции централизованного управления администратор должен установить все необходимые программы и настроить цифровые сертификаты на сервере iSeries. См. раздел Предварительные требования и предположения из описания данного сценария. После выполнения всех предварительных требований администратор может активировать SSL на сервере централизованного управления.

Шаг 1: Отключите поддержку SSL в Навигаторе iSeries на клиенте

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **Защита** и отмените выбор опции **Применять SSL**.

4. Перезапустите Навигатор iSeries.

Из контейнера Централизованное управление в Навигаторе iSeries исчезнет значок замка. Это значит, что соединение между клиентом и центральной системой компании теперь не защищено.

Шаг 2: Задайте уровень идентификации для сервера централизованного управления.

1. В окне программы Навигатор iSeries щелкните правой кнопкой мыши на папке **Централизованное управление** и выберите пункт **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. В качестве значения уровня идентификации выберите значение **Любой** (это значение доступно в iSeries Access для Windows V5R3 или более поздних версий).
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Шаг 3: Перезапустите сервер Централизованного управления в центральной системе

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. В **Системе А**, разверните опции **Сеть** —> **Серверы** и выберите **TCP/IP**.
3. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**. Список под именем центральной системы будет свернут. Появится сообщение о том, что соединение с сервером прервано.
4. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 4: Включите SSL в Навигаторе iSeries:

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **SSL** и выберите опцию **Применять SSL для соединения**.
4. Перезапустите Навигатор iSeries.

В Навигаторе iSeries рядом с сервером центрального управления появится значок замка, означающий, что соединение защищено с помощью SSL. Таким образом, администратор успешно установил защищенное соединение между своим клиентом и центральной системой компании.

Примечание: Эта процедура защищает только соединение между одним компьютером и сервером централизованного управления. Соединения остальных клиентов и конечных систем сети с этим сервером не будут защищены. Для того чтобы защитить подключения других клиентов, убедитесь, что для них выполнены предварительные требования и повторите Шаг 4. Для того чтобы защитить другие соединения с сервером централизованного управления, обратитесь к разделу Сценарий: Защита всех соединений с сервером централизованного управления с помощью SSL.

Необязательный шаг: Отключите поддержку SSL в Навигаторе iSeries на клиенте

Когда администратор работает в офисе, то он может отключить SSL, что позволит несколько повысить производительность компьютера. Для выключения SSL выполните следующие действия:

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите пункт **Свойства**.
3. Перейдите на страницу **Защита** и отмените выбор опции **Применять SSL**.
4. Перезапустите Навигатор iSeries.

В Навигаторе iSeries исчезнет значок замка, показанный рядом с сервером централизованного управления. Это означает, что соединение между клиентским компьютером и центральной системой больше не защищается.

В разделе Сценарии вы найдете другие сценарии SSL.

Сценарий: Защита всех соединений с сервером централизованного управления с помощью SSL

Ситуация:

Недавно была создана глобальная сеть (WAN) фирмы, содержащая несколько удаленных серверов iSeries (конечных систем). Для управления этими системами применяется центральный сервер iSeries, расположенный в главном офисе компании. В этой компании предусмотрена должность администратора системы безопасности. Он хочет использовать SSL для защиты подключений всех конечных систем и клиентов к центральной системе.

Подробности:

С помощью SSL администратор может **безопасно** осуществлять все соединения с сервером централизованного управления. Для применения SSL он должен настроить защиту приложений iSeries Access для Windows и Навигатор iSeries на том персональном компьютере, на котором запущена функция Централизованное управление.

Можно выбрать один из двух уровней идентификации:

Идентификация сервера

Обеспечивает идентификацию сертификата сервера конечной системы. Центральная система выступает в соединении с конечной системой в роли клиента SSL. Конечная система выступает в роли сервера SSL и должна предъявить удостоверение личности в виде сертификата, выданного сертификатной компанией, зарегистрированной центральной системой. Для каждой конечной системы необходим сертификат, выданный уполномоченной сертификатной компанией.

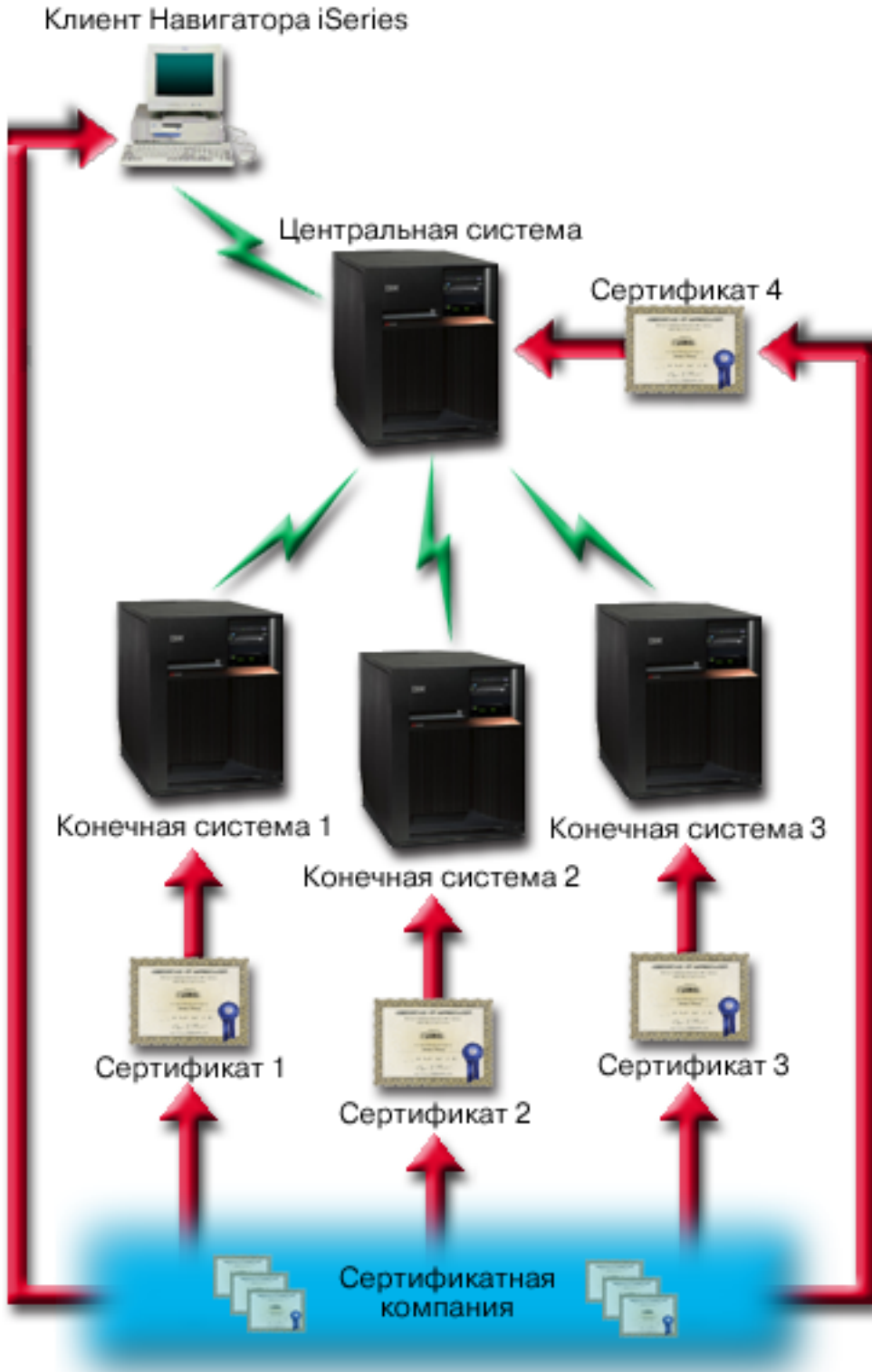
Идентификация сервера и клиента

Обеспечивает идентификацию сертификатов центральной и конечной систем. Это более высокий уровень защиты, чем идентификация сервера. В других приложениях это называется идентификацией клиента, так как клиент должен предоставить надежный базовый сертификат. Когда центральная система (клиент SSL) устанавливает соединение с конечной системой (сервером SSL), обе системы проверяют подлинность сертификатов друг друга.

В отличие от других приложений, Централизованное управление также поддерживает идентификацию с помощью контрольного списка, называемого контрольным списком Уполномоченной группы. Обычно в контрольном списке хранится информация, идентифицирующая пользователя, такая как ИД пользователя и информация идентификации: пароль, личный идентификационный номер или цифровой сертификат. Информация идентификации зашифрована.

В большинстве приложений нет опций для настройки идентификации клиента и сервера, поскольку идентификация сервера почти всегда происходит в процессе установления сеанса связи SSL. Во многих приложениях можно дополнительно настроить идентификацию клиента. В Централизованном управлении вместо идентификации клиента применяется термин "идентификация клиента и сервера", так как центральная система выполняет в сети две функции. Когда персональный компьютер устанавливает с центральной системой соединение SSL, последняя играет роль сервера. Однако при соединении центральной системы с другой конечной системой центральная система является клиентом. Ниже приведен пример выполнения центральной системой функций клиента и сервера в сети.

Примечание: В этом примере копия сертификата, связанного с сертификатной компанией, должна храниться в базах данных ключей центральной системы и всех конечных систем.



Предварительные требования и предположения:

Для применения SSL в Централизованном управлении администратор должен выполнить следующие задачи настройки и администрирования (см. рисунок WAN с централизованным управлением, защищенная с помощью SSL):

1. В центральной системе должны быть выполнены все предварительные требования для применения SSL (дополнительная информация приведена в разделе Предварительные требования SSL).
2. На центральном сервере iSeries и на всех конечных системах должна быть установлена операционная система OS/400 V5R2 или более поздней версии. Если на этих серверах применяется выпуск V5R1, необходимо установить следующие исправления (PTF) для OS/400 (5722-SS1):
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. На компьютере клиента должен применяться Навигатор iSeries, входящий в состав продукта iSeries Access для Windows V5R2 или более поздней версии. Если клиент относится к выпуску V5R1, установите пакет обслуживания PTF SI01907 (или выше) для iSeries Access для Windows выпуска V5R1 (5722-XE1).
4. Выберите сертификатную компанию (CA) для серверов iSeries.
5. Создайте сертификаты, подписанные CA, для всех серверов iSeries, администрирование которых выполняется с помощью Централизованного управления с поддержкой SSL.
6. Отправьте сертификаты сервера и сертификатной компании на все серверы iSeries и импортируйте их в базу данных ключей.
7. С помощью функции идентификации приложений Централизованного управления назначьте сертификаты конечным серверам, которые применяет Навигатор iSeries:
 - a. Запустите Диспетчер цифровых сертификатов IBM на центральном сервере. Если администратору требуется создать или получить сертификаты, либо выполнить другие действия с сертификатами, он должен сделать это сейчас (информация о настройке сертификатов приведена в разделе Работа с Диспетчером цифровых сертификатов).
 - b. Нажмите кнопку **Выбрать хранилище сертификатов**.
 - c. Выберите ***SYSTEM** и нажмите кнопку **Далее**.
 - d. Введите **пароль хранилища сертификатов *SYSTEM** и нажмите кнопку **Далее**. После обновления меню разверните папку **Управление приложениями**.
 - e. Нажмите **Обновить присвоение сертификата**.
 - f. Выберите **Сервер** и нажмите кнопку **Далее**.
 - g. Выберите **Сервер Централизованного управления** и нажмите **Обновить присвоение сертификата**. Теперь серверу централизованного управления присвоен сертификат.
 - h. Нажмите **Назначить новый сертификат**. DCM снова откроет страницу **Обновить присвоение сертификата** с подтверждающим сообщением.
 - i. Нажмите кнопку **Готово**.
 - j. Повторите эту процедуру для всех конечных серверов, которые применяются Навигатором iSeries.
8. Настройте Навигатор iSeries:
 - a. Установите компонент SSL программы Навигатор iSeries. Для этого выполните процедуру выборочной установки.
 - b. Загрузите CA на компьютер-клиент.

Действия по настройке

Перед применением SSL в функции централизованного управления администратор должен установить все необходимые программы и настроить цифровые сертификаты в центральной системе. См. раздел Предварительные требования и предположения из описания данного сценария. После выполнения всех предварительных требований администратор может активировать all для применения в Централизованном управлении, выполнив описанные ниже действия:

Примечание: Если функция SSL включена в Навигаторе iSeries, то администратор должен выключить ее перед активацией SSL в Централизованном управлении. Если функция SSL будет включена в Навигаторе iSeries и не будет включена в Централизованном управлении, то Навигатору iSeries не удастся подключиться к центральной системе.

- Шаг 1: Настройте центральную систему для идентификации сервера
- Шаг 2: Настройте конечные системы для идентификации сервера
- Шаг 3: Перезапустите сервер Централизованного управления в центральной системе:
- Шаг 4: Перезапустите сервер Централизованного управления во всех конечных системах.
- Шаг 5: Включите SSL в Навигаторе iSeries на клиенте.
- Шаг 6: Настройте центральную систему для идентификации клиента
- Шаг 7: Настройте конечные системы для идентификации клиента
- Шаг 8: Скопируйте контрольный список в конечные системы
- Шаг 9: Перезапустите сервер Централизованного управления в центральной системе
- Шаг 10: Перезапустите сервер Централизованного управления во всех конечных системах

Подробные инструкции по настройке приведены в разделе Подробные сведения о настройке: Защита соединения клиента с сервером централизованного управления с помощью SSL.

Подробные сведения о настройке: Защита всех соединений с сервером централизованного управления с помощью SSL

Эта информация предполагает, что вы ознакомились с пунктом Сценарий: Защитить все подключения к серверу централизованного управления с помощью SSL. Ниже приведены инструкции по настройке защищенного подключения всех клиентов к серверу централизованного управления. Вы можете вслед за администратором нашей гипотетической сети выполнить все необходимые операции.

Перед применением SSL в функции централизованного управления администратор должен установить все необходимые программы и настроить цифровые сертификаты на сервере iSeries. См. раздел Предварительные требования и предположения из описания данного сценария. После выполнения всех предварительных требований администратор может активировать all для применения в Централизованном управлении, выполнив описанные ниже действия.

Примечание: Если функция SSL включена в Навигаторе iSeries, то администратор должен выключить ее перед активацией SSL в Централизованном управлении. Если функция SSL будет включена в Навигаторе iSeries и не будет включена в Централизованном управлении, то Навигатору iSeries не удастся подключиться к центральной системе.

Шаг 1: Настройте центральную систему для идентификации сервера

С помощью SSL администратор может обеспечить защиту данных, передаваемых по соединению между центральной и конечной системами, а также по соединению между Навигатором iSeries и центральной системой. SSL обеспечивает передачу и идентификацию сертификатов и шифрование данных. Соединение SSL может быть установлено только между центральной и конечной системами, поддерживающими SSL. Прежде чем настраивать идентификацию клиента, необходимо настроить идентификацию сервера.

1. В окне программы Навигатор iSeries щелкните правой кнопкой мыши на папке **Централизованное управление** и выберите пункт **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. Выберите уровень идентификации **Сервер**.
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Примечание: Не перезапускайте сервер Централизованного управления до тех пор, пока идентификация сервера не будет настроена в конечных системах.

5. Настройте конечные системы для идентификации сервера.

Шаг 2: Настройте конечные системы для идентификации сервера

После настройки идентификации сервера в центральной системе администратор должен настроить идентификацию сервера во всех конечных системах. Для этого необходимо выполнить следующие действия:

1. Откройте представление **Централизованное управление**.
2. Сравните и обновите системные значения в конечных системах.
 - a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр**—>**Собрать**.
 - b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций.
 - c. Правой кнопкой мыши щелкните на пункте **Группы систем**—>**Создать группу систем**.
 - d. Определите новую группу систем, включающую все конечные системы, для работы с которыми будет применяться SSL.
 - e. Новая группа появится в списке групп систем.
 - f. После создания реестра щелкните правой кнопкой мыши на группе систем и выберите пункт **Системные значения**—>**Сравнить и обновить**.
 - g. Убедитесь, что в поле **Модельная система** указано имя центральной системы.
 - h. Выберите категорию **Централизованное управление** и убедитесь, что заданы следующие значения (отметьте переключатель рядом с ними):
 - Укажите значение **Да** для опции **Применять SSL**.
 - Выберите уровень идентификации **Сервер**.Эти значения устанавливаются в центральной системе при выполнении процедуры Настройка центральной системы для идентификации сервера.
 - i. Нажмите кнопку **ОК**. Указанные значения будут установлены во всех конечных системах из новой группы систем.
 - j. Подождите, пока завершится **Сравнение и обновление**. Не перезапускайте пока сервер Централизованного управления. Операция сравнения и обновления может занять несколько минут.

Шаг 3: Перезапустите сервер Централизованного управления в центральной системе

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Разверните значок центральной системы.
3. Разверните **Сеть**—> **Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**. Список под именем центральной системы будет свернут и появится сообщение о том, что соединение с сервером прервано.
5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 4: Перезапустите сервер Централизованного управления во всех конечных системах.

1. Разверните значок конечной системы, в которой нужно перезапустить сервер.
2. Разверните **Сеть**—> **Серверы** и выберите **TCP/IP**.
3. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**.
4. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.
5. Выполните эту процедуру во всех конечных системах.

Шаг 5: Включите SSL в Навигаторе iSeries:

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.

3. Перейдите на страницу **SSL** и выберите опцию **Применять SSL** для соединения.
4. Перезапустите Навигатор iSeries.

Шаг 6: Настройте центральную систему для идентификации клиента (необязательный шаг)

При необходимости после настройки идентификации сервера администратор может выполнить следующие процедуры настройки идентификации клиента. При идентификации клиента выполняется проверка Сертификатной компании и уполномоченной группы как центральной, так и конечных систем. Когда центральная система (клиент SSL) пытается установить соединение SSL с конечной системой (сервером SSL), то и центральная, и конечная системы идентифицируют сертификаты друг друга с помощью процедуры идентификации клиента. Эту процедуру называют также идентификацией сертификатной компании или защищенной группы.

Примечание: Настроить идентификацию клиента можно только после того, как настроена идентификация сервера.

1. В окне программы Навигатор iSeries щелкните правой кнопкой мыши на папке **Централизованное управление** и выберите пункт **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. Выберите уровень идентификации **Клиент и сервер**.
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Примечание: Не перезапускайте сервер Централизованного управления до тех пор, пока идентификация клиента и сервера с применением SSL не будет настроена во всех конечных системах.

5. Настройте конечные системы для идентификации клиента.

Шаг 7: Настройте конечные системы для идентификации клиента (необязательно)

1. Сравните и обновите системные значения в конечных системах.

Примечание: Эту задачу нельзя выполнить на серверах iSeries, в которых установлен выпуск V4R5.

- a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр—>Собрать**.
- b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций.
- c. Правой кнопкой мыши щелкните на пункте **Группы систем—>Создать группу систем**.
- d. Определите группу систем, включающую все конечные системы, с которыми планируется устанавливать соединения SSL.
- e. Новая группа появится в списке групп систем.
- f. После создания реестра щелкните правой кнопкой мыши на группе систем и выберите пункт **Системные значения—>Сравнить и обновить**.
- g. Убедитесь, что в поле **Модельная система** указана **Центральная система**.
- h. Выберите категорию **Централизованное управление** и убедитесь, что заданы следующие значения:
 - Укажите значение **Да** для опции **Применять SSL**.
 - Выберите уровень идентификации **Клиент и сервер**.

Эти значения устанавливаются в центральной системе при выполнении процедуры Настройка центральной системы для идентификации клиента. Отметьте переключатель **Обновить** напротив указанных значений.

- i. Нажмите кнопку **ОК**. Указанные значения будут установлены во всех конечных системах из новой группы систем.

Шаг 8: Скопируйте контрольный список в конечные системы

1. В следующей процедуре предполагается, что в центральной системе установлен выпуск операционной системы V5R3 или выше: В окне программы Навигатор iSeries разверните **Централизованное управление**—>**Определения**.
2. Щелкните правой кнопкой мыши на **Пакет** и выберите **Создать определение**.
3. В окне **Создать определение** задайте следующие значения:
 - **Имя:** Введите имя определения.
 - **Исходная система:** Введите имя центральной системы.
 - **Выбранные файлы и папки:** Щелкните мышью в поле и введите /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL.
4. Перейдите на страницу **Опции** и выберите пункт **Заменить существующий файл на отправленный файл**.
5. Нажмите кнопку **Дополнительно**.
6. В окне **Дополнительные опции** разрешите наличие различий в объектах при выполнении операции восстановления. Для этого задайте значение **Да**.
7. Нажмите кнопку **ОК**. Будет обновлен список определений и показан новый пакет.
8. Щелкните на новом пакете правой кнопкой мыши и выберите опцию **Отправить**.
9. В окне **Отправить** разверните **Группы систем**->**Уполномоченная группа** в списке **Доступные системы и группы**. Поочередно добавьте все системы выпуска V5R3 или выше в список **Выбранные системы и группа**. Удалите все остальные системы из списка **Выбранные системы и группа** и нажмите **ОК**. Уполномоченная группа - это группа систем, которая была определена в части 1.с. этапа Шаг 7: Настройте конечные системы для идентификации клиента.

Примечание: Задача **Отправить** не будет выполнена в центральной системе, так как она является исходной системой. Во всех конечных системах задача **Отправить** должна быть успешно выполнена.

В системах iSeries выпусков до V5R3 файл QYPSVLDL.VLDL находился в библиотеке QUSRSYS.LIB, а не QMGTC2.LIB. По этой причине, если вы отправляете контрольный список в системы выпусков до V5R3, то его необходимо будет поместить в QUSRSYS.LIB, а не в QMGTC2.LIB. Для этого выполните следующие действия:

- a. Щелкните правой кнопкой мыши на созданном ранее определении пакета и выберите **Создать на основе существующего**.
- b. Присвойте определению новое имя, чтобы отличать его от исходного.
- c. На вкладке **Общие** этого определения, в столбце **Целевой путь** щелкните на пути /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL. Это позволит отредактировать его. Исправьте QMGTC2 на QUSRSYS.

Примечание: Помните, что вы должны отредактировать **Целевой путь**, а не **Исходный путь**.

- d. Нажмите **ОК**, чтобы сохранить новое определение пакета.
- e. Щелкните правой кнопкой мыши на новом определении пакета и выберите **Отправить**.
- f. В окне **Отправить** разверните **Группы систем**->**Уполномоченная группа** в списке **Доступные системы и группы**. Поочередно добавьте все системы выпусков до V5R3 в список **Выбранные системы и группа**. Удалите все остальные системы из списка **Выбранные системы и группа** и нажмите **ОК**. **Уполномоченная группа** - это группа систем, которая была определена в части 1.с. этапа Шаг 7: Настройте конечные системы для идентификации клиента.

Шаг 9: Перезапустите сервер Централизованного управления в центральной системе

1. В окне программы Навигатор iSeries разверните список **Мои соединения**.
2. Разверните значок центральной системы.
3. Разверните **Сеть**—>**Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**. Список под именем центральной системы будет свернут и появится сообщение о том, что соединение с сервером прервано.

5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 10: Перезапустите сервер Централизованного управления во всех конечных системах

Примечание: Выполните эту процедуру во всех конечных системах.

1. Разверните значок конечной системы, в которой нужно перезапустить сервер.
2. Разверните **Сеть** → **Серверы** и выберите **TCP/IP**.
3. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**.
4. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

В разделе Сценарии вы найдете другие сценарии SSL.

Принципы работы

Протокол SSL позволяет устанавливать защищенные соединения между приложениями клиента и сервера, которые обеспечивают идентификацию одной или обеих конечных систем. SSL гарантирует секретность и целостность данных, которыми обмениваются клиент с сервером.

Приведенная ниже информация поможет вам лучше понять принцип работы SSL на сервере iSeries:

- История появления SSL
- Принципы работы SSL
- Поддержка протоколов SSL и Transport Layer Security (TLS)
- Идентификация сервера
- Идентификация клиента

История появления SSL

Протокол Secure Sockets Layer (SSL) был разработан фирмой Netscape в 1994 году для защиты данных, передаваемых по сети Internet. Несмотря на то, что первоначально SSL предназначался для защиты соединений между Web-браузером и Web-сервером, спецификация SSL позволяет применять этот протокол и другим приложениям, в том числе TELNET и FTP. Дополнительная информация об SSL и других связанных с ним протоколах приведена в разделе Поддержка протоколов SSL и Transport Layer Security (TLS).

Принципы работы SSL

SSL представляет собой, фактически, два протокола. Это протокол согласования и протокол передачи данных. Протокол передачи данных управляет потоком данных между двумя конечными системами соединения SSL.

Протокол согласования служит для идентификации одной или обеих конечных систем соединения SSL и создания уникального симметричного ключа, с помощью которого генерируются ключи для шифрования и расшифровки данных, передаваемых по этому соединению. Для идентификации конечных систем в протоколе SSL применяется асимметричное шифрование, цифровые сертификаты и процедуры согласования SSL. Обычно SSL идентифицирует сервер, но может использоваться и для идентификации клиента. Цифровой сертификат, выданный сертификатной компанией, может быть связан с каждой из конечной систем или с приложениями, применяющими протокол SSL в конечных системах.

Цифровой сертификат состоит из общего ключа и идентификационной информации с цифровой подписью уполномоченной сертификатной компании (CA). С каждым общим ключом связан частный ключ. Частный ключ не входит в состав сертификата и хранится отдельно от него. При идентификации клиента или сервера конечная система должна предоставить доказательство наличия частного ключа, соответствующего общему ключу цифрового сертификата.

Применение общих и частных ключей в операциях шифрования обуславливает высокие требования согласований SSL к производительности системы. После установления первого соединения SSL между двумя конечными системами информация об этом соединении и приложениях может быть занесена в кэш в защищенной памяти для ускорения последующих согласований SSL. При возобновлении соединения SSL конечные системы проверяют наличие доступа к уникальной информации путем выполнения сокращенной процедуры согласования без применения общего и частного ключей. Если обе системы предоставят доказательства наличия доступа к этой информации, будут созданы новые симметричные ключи и соединение SSL возобновится. Кэшированная информация соединений TLS версии 1.0 и SSL версии 3.0 будет удалена из защищенной памяти по истечении 24 часов. В выпуске V5R2M0 влияние процедуры согласования SSL на центральный процессор можно минимизировать, установив аппаратное обеспечение для шифрования.

Поддержка протоколов SSL и Transport Layer Security (TLS)

Существует несколько версий протокола SSL. Последней из них является протокол Transport Layer Security (TLS). Он основан на протоколе SSL версии 3.0 и был разработан Рабочей группой Internet (IETF). Реализация OS/400 поддерживает следующие версии протоколов SSL и TLS:

- TLS версии 1.0
- TLS версии 1.0, с поддержкой SSL версии 3.0

Примечания:

1. TLS версии 1.0 с поддержкой SSL версии 3.0 означает, что будет выполняться согласование TLS, а если это невозможно, то согласование SSL версии 3.0. Если согласование SSL версии 3.0 выполнить нельзя, то процедура согласования SSL не будет выполнена.
2. Кроме того, поддерживается TLS версии 1.0 с SSL версии 3.0 и 2.0. Этой функции соответствует значение протокола **ALL**, при котором будет выполняться процедура согласования TLS, а если это невозможно, то процедура согласования SSL версии 3.0. Если применить процедуру согласования SSL версии 3.0 невозможно, то выполняется согласование SSL версии 2.0. Если согласование SSL версии 2.0 выполнить нельзя, то процедура согласования SSL выполнена не будет.

- SSL версии 3.0
- SSL версии 2.0
- SSL версии 3.0 с поддержкой SSL версии 2.0

Сравнение SSL версии 3.0 с SSL версии 2.0

Протоколы SSL версии 3.0 и SSL версии 2.0 имеют мало общего. Наиболее важные отличия этих двух протоколов перечислены ниже:

- Поток процедуры согласования SSL версии 3.0 отличается от соответствующих потоков согласования SSL версии 2.0.
- SSL версии 3.0 применяет реализацию BSAFE 3.0 компании RSA Data Security, Incorporated. BSAFE 3.0 содержит исправления, защищающие от атак с нарушением синхронизации, и применяют алгоритм хеширования SHA-1. Алгоритм хеширования SHA-1 считается более надежным, чем алгоритм MD5. Применение SHA-1 позволяет SSL версии 3.0 поддерживать дополнительные сеансы шифрования с SHA-1 вместо MD5.
- Протокол SSL версии 3.0 защищает от атак типа man-in-the-middle (MITM) в процессе согласования SSL. В SSL версии 2.0 существовала небольшая вероятность успешного ослабления шифра с помощью атаки MITM. Ослабление шифра может позволить постороннему пользователю взломать ключ сеанса SSL.

Сравнение TLS версии 1.0 и SSL версии 3.0

Протокол Transport Layer Security (TLS) версии 1.0, основанный на SSL версии 3.0, является последними отраслевым стандартом SSL. Его спецификация определена рабочей группой IETF в документе RFC 2246,

"The TLS Protocol." 

Цель создания TLS - повышение защиты SSL и более точное и полное определение протокола. TLS обладает следующими преимуществами по сравнению с SSL версии 3.0:

- Более надежный алгоритм MAC
- Более детальные предупреждения
- Более четкие определения спецификаций "серой области"

Все приложения iSeries, поддерживающие SSL, автоматически поддерживают TLS, если явно не указано, что приложение должно применять SSL версии 3.0 или 2.0.

TLS предоставляет следующие усовершенствованные способы защиты:

- **Хеширование при идентификации сообщений**
TLS применяет в коде идентификации сообщения (HMAC) хеширование, предотвращающее от изменения записи при передаче по незащищенной сети, например в Internet. SSL версии 3.0 также поддерживает идентификацию сообщений с помощью ключей, но HMAC считается более надежным, чем функция MAC, применяемая в SSL версии 3.0.
- **Улучшенная псевдослучайная функция (PRF)**
С помощью PRF создаются данные ключа. В TLS функция PRF определена с помощью HMAC. PRF применяет два алгоритма хеширования, обеспечивающих ее защиту. Если один из алгоритмов будет взломан, данные будут защищены вторым алгоритмом.
- **Улучшенная проверка с сообщением о завершении**
Протоколы TLS версии 1.0 и SSL версии 3.0 отправляют обеим конечным системам сообщение "Готово", означающее, что доставленное сообщение не было изменено. Однако в TLS эта проверка основана на значениях PRF и HMAC, что обеспечивает более высокий уровень защиты по сравнению с SSL версии 3.0.
- **Совместимость обработки сертификатов**
В отличие от SSL версии 3.0, TLS пытается указать тип сертификата, который может применяться различными реализациями TLS.
- **Конкретные сообщения с предупреждениями**
TLS предоставляет более точные и полные предупреждения о неполадках, обнаруженных одной из конечных систем. TLS также содержит информацию о том, когда какие сообщения с предупреждениями следует отправлять.

Идентификация сервера

При идентификации сервера клиент проверяет подлинность сертификата сервера и наличие в нем подписи сертификатной компании, уполномоченной клиентом. С помощью асимметричного шифрования и протокола согласования SSL генерирует симметричный ключ, который будет применяться только для данного соединения. С помощью этого ключа создается набор ключей для шифрования и расшифровки данных, передаваемых через соединение SSL. По окончании процедуры согласования SSL будет идентифицирована одна или обе конечные системы соединения, и будет создан уникальный ключ для шифрования и расшифровки данных. После согласования данные уровня приложения будут передаваться через соединение SSL в зашифрованном виде.

Идентификация клиента

Многие приложения поддерживают опцию идентификации клиента. При идентификации клиента сервер проверяет подлинность сертификата клиента и наличие в нем подписи сертификатной компании, уполномоченной сервером. Идентификацию клиента поддерживают следующие приложения iSeries:

- IBM HTTP Server (на основе Apache)
- Сервер FTP
- Сервер Telnet
- Конечная система Централизованного управления
- Службы каталогов (LDAP)

Планирование настройки SSL

При планировании применения SSL на сервере iSeries обратите внимание на следующее:

- Предварительные требования SSL
- Требуемый тип цифровых сертификатов и планируемый источник сертификатов

Предварительные требования SSL:

- Диспетчер цифровых сертификатов IBM (DCM), компонент 34 операционной системы OS/400 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- Если при работе с DCM вы планируете применять сервер HTTP, необходимо установить продукт IBM Developer Kit for Java (5722-JV1). В противном случае вам не удастся запустить сервер администрирования HTTP.
- Продукт IBM Cryptographic Access Provider, 5722-AC3 (128-разрядный). Разрядность характеризует максимальный размер секретных данных в симметричных ключах, применяемых для шифрования. Максимальный размер симметричного ключа определяется законами о импорте и экспорте конкретной страны. Чем больше разрядность ключа, тем надежнее защищено соединение.
- Вы также можете установить аппаратное обеспечение для шифрования, которое позволяет ускорить процесс согласования SSL. В разделе Cryptographic hardware вы найдете информацию о доступных опциях. Если вы решите установить 4758 IBM Cryptographic Coprocessor или 4764 IBM Cryptographic Coprocessor, вам потребуется установить компонент 35, Cryptographic Service Provider.

Для применения SSL в компонентах Access for Windows необходимо установить продукт iSeries Client Encryption, 5722-CE3 (128-разрядный). Этот продукт применяется приложением iSeries Access for Windows для установления защищенных соединений.

Примечание: Продукт Client Encryption не требуется для работы эмулятора PC5250, поставляемого с продуктом Personal Communications. Программы Personal Communications содержат собственный код шифрования.

Цифровые сертификаты

В разделе Применение глобальных сертификатов и выдача локальных сертификатов описаны различия между глобальными и локальными сертификатами и даны рекомендации, в каких случаях лучше применять те или иные сертификаты.

Для управления цифровыми сертификатами на сервере iSeries применяется Диспетчер цифровых сертификатов (DCM) фирмы IBM. Дополнительная информация о DCM приведена в разделе Работа с Диспетчером цифровых сертификатов справочной системы Information Center.

Защита приложений с помощью SSL

SSL может применяться для защиты следующих приложений сервера iSeries:

- Enterprise Identity Mapping (EIM)
- Сервер FTP
- Сервер HTTP (на основе Apache)
- Приложения iSeries Access for Windows
- Службы каталогов (LDAP)
- Сервер архитектуры распределенных реляционных баз данных (DRDA) и управления распределенными данными (DDM)
- Центральная система Централизованного управления
- Сервер Telnet
- Websphere Application Server — Express

- Приложения, написанные с использованием интерфейсов прикладных программ (API) iSeries Access for Windows
- Приложения, созданные с применением API защищенных сокетов, поддерживаемых на сервере iSeries. Поддерживаются API из Global Secure Toolkit (GSKit) и встроенные API SSL_ системы iSeries. Информация о GSKit и SSL_API приведена в разделе API защищенных сокетов.

Устранение неполадок SSL

В этом разделе приведены общие рекомендации по устранению неполадок, которые могут возникнуть на сервере iSeries при работе с SSL. Данный раздел не является полным руководством по устранению неполадок.

Убедитесь, что выполнены следующие условия:

- На сервере iSeries выполнены предварительные требования SSL (дополнительная информация приведена в разделе Предварительные требования SSL).
- Если вы планируете применять функцию Централизованное управление программы Навигатор iSeries в системе выпуска V5R1, убедитесь, что в этой системе установлены следующие PTF:
 - si01375
 - si01376
 - si01377
 - si01378
 - si01838
- Убедитесь, что срок действия сертификатной компании и сертификатов не истек, и сертификатная компания является уполномоченной CA.

Если несмотря на соблюдение всех перечисленных выше условий на вашем сервере возникла неполадка SSL, попробуйте выполнить следующие действия:

- Найдите код ошибки SSL в протоколе задания сервера, а затем найдите дополнительную информацию об ошибке в таблице ошибок по ее коду. Информация о сообщениях с кодами ошибок SSL приведена на странице Сообщения с кодами ошибок API SSL. Например, если в протоколе задания сервера указан код ошибки -93, то по таблице можно определить, что он соответствует константе `SSL_ERROR_SSL_NOT_AVAILABLE`.
 - Отрицательный код возврата (есть дефис перед значением кода) означает, что применялся `SSL_API`.
 - Положительный код возврата означает, что применялся `API GSKit`. Для получения краткого описания кода возврата, свидетельствующего об ошибке, в программах могут применяться `API gsk_strerror()` и `SSL_strerror()`. С помощью этих API приложение может занести в протокол задания сообщение с описанием ошибки.

Для получения более подробной информации просмотрите сообщение с идентификатором, указанным в таблице, на сервере iSeries. В этом сообщении описана возможная причина ошибки и перечислены действия по ее исправлению. Дополнительную информацию с описанием кодов ошибок можно найти в документации по тому API защищенных сокетов, который вернул код ошибки.

- Имена констант, соответствующие системным кодам возврата SSL, перечислены и в указанных ниже файлах заголовков (без ссылки на ID сообщения):
 - `QSYSINC/H.GSKSSL`
 -



`QSYSINC/H.QS0SSL`

Хотя все имена констант, перечисленные в этих файлах, уникальны, один код возврата может соответствовать разным ошибкам.

Дополнительная информация об устранении неполадок на сервере iSeries приведена на странице >Устранение неполадок и обслуживание.



Связанная информация

Ниже перечислены источники дополнительной информации об SSL:


Источники IBM

- На странице SSL и Java Secure Socket Extension (JSSE) приведено краткое описание JSSE и информация о его применении.
- На странице IBM Toolbox for Java приведено краткое описание классов Java и рекомендации по их использованию.

Документы RFC

- RFC 2246: "The TLS Protocol Version 1.0"  содержит подробное описание протокола TLS.
- RFC2818: "HTTP Over TLS"  содержит информацию о защите соединений HTTP в Internet с помощью TLS.

Другие источники

- Документ The SSL Protocol Version 3.0  содержит подробное описание протокола SSL версии 3.0.

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
500 Columbus Avenue
Thornwood, NY 10594-1785
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, 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, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации 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 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.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и других странах:

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows
NT

Lotus, Freelance и WordPro являются товарными знаками International Business Machines Corporation и Lotus Development Corporation в США и других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками Microsoft в США и других странах.

Названия других компаний, продуктов и услуг могут быть товарными или сервисными знаками других компаний.

Условия загрузки и печати публикаций

Разрешение на использование выбранных для загрузки публикаций предоставляется в соответствии с следующими условиями и при подтверждении вашего с ними согласия.

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 данные 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 или применения для каких-либо конкретных целей.

Авторские права на все материалы принадлежат IBM Corporation.

Загружая или печатая публикации с этого сайта, вы тем самым подтверждаете свое согласие с приведенными условиями.



Напечатано в Дании