IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

Примечание

Перед началом работы с этим изданием и описанным в нем продуктом ознакомьтесь с информацией в разделе “Примечания” на стр. 47.

Данное издание относится к IBM PowerSC версии 1.1.3, а также ко всем последующим выпускам и модификациям, если в соответствующих изданиях не будет оговорено обратное.

Содержание

Об этом документе

В этом документе, адресованной системным администраторам, приведена информация о защите файлов, систем и сетей.

Выделение текста

В данном документе применяются следующие специальные обозначения:

Полужирный шрифт	Этим шрифтом выделены команды, функции, ключевые слова, файлы, структуры, каталоги и другие элементы, имена которых предопределены в системе. Кроме того, этим шрифтом выделены графические объекты, выбираемые пользователем: кнопки, метки и значки.
Курсив	Этим шрифтом выделены параметры, фактические имена или значения которых указываются пользователем.
`Непропорциональный шрифт`	Этим шрифтом выделены примеры конкретных значений, образцы фрагментов текста, которые могут быть показаны на экране, примеры программного кода, схожие с реальными, системные сообщения и информация, вводимая пользователем.

Учет регистра символов в AIX

В операционной системе AIX учитывается регистр символов, т.е. различаются прописные и строчные буквы. Например, команда **ls** выдает список файлов. При вводе `LS` система выдаст сообщение, что команда `не найдена`. Аналогично, имена файлов `FILEA`, `FiLea` и `filea` считаются разными, даже если эти файлы расположены в одном каталоге. Во избежание нежелательных последствий всегда контролируйте регистр вводимых символов.

ISO 9000

При разработке и производстве данного продукта использовались зарегистрированные системы ISO 9000.

IBM PowerSC Standard Edition 1.1.3

IBM® PowerSC Standard Edition включает в себя компоненты Надежная загрузка, Надежный брандмауэр, Надежное ведение протоколов, Надежное сетевое соединение и управление исправлениями, а также Автоматизация защиты и совместимости.

Новое в PowerSC Standard Edition 1.1.3

Здесь приведена новая и значительно измененная информация в наборе разделов для PowerSC Standard Edition версии 1.1.3.

В этом файле PDF можно увидеть полосы исправлений (|) на левом поле, которые означают новую или измененную информацию.

Декабрь 2013 г.

- В “Концепции PowerSC Standard Edition 1.1.3” обновлены системные требования.
- В разделе “Предварительные требования для Trusted Boot” на стр. 5 определена необходимая замена файла Trusted Boot при переустановке операционной системы AIX.
- В “Монитор Надежного брандмауэра” на стр. 13 добавлены сведения о функции мониторинга Trusted Firewall.
- В “Ведение протоколов Надежного брандмауэра” на стр. 13 добавлены сведения о функции ведения протоколов Trusted Firewall.
- Добавлен раздел “Установка Защищенных протоколов” на стр. 18.
- В “Настройка сервера управления исправлениями” на стр. 24 добавлена информация об обновлениях промежуточных исправлений для Trusted Network Connect.
- В “Создание отчетов о сервере TNC” на стр. 30 добавлена информация об отчетности сервера Trusted Network Connect.
- В раздел “Установка компонента проверки” на стр. 7 добавлена информация об установке утилиты проверки Trusted Network Connect.
- В раздел “Команды PowerSC Standard Edition” на стр. 31 добавлены команды Trusted Firewall.
- Команда **tscpmconsole** переименована в **pmconf** и ее описание добавлено в раздел “Команда pmconf” на стр. 35.
- Команда **tscconsole** переименована в **psconf** и ее описание добавлено в раздел “Команда psconf” на стр. 39.
- В разделе “Команда vlantfw” на стр. 44 обновлена информация об опциях команды **vlantfw**.

Ноябрь 2012 г.

Обновлена информация в разделе “Надежное сетевое соединение и управление исправлениями” на стр. 20.

Май 2012 г.

Добавлена документация по новой функции для “Надежный брандмауэр” на стр. 10.

Концепции PowerSC Standard Edition 1.1.3

В обзоре PowerSC Standard Edition описаны функции, компоненты и поддержка оборудования, относящиеся к компоненту PowerSC Standard Edition.

PowerSC Standard Edition обеспечивает функции защиты и управления системами, работающими в облачной среде или виртуализированных центрах обработки данных, а также предоставляет функции управления и

просмотра предприятия. PowerSC Standard Edition - это комплект компонентов, включающий автоматизацию защиты и согласования, Trusted Boot, Trusted Firewall, Trusted Logging, а также Trusted Network Connect и управление исправлениями. Технология защиты на уровне виртуализации предоставляет дополнительную защиту для автономных систем.

В приведенной ниже таблице приведены сведения о редакциях, включенных в редакции функциях, компонентах, а также доступных для каждого компонента аппаратных ресурсах на основе процессоров.

Таблица 1. Компоненты PowerSC Standard Edition, описание, поддержка операционной системы и аппаратная поддержка

Компоненты	**Описание**	**Поддерживаемая операционная система**	**Поддерживаемое аппаратное обеспечение**
Автоматизация защиты и согласования	Автоматизация настройки, отслеживания и контроля конфигурации защиты и согласования для следующих стандартов: • Стандарт защиты данных отрасли платежных карт (PCI DSS) • Закон Сарбейна-Оксли и согласование с COBIT (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Закон о преемственности и подотчетности медицинского страхования (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Trusted Boot	Определяет образ загрузки, операционную систему и приложения; проверяет их надежность с помощью технологии виртуального модуля надежной платформы (TPM).	• AIX 6 с пакетом обслуживания 6100-07 или более поздней версии • AIX 7 с пакетом обслуживания 7100-01 или более поздней версии	POWER7 firmware eFW7.4 или более поздней версии
Trusted Firewall	Экономит время и ресурсы за счет включения прямой маршрутизации через заданные виртуальные LAN (VLAN), управляемые одним Сервер виртуального ввода-вывода.	• AIX 6.1 • AIX 7.1 • VIOS версии 2.2.1.4 или более поздней	• POWER6 • POWER7 • Сервер виртуального ввода-вывода версии 6.1S или более поздней
Trusted Logging	Протоколы AIX централизованно собираются на виртуальном сервере ввода-вывода (VIOS) в реальном времени. Эта функция обеспечивает защищенное от внешних воздействий ведение протоколов и удобное резервное копирование протоколов и управление ими.	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7

Таблица 1. Компоненты PowerSC Standard Edition, описание, поддержка операционной системы и аппаратная поддержка (продолжение)

Компоненты	Описание	Поддерживаемая операционная система	Поддерживаемое аппаратное обеспечение
Trusted Network Connect и управление исправлениями	Проверяет уровень программного обеспечения и исправлений для всех систем AIX в виртуальной среде и предоставляет инструменты управления обновления всех систем AIX до заданного уровня ПО. Обеспечивает выдачу уведомлений при добавлении в сеть виртуальной системы более низкого уровня либо при применении исправления защиты, влияющего на системы.	• AIX 5.3 • AIX 6.1 • AIX 7.1 Для клиента Trusted Network Connect требуется один из следующих компонентов: • AIX 6.1 с пакетом обслуживания 6100-06 или более поздней версии • Система консоли SUMA для AIX версии 7.1 в среде SUMA для управления исправлениями	• POWER5 • POWER6 • POWER7

Установка PowerSC Standard Edition 1.1.3

Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Для PowerSC Standard Edition доступны следующие наборы файлов:

- `powerscExp.ice`: устанавливается в системах AIX, для которых требуется функция автоматизации защиты и согласования в PowerSC Standard Edition.
- `powerscStd.vtpm`: устанавливается в системах AIX, для которых требуется функция Trusted Boot в PowerSC Standard Edition.
- `powerscStd.vlog`: устанавливается в системах AIX, для которых требуется функция доверенного протоколирования в PowerSC Standard Edition.
- `powerscStd.tnc_pm`: устанавливается в AIX версии 6.1 с технологическим пакетом обслуживания 6100-06 или выше либо в системе консоли SUMA AIX версии 7.1 в среде SUMA для управления исправлениями.
- `powerscStd.svm`: устанавливается в системах AIX для использования функций маршрутизации PowerSC Standard Edition.

PowerSC Standard Edition можно установить с помощью одного из следующих интерфейсов:

- Команды **installp** из интерфейса командной строки (CLI)
- Интерфейса SMIT

Для установки PowerSC Standard Edition с помощью интерфейса SMIT выполните следующие действия:

1. Введите следующую команду:
   ```
   % smitty installp
   ```
2. Выберите опцию **Установить программное обеспечение**.
3. Выберите входное устройство или каталог для ПО с целью указания расположения и установочного файла образа IBM Compliance Expert. Например, если именем файла установочного образа является `/usr/sys/inst.images/powerscStd.vtpm`, то необходимо указать путь к файлу в поле **ВВОД**.
4. Просмотрите и примите лицензионное соглашение. Для принятия лицензионного соглашения нажмите стрелку вниз для выбора пункта **ПРИНЯТЬ новые лицензионные соглашения**, затем нажмите клавишу tab для изменения значения на **Да**.
5. Для начала установки нажмите клавишу **Enter**.
6. После завершения установки убедитесь, что значением состояния команды является **OK**.

Просмотр лицензии на программное обеспечение

Лицензию на программное обеспечение можно просмотреть в CLI с помощью следующей команды:

```
% installp -lE -d путь/имя-файла
```

, где *путь/имя-файла* указывает установочный образ PowerSC Standard Edition.

Например, с помощью CLI можно ввести следующую команду для указания сведений о лицензии, связанных с PowerSC Standard Edition:

```
% installp -lE -d  /usr/sys/inst.images/powerscStd.vtpm
```

Понятия, связанные с данным:

“Концепции PowerSC Standard Edition 1.1.3” на стр. 1
В обзоре PowerSC Standard Edition описаны функции, компоненты и поддержка оборудования, относящиеся к компоненту PowerSC Standard Edition.

“Установка функции Надежная загрузка” на стр. 6
Для установки функции Надежная загрузка требуются некоторые конфигурации аппаратного и программного обеспечения.

“Установка Trusted Network Connect” на стр. 22
Для установки компонентов Trusted Network Connect (TNC) необходимо выполнить следующие действия.

Задачи, связанные с данной:

“Установка Надежного брандмауэра” на стр. 12
Установка Надежного брандмауэра PowerSC подобна установке любой другой функции PowerSC.

“Установка Защищенных протоколов” на стр. 18
Можно установить функцию Защищенные протоколы PowerSC с помощью интерфейса командной строки или инструмента SMIT.

Надежная загрузка

Функция Надежная загрузка использует Virtual Trusted Platform Module (VTPM), который является виртуальным экземпляром TPM компании Trusted Computing Group. VTPM используется для безопасного сохранения измерений загрузки системы для будущей проверки.

Концепции Надежной загрузки

Важно понимать целостность процесса загрузки и способ классификации загрузки в качестве надежной или ненадежной.

Можно настроить не более 60 логических разделов с включенным VTPM (LPAR) для каждой физической системы, используя Консоль аппаратного обеспечения (HMC). Когда он настроен, VTPM является уникальным для каждого LPAR. При использовании с технологией AIX Trusted Execution, VTPM обеспечивает защиту и гарантию следующим разделам:

- Загрузочный образ на диске
- Вся операционная система
- Уровни приложений

Администратор может просматривать надежные и ненадежные системы из центральной консоли, установленной с помощью верификатора **openpts**, который доступен в пакете расширения AIX. Консоль **openpts** управляет одним или несколькими серверами Power Systems и отслеживает или удостоверяет состояние систем AIX по всему центру обработки данных. Удостоверение — это процесс, в котором верификатор определяет (или удостоверяет), выполнил ли коллектор надежную загрузку.

Состояние Надежной загрузки

Раздел называется надежным, если верификатор успешно удостоверил целостность коллектора. Верификатор — это удаленный раздел, который определяет, выполнил ли коллектор надежную загрузку. Коллектор — это раздел AIX, к которому присоединен Virtual Trusted Platform Module (VTPM), и в котором установлен Trusted Software Stack (TSS). Он указывает, что записанные в VTPM измерения соответствуют набору ссылок, хранимому в верификаторе. Состояние надежной загрузки указывает, загружен ли раздел надежным способом. Это утверждение относится к целостности процесса загрузки системы и не указывает текущего уровня защиты системы.

Состояние Ненадежной загрузки

Раздел входит в ненадежное состояние, если верификатор не может успешно удостоверить целостность процесса загрузки. Ненадежное состояние указывает на то, что какой-то аспект процесса загрузки несовместим со справочной информацией, хранимой в верификаторе. Возможными причинами неудачного удостоверения могут быть загрузка из другого загрузочного устройства, загрузка другого образа ядра и изменение существующего загрузочного образа.

Понятия, связанные с данным:

“Устранение неполадок функции Надежная загрузка” на стр. 9
Существует несколько общих сценариев и корректирующих действий, требуемых для определения причины невозможности удостоверения при использовании функции Надежная загрузка.

Планирование Trusted Boot

В статье описаны конфигурации аппаратного и программного обеспечения, требуемые для установки Trusted Boot.

Предварительные требования для Trusted Boot

Установка Trusted Boot предполагает настройку утилиты проверки и программы сбора статистики.

| При подготовке к переустановке операционной системы AIX в системе с уже установленным компонентом
| Trusted Boot необходимо скопировать файл `/var/tss/lib/tpm/system.data` и заменить файл в этом же
| расположении после переустановки. Если этот файл не был скопирован, то необходимо удалить
| виртуализированный модуль надежной платформы из консоли управления и переустановить его в разделе.

Программа сбора статистики

Предварительные требования к конфигурации при установке программы сбора статистики:

- Аппаратное обеспечение POWER7, работающее на выпуске промежуточного ПО 740.
- Установите IBM AIX 6 с технологическим пакетом обслуживания 7 или IBM AIX 7 с технологическим пакетом обслуживания 1.
- Установите консоль управления оборудованием (HMC) версии 7.4 или более поздней.
- Настройте раздел для использования VTPM и минимум 1 ГБ памяти.
- Установите SSH, а именно OpenSSH или аналог.

Verifier

Для доступа к утилите проверки **openpts** используется как интерфейс командной строки, так и графический пользовательский интерфейс, разработанный для работы на различных платформах. Версия утилиты проверки OpenPTS verifier для AIX доступна в пакете расширения AIX. Версии утилиты OpenPTS verifier для Linux и других платформ доступны для загрузки на веб-сайте. Для настройки должны быть выполнены следующие предварительные требования:

- Установите SSH, а именно OpenSSH или аналог.
- Установите сетевое соединение с программой сбора статистики (с помощью SSH).

- Установите Java™ 1.6 или выше для доступа к консоли **openpts** с помощью графического интерфейса.

Подготовка к исправлению

Описанная здесь информация о компоненте Надежная загрузка служит руководством для определения ситуаций, которые могут потребовать исправления. Она не влияет на процесс загрузки.

Существует много причин, которые могут помешать удостоверению, и трудно предсказать, какие условия могут возникнуть. Необходимо выбрать подходящее действие в зависимости от условий. Однако, полезно подготовиться к некоторым серьезным сценариям и иметь стратегию или поток операций для обработки таких случаев. Исправление — это корректирующее действие, которое должно быть выполнено, когда удостоверение сообщает о том, что один или несколько коллекторов ненадежны.

Например, если неполадка удостоверения возникает из-за того, что загрузочный образ отличается от ссылки верификатора, необходимо иметь ответы на следующие вопросы:

- Как можно проверить вероятность угрозы?
- Выполнялось ли недавно запланированное обслуживание, обновление AIX или установка нового аппаратного обеспечения?
- Можете ли вы обратиться к администратору, который имеет доступ к этой информации?
- Когда система была последний раз загружена в надежном состоянии?
- Если угроза выглядит правдоподобной, какое действие необходимо выполнить? (Варианты включают в себя сбор данных протоколов контроля, отключение системы от сети, выключение системы и смена пользователей).
- Случалось ли это на других системах, которые необходимо проверить?

Понятия, связанные с данным:

“Устранение неполадок функции Надежная загрузка” на стр. 9
Существует несколько общих сценариев и корректирующих действий, требуемых для определения причины невозможности удостоверения при использовании функции Надежная загрузка.

Замечания о миграции

Перед переносом раздела, включенного для VTPM, необходимо выполнить описанные ниже предварительные требования.

Преимуществом VTPM над физическим TPM является возможность переноса раздела между системами с его сохранением в VTPM. Для защищенного переноса логического раздела перед передачей промежуточное ПО шифрует данные VTPM. Для обеспечения защищенного переноса необходимо обеспечить выполнение следующих условий безопасности:

- Включить IPSEC между Сервер виртуального ввода-вывода (VIOS), выполняющими перенос.
- Указать с помощью консоли управления оборудованием (HMC) ключ надежных систем в управляемых системах для обеспечения возможности расшифровки данных VTPM после переноса. Для успешного переноса данных ключ в целевой системе и исходной должен быть одинаковым.

Информация, связанная с данной:

Использование HMC

Миграция VIOS

Установка функции Надежная загрузка

Для установки функции Надежная загрузка требуются некоторые конфигурации аппаратного и программного обеспечения.

Информация, связанная с данной:

“Установка PowerSC Standard Edition 1.1.3” на стр. 3
Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Установка программы сбора статистики

Программу сбора статистики необходимо установить с помощью набора файлов на базовом компакт-диске AIX.

Для установки программы сбора статистики установите пакеты `powerscStd.vtpm` и `openpts.collector` с базового компакт-диска с помощью команды **smit** или **installp**.

Установка компонента проверки

Компонент проверки OpenPTS работает в операционной системе AIX, а также на других платформах.

Версию компонента проверки для AIX можно установить из набора файлов с помощью пакета расширения AIX. Для установки компонента проверки в операционной системе AIX установите пакет `openpts.verifier` из пакета расширений AIX с помощью команды **smit** или **installp**. При этом будут установлены и версия для командной строки, и версия компонента с графическим интерфейсом.

Компонент проверки OpenPTS для других операционных систем можно загрузить из раздела `Загрузить Linux OpenPTS Verifier для использования с AIX Trusted Boot`.

Информация, связанная с данной:

Загрузить Linux OpenPTS Verifier для использования с AIX Trusted Boot

Настройка Надежной загрузки

В этом разделе описана процедура регистрации системы и ее удостоверение для Надежной загрузки.

Регистрация системы

В статье описана процедура регистрации системы в утилите проверки.

Регистрация системы - это процесс передачи набора начальных параметров в утилиту проверки, которая формирует основу для последующих запросов аттестации. Для регистрации системы с помощью командной строки выполните в утилите проверки следующую команду:

```
openpts -i <имя-хоста>
```

Сведения о зарегистрированном разделе расположены в каталоге `$HOME/.openpts`. Каждому новому разделу во время регистрации присваивается уникальный идентификатор, и вся информация, связанная с зарегистрированными разделами, хранится в каталоге, соответствующем этому уникальному ИД.

Для регистрации системы с помощью графического интерфейса выполните следующие действия:

1. Запустите графический интерфейс с помощью команды **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. В меню навигации выберите **Регистрация**.
3. Введите имя хоста и идентификационные данные SSH системы.
4. Нажмите кнопку **Зарегистрировать**.

Понятия, связанные с данным:

“Проверка системы”
В статье описана процедура аттестации системы из командной строки или с помощью графического интерфейса.

Проверка системы

В статье описана процедура аттестации системы из командной строки или с помощью графического интерфейса.

Для запроса целостности загрузки системы выполните в утилите проверки следующую команду:

```
openpts <имя-хоста>
```

Для аттестации системы с помощью графического интерфейса выполните следующие действия:

1. Выберите категорию в меню навигации.
2. Выберите одну или несколько систем для аттестации.
3. Нажмите кнопку **Проверка**.

Регистрация и аттестация системы без пароля

Запрос аттестации отправляет с помощью протокола SSH. Для организации соединений SSH между утилитой проверки и программой сбора статистики без пароля установите в программе сбора статистики сертификат утилиты проверки.

Для настройки сертификата утилиты проверки в системе программы сбора статистики выполните следующие действия:

- В утилите проверки выполните следующие команды:

  ```
  ssh-keygen    # No passphrase
  scp ~/.ssh/id_rsa.pub <программа-сбора-статистики>:/tmp
  ```

- В программе сбора статистики выполните следующую команду:

  ```
  cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
  ```

Управление функцией Надежная загрузка

Здесь описана процедура управления результатами удостоверения Надежной загрузки.

Анализ результатов аттестации

В статье описана процедура для просмотра и изучения результатов аттестации.

Аттестация может выполниться с одним из следующих состояний:

1. Запрос аттестации не выполнен: запрос аттестации не выполнен. Возможные причины неполадки приведены в разделе Устранение неполадок.
2. Допустимая целостность системы: аттестация выполнена успешно, загрузка системы соответствует справочной информации, зафиксированной утилитой проверки. Это означает успешное выполнение Trusted Boot.
3. Целостность системы нарушена: запрос аттестации выполнен, но обнаружены различия между собранной во время загрузки системы информацией и справочной информацией, зафиксированной утилитой проверки. Это означает ненадежное выполнение загрузки.

Аттестация также выдает отчет об обновлении, примененном к программе сбора статистики, с помощью следующего сообщения:

Доступно обновление системы: это сообщение уведомляет, что было выполнено обновление программы сбора статистики, и доступен набор обновленной справочной информации, готовый к следующей загрузке. Пользователю в утилите проверки будет выдан запрос о принятии или отклонении обновлений. Например, пользователь может принимать эти обновления, если обладает информацией о процессах в программе сбора статистики.

Для исследования ошибки аттестации с помощью графического интерфейса выполните следующие действия:

1. Выберите категорию в меню навигации.
2. Выберите систему для проверки.
3. Щелкните дважды на записи, соответствующей системе. Будет показано окно свойств. В этом окне содержится протокол выполненной с ошибкой аттестации.

Удаление систем

В разделе описана процедура удаления системы из базы данных компонента проверки.

Для удаления системы из базы данных компонента проверки выполните следующую команду:

```
openpts -r <имя-хоста>
```

Устранение неполадок функции Надежная загрузка

Существует несколько общих сценариев и корректирующих действий, требуемых для определения причины невозможности удостоверения при использовании функции Надежная загрузка.

Команда **openpts** объявляет систему как неверную, если текущее состояние загрузки системы не соответствует справочной информации, хранимой в верификаторе. Команда **openpts** определяет возможную причину нарушения целостности. Существует несколько переменных в полной загрузке AIX, и неудачное удостоверение требует анализа для определения причины неполадки.

В следующей таблице перечислены некоторые обычные сценарии и действия по исправлению, применяемые для определения причины неполадки:

Таблица 2. Некоторые обычные сценарии устранения неполадок

Причина неполадки	Возможные причины неполадки	Рекомендуемый способ исправления

Удостоверение не выполнено.	• Неверное имя хоста.
	• Не существует сетевого маршрута между источником и назначением.
	• Неверные идентификационные данные защиты.
		Проверьте соединение Защищенной оболочки (SSH) с помощью следующей команды:
		`ssh ptsc@hostname`
		
		Если соединение SSH установлено успешно, проверьте следующие причины неудачного удостоверения:
		• В удостоверяемой системе не запущен демон **tcsd**.
		• Удостоверяемая система не инициализирована командой **ptsc**. Этот процесс должен выполняться автоматически в процессе запуска системы, но проверьте наличие каталога `/var/ptsc/` в коллекторе. Если каталог `/var/ptsc/` не существует, выполните следующую команду в коллекторе:
		`ptsc -i`

Встроенное ПО CEC было изменено.	• Применено обновление встроенного ПО. • LPAR перенесен в систему, которая выполняет другую версию встроенного ПО.	Проверьте уровень встроенного ПО системы, в которой расположен LPAR.
Ресурсы, выделенные для LPAR, изменены.	CPU или память, выделенные для LPAR, изменены.	Проверьте профайл раздела в HMC.
Встроенное ПО изменено для адаптеров, доступных в LPAR.	Аппаратное устройство добавлено или удалено из LPAR.	Проверьте профайл раздела в HMC.
Список устройств, присоединенных к LPAR, изменен.	Аппаратное устройство добавлено или удалено из LPAR.	Проверьте профайл раздела в HMC.
Изменен загрузочный образ, который содержит ядро операционной системы.	• Применено обновление AIX, и верификатор не знает об этом. • Выполнена команда **bosboot**.	• Проверьте вместе с администратором коллектора, выполнялось ли какое-либо обслуживание перед последней операцией загрузки. • Проверьте протоколы в коллекторе на наличие обслуживающих действий.

Таблица 2. Некоторые обычные сценарии устранения неполадок (продолжение)

Причина неполадки	Возможные причины неполадки	Рекомендуемый способ исправления
LPAR загружен из другого устройства.	• Выполнена регистрация сразу после сетевой установки. • Система загружена с устройства обслуживания.	Флаги и устройство загрузки можно проверить может быть команды **bootinfo**. Если регистрация выполнена сразу после установки Управления сетевой установкой (NIM) и перед операцией загрузки, сведения регистрации относятся к сетевой установке, а не к последующей загрузки с диска. Эта регистрация может быть исправлена путем удаления ее удаления и повторной регистрации логического раздела.
Вызвано интерактивное меню загрузки Служб управления системой (SMS).		Процесс загрузки должен быть выполнен непрерывно, без вмешательства пользователя, чтобы система считалась надежной. Ввод меню загрузки SMS приводит к ненадежности загрузки.
База данных надежного выполнения (TE) изменена.	• Двоичные файлы добавлены или удалены из базы данных TE. • Двоичные файлы в базе данных изменены.	Выполните команду **trustchk** для проверки базы данных.

Понятия, связанные с данным:

“Подготовка к исправлению” на стр. 6
Описанная здесь информация о компоненте Надежная загрузка служит руководством для определения ситуаций, которые могут потребовать исправления. Она не влияет на процесс загрузки.

“Концепции Надежной загрузки” на стр. 4
Важно понимать целостность процесса загрузки и способ классификации загрузки в качестве надежной или ненадежной.

Информация, связанная с данной:

Использование HMC

Надежный брандмауэр

Функция Надежный брандмауэр предоставляет защиту на уровне виртуализации, которая повышает производительность и эффективность использования ресурсов при связи между областями защиты виртуальных LAN (VLAN) на одном сервере Power Systems. Надежный брандмауэр снижает загрузку внешней сети, перенося возможности фильтрации пакетов брандмауэра, удовлетворяющих заданным правилам, на уровень виртуализации. Эта возможность фильтрации управляется легко определяемыми правилами фильтрации сети, которые позволяют защищенному сетевому потоку данных переходить между областями защиты VLAN, не покидая виртуальной среды. Надежный брандмауэр защищает и маршрутизирует внутренний сетевой поток данных между операционными системами AIX, IBM i и Linux.

Концепции Надежного брандмауэра

Существует несколько основных концепций для понимания того, когда следует использовать Надежный брандмауэр.

Аппаратное обеспечение Power Systems можно настроить с помощью нескольких областей защиты виртуальной LAN (VLAN). Настроенная пользователем стратегия, созданная как правило фильтрации Надежного брандмауэра, позволяет направлять некоторый сетевой поток данных через области VLAN, оставляя его внутренним для уровня виртуализации. Это подобно введению подключенного к сети физического брандмауэра в виртуализированную среду, который предоставляет более эффективный с точки зрения производительности метод реализации возможностей брандмауэра для виртуализированных центров обработки данных.

С помощью Надежного брандмауэра можно настроить правила, разрешающие передавать определенные типы потока данных непосредственно из одной VLAN в Сервер виртуального ввода-вывода (VIOS) в другую VLAN в том же VIOS, поддерживая в то же время высокий уровень защиты посредством ограничения других типов потока данных. Это настраиваемый брандмауэр на уровне виртуализации серверов Power Systems.

Пример в рис. 1 предназначен для того, чтобы научить безопасно и эффективно передавать информацию из LPAR1 в VLAN 200 и из LPAR2 в VLAN 100. Без Надежного брандмауэра информация, предназначенная для LPAR2 из LPAR1, отправляется из внутренней сети на маршрутизатор, который направляет ее назад в LPAR2.

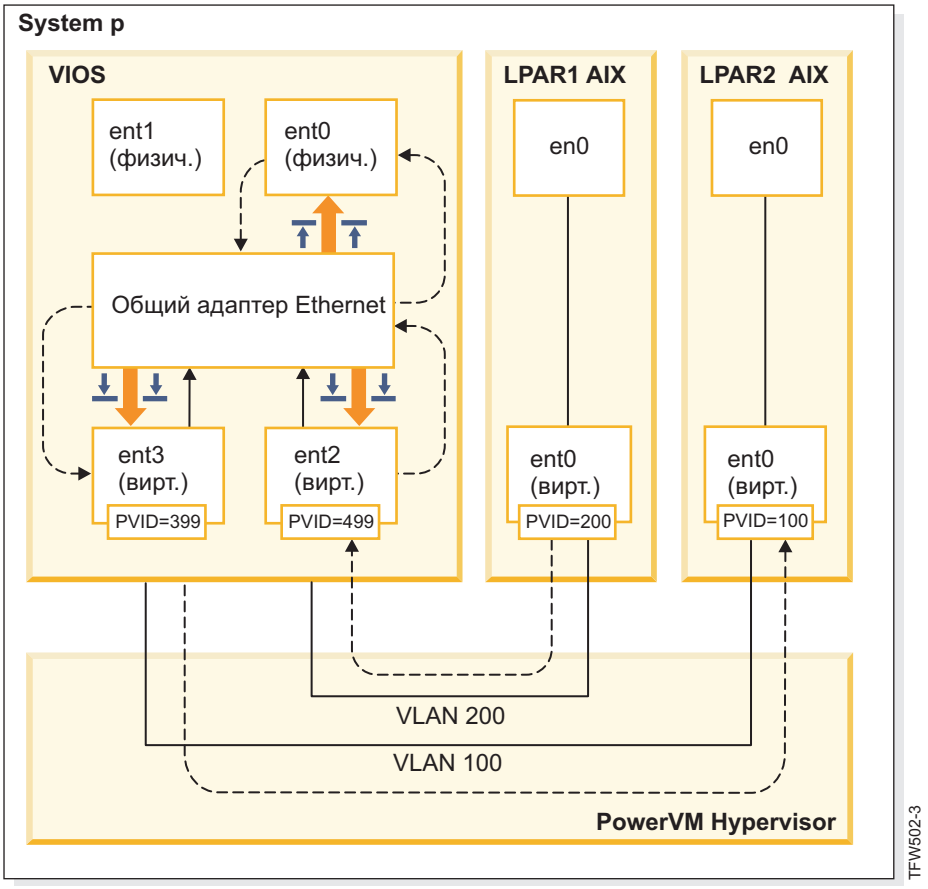

Рисунок 1. Пример передачи информации между VLAN без Надежного брандмауэра

С помощью Надежного брандмауэра можно настроить правила передачи информации из LPAR1 в LPAR2, так чтобы она не покидала внутреннюю сеть. Этот путь показан в рис. 2 на стр. 12.

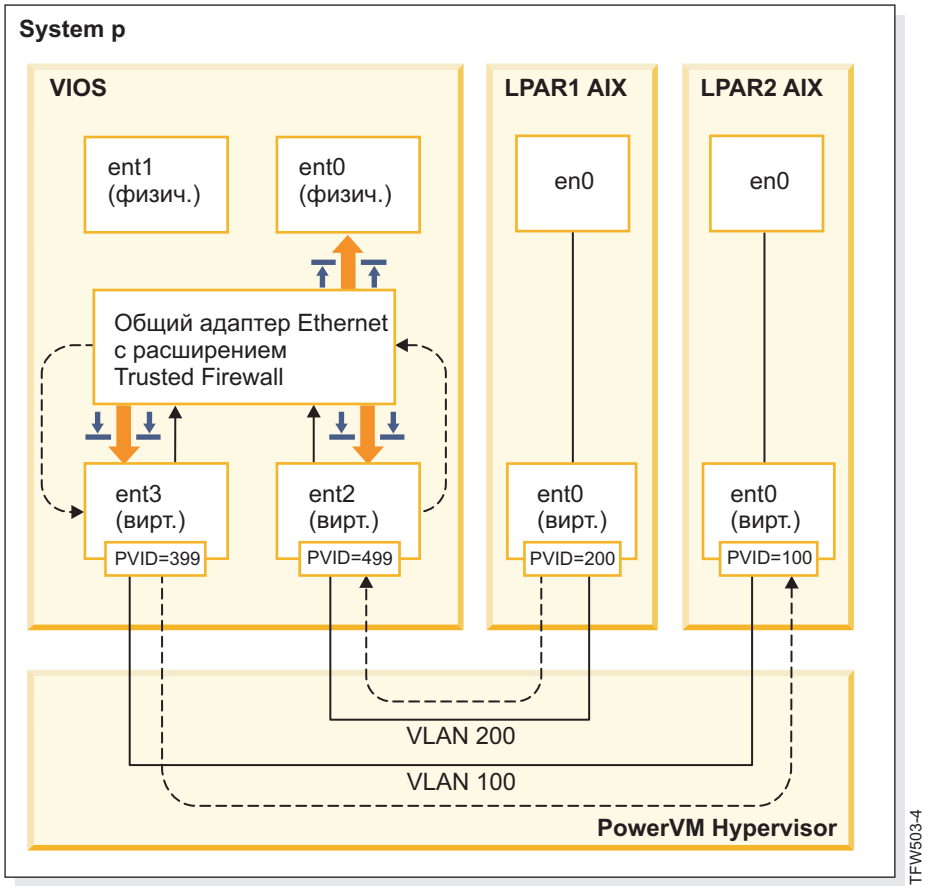

Рисунок 2. Пример передачи информации между VLAN с помощью Надежного брандмауэра

Правила конфигурации, позволяющие безопасно передавать определенную информацию между VLAN, сокращают путь к назначению. Надежный брандмауэр использует Общий адаптер Ethernet (SEA) и расширение ядра Виртуальной машины защиты (SVM) для обеспечения связи.

Общий адаптер Ethernet

SEA — это начало и конец маршрутизации. Когда SVM зарегистрирован, SEA получает пакеты и перенаправляет их в SVM. Если SVM определяет, что пакет предназначен для LPAR на том же сервере Power Systems, он обновляет заголовок второго уровня пакета. Пакет возвращается в SEA для пересылки в окончательное назначение или внутри системы, или во внешней сети.

Виртуальная машина защиты

SVM — это место применения правил фильтрации. Правила фильтрации необходимы для обеспечения защиты во внутренней сети. После регистрации SVM в SEA пакеты направляются в SVM перед их отправкой во внешнюю сеть. На основании активных правил фильтрации SVM определяет, остается ли пакет во внутренней сети или передается во внешнюю сеть.

Установка Надежного брандмауэра

Установка Надежного брандмауэра PowerSC подобна установке любой другой функции PowerSC.

Предварительные требования:

- PowerSC версии ниже 1.1.1.0 не имеет требуемого набора файлов для установки Надежного брандмауэра. Убедитесь в том, что у вас есть установочный компакт-диск PowerSC для версии 1.1.1.0 или выше.
- Для того чтобы воспользоваться Надежным брандмауэром, необходимо уже настроить виртуальные LAN (VLAN) с помощью Консоли аппаратного обеспечения (HMC) или Сервер виртуального ввода-вывода (VIOS).

Надежный брандмауэр предоставлен в качестве дополнительного набора файлов на установочном компакт-диске PowerSC Standard Edition. Имя файла: `powerscStd.svm.rte`. Можно добавить Надежный брандмауэр в существующий экземпляр PowerSC версии 1.1.0.0 или выше или установить его в составе новой установки PowerSC версии 1.1.1.0 или выше.

Для того чтобы добавить функцию Надежный брандмауэр в существующий экземпляр PowerSC:

1. Убедитесь в том, что запущен VIOS версии 2.2.1.4 или более поздней версии.
2. Вставите установочный компакт-диск PowerSC версии 1.1.1.0 или загрузите его образ.
3. Выполните команду **oem_setup_env**.
4. Используйте команду **installp** или инструмент SMIT для установки набора файлов `PowerscStd.svm.rte`.

Информация, связанная с данной:

“Установка PowerSC Standard Edition 1.1.3” на стр. 3
Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Настройка Надежного брандмауэра

Дополнительная настройка параметров конфигурации требуется для функции Надежный брандмауэр после ее установки.

Монитор Надежного брандмауэра

Монитор Надежного брандмауэра анализирует поток данных в системе из различных логических разделов (LPAR) для предоставления полезной информации, помогающей определить, повышает ли выполняющийся Надежный брандмауэр производительность системы.

Если функция монитора Надежного брандмауэра записывает значительный объем потока данных из различных виртуальных LAN (VLAN), которые находятся в одном и том же центральном электронном комплексе, включение Надежного брандмауэра должно принести пользу в системе.

Для того чтобы включить монитор Надежного брандмауэра, введите следующую команду:

```
vlantfw -m
```

Для того чтобы показать результаты монитора Надежного брандмауэра, введите следующую команду:

```
vlantfw -D
```

Для того чтобы выключить монитор Надежного брандмауэра, введите следующую команду:

```
vlantfw -M
```

Ведение протоколов Надежного брандмауэра

Ведение протоколов Надежного брандмауэра составляет список путей сетевого потока данных в центральном электронном комплексе. Список показывает фильтры, используемые Надежным брандмауэром для маршрутизации потока данных.

Когда монитор Надежного брандмауэра определяет, что внутренняя маршрутизация потока данных повышает эффективность, агент ведения протоколов Надежного брандмауэра составляет список путей в файле `svm.log`. Максимальный размер файла `svm.log` — 16 Мб. Если записи превышают ограничение 16 Мб, прежние записи удаляются из файла протокола.

Для того чтобы запустить ведение протоколов Надежного брандмауэра, введите следующую команду:

```
vlantfw -l
```

Для того чтобы завершить ведение протоколов Надежного брандмауэра, введите следующую команду:

```
vlantfw -L
```

Файл протокола можно просмотреть в следующем расположении: `/home/padmin/svm/svm.log`.

Несколько Общих адаптеров Ethernet

Можно настроить Надежный брандмауэр на системы, использующие несколько Общих адаптеров Ethernet.

Некоторые конфигурации используют множественные Общие адаптеры Ethernet (SEA) в одном Сервер виртуального ввода-вывода (VIOS). Несколько SEA могут обеспечить преимущества защиты с передачей управления и использования уровней ресурсов. Надежный брандмауэр поддерживает маршрутизацию между несколькими SEA в одном и том же VIOS.

рис. 3 показывает среду с несколькими SEA.

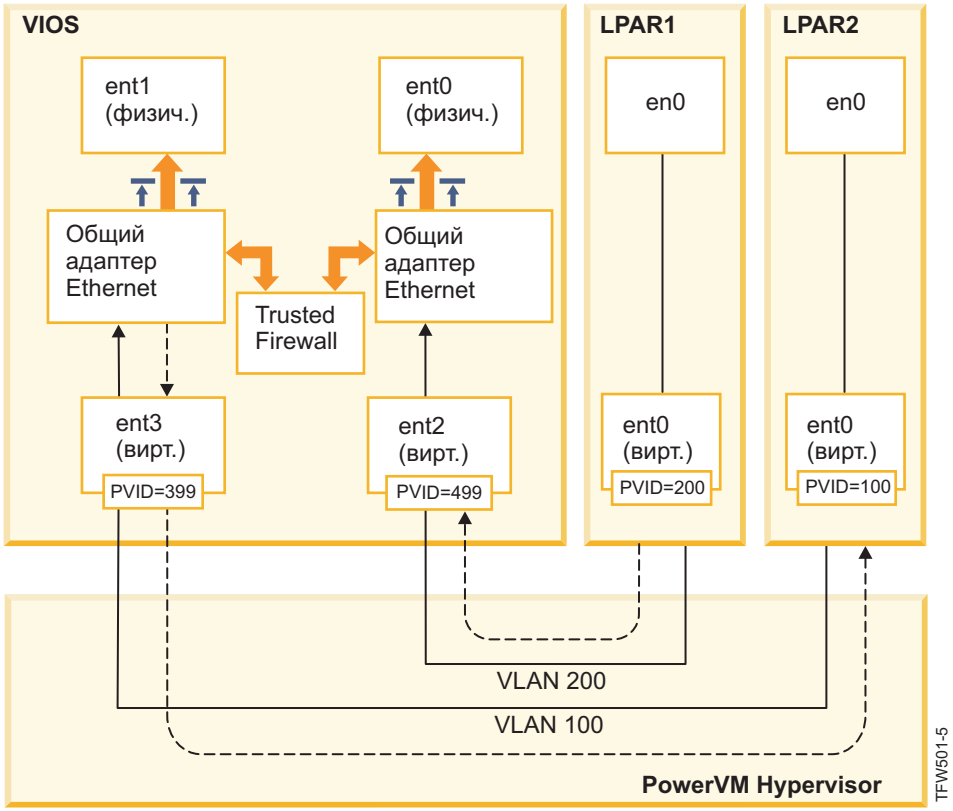

Рисунок 3. Конфигурация с несколькими Общими адаптерами Ethernet в одном VIOS

Ниже приведены примеры конфигураций с несколькими SEA, поддерживаемых Надежным брандмауэром:

- SEA настроены с помощью магистральных адаптеров в одном виртуальном коммутаторе гипервизора Power. Эта конфигурация поддерживается, так как все SEA получают сетевой поток данных с помощью различных ИД VLAN.
- SEA настроены с помощью магистральных адаптеров в различных виртуальных коммутаторах гипервизора Power, и все магистральные адаптеры находятся в различных ИД VLAN. В этой конфигурации все SEA также получают сетевой поток данных с помощью различных ИД VLAN.
- SEA настроены с помощью магистральных адаптеров в различных виртуальных коммутаторах гипервизора Power, и одинаковые ИД VLAN повторно используются в виртуальных коммутаторах. В этом случае поток данных для обоих SEA имеет одинаковые ИД VLAN.

  Примером этой конфигурации является наличие LPAR2 в VLAN200 с виртуальным коммутатором 10 и LPAR3 в VLAN200 с виртуальным коммутатором 20. Так как оба LPAR и соответствующие им SEA используют одинаковый ИД VLAN (VLAN200), оба SEA имеют доступ к пакетам с помощью этого ИД VLAN.

Невозможно включить мост для более чем одного VIOS. По этой причине следующие конфигурации с несколькими SEA не поддерживаются Надежным брандмауэром:

- Несколько VIOS и несколько драйверов SEA.
- Распределение нагрузки с помощью избыточного SEA: магистральные адаптеры, настроенные для маршрутизации внутри VLAN, не могут быть разбиты между серверами VIOS.

Удаление Общих адаптеров Ethernet

Действия по удалению Общих адаптеров Ethernet из системы должны быть выполнены в определенном порядке.

Для того чтобы удалить Общий адаптер Ethernet (SEA) из системы, выполните следующие действия:

1. Удалите Виртуальную машину защиты, связанную с SEA, введя следующую команду:

   ```
   rmdev -dev svm
   ```

2. Удалите SEA, введя следующую команду:

   ```
   rmdev -dev ИД общего адаптера
   Ethernet
   ```

Примечание: Удаление SEA перед удалением SVM может привести к сбою системы.

Создание правил

Можно создать правила маршрутизации между VLAN с помощью Надежного брандмауэра.

Для того чтобы включить функции маршрутизации в Надежном брандмауэре, необходимо создать правила, указывающие, какие связи разрешены. Для обеспечения повышенной защиты не существует одного правила, которое разрешает связь между всеми VLAN в системе. Каждое разрешенное соединение требует собственного правила, хотя каждое активированное правило разрешает связь в обоих направлениях для указанных в нем конечных точек.

Так как правило создается в интерфейсе Сервер виртуального ввода-вывода (VIOS), дополнительная информация о командах доступна в наборе разделов VIOS информационной системы Power Systems Hardware Information Center.

Для того чтобы создать правило, выполните следующие действия:

1. Откройте интерфейс командной строки VIOS.
2. Инициализируйте драйвер SVM, введя следующую команду:

   ```
   mksvm
   ```

3. Запустите Надежный брандмауэр, введя команду запуска:

   ```
   vlantfw -s
   ```

4. Для того чтобы показать все известные MAC-адреса и IP-адреса LPAR, введите следующую команду:

   ```
   vlantfw -d
   ```

   Вам потребуются MAC-адреса и IP-адреса логических разделов (LPAR), для которых создаются правила.

5. Создайте правило фильтрации, чтобы разрешить связь между двумя LPAR (LPAR1 и LPAR2), введя одну из следующих команд:
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -O gt -P 23`

   Примечание: Одно правило фильтрации по умолчанию разрешает связь в обоих направлениях в зависимости от записей протокола и порта. Например, можно разрешить соединение Telnet из LPAR1 в LPAR2, выполнив следующую команду:

   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o
   any -p 0 -O eq -P 23
   ```

6. Активируйте все правила фильтрации в ядре, введя следующую команду:
   ```
   mkvfilt -u
   ```

Примечание: Эта процедура активирует это правило и все другие правила фильтрации, которые существуют в системе.

Дополнительные примеры

Следующие примеры показывают некоторые другие правила фильтрации, которые можно создать с помощью Надежного брандмауэра.

- Для того чтобы разрешить связь Secure Shell из LPAR в VLAN 100 в LPAR в VLAN 200, введите следующую команду:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- Для того чтобы разрешить передачу потока данных между всеми портами 0 - 499, введите следующую команду:
  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- Для того чтобы разрешить передачу всего потока данных TCP между LPAR, введите следующую команду:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  Если порты или операции портов не указаны, поток данных может использовать все порты.
- Для того чтобы обмен сообщениями Internet Control Message Protocol между LPAR, введите следующую команду:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Понятия, связанные с данным:

“Деактивация правил”
Можно деактивировать правила, которые разрешают маршрутизацию между VLAN в функции Надежный брандмауэр.

Ссылки, связанные с данной:

“Команда genvfilt” на стр. 33

“Команда mkvfilt” на стр. 34

“Команда vlantfw” на стр. 44

Информация, связанная с данной:

Virtual I/O Server (VIOS)

Деактивация правил

Можно деактивировать правила, которые разрешают маршрутизацию между VLAN в функции Надежный брандмауэр.

Так как правила деактивируются в интерфейсе Сервер виртуального ввода-вывода (VIOS), дополнительная информация о командах и процессе доступна в наборе разделов VIOS информационной системы Power Systems Hardware Information Center.

Для того чтобы деактивировать правило, выполните следующие действия:

1. Откройте интерфейс командной строки VIOS.
2. Для того чтобы показать все активные правила фильтрации, введите следующую команду:
   ```
   lsvfilt -a
   ```

   Можно опустить флаг **-a**, чтобы показать все правила фильтрации, которые хранятся в Администраторе данных объектов.
3. Запомните идентификатор правила фильтрации, которое деактивируется. Для этого примера идентификатором правила фильтрации является 23.

4. Деактивируйте правило фильтрации 23, когда оно активно в ядре, введя следующую команду:
   `rmvfilt -n 23`

   Для того чтобы деактивировать все правила фильтрации в ядре, введите следующую команду:
   `rmvfilt -n all`

Понятия, связанные с данным:

“Создание правил” на стр. 15
Можно создать правила маршрутизации между VLAN с помощью Надежного брандмауэра.

Ссылки, связанные с данной:

“Команда lsvfilt” на стр. 34

“Команда rmvfilt” на стр. 44

Защищенные протоколы

Защищенные протоколы PowerVM позволяют LPAR в системе AIX записывать файлы протокола в присоединенный Сервер виртуального ввода-вывода (VIOS). Данные передаются в VIOS непосредственно через гипервизор, и сетевая связь не требуется между LPAR клиента и VIOS.

Виртуальные протоколы

Администратор Сервер виртуального ввода-вывода (VIOS) создает и управляет файлами протоколов, и они представляются в операционной системе AIX как устройства виртуальных протоколов в каталоге `/dev`, подобно виртуальным дискам или виртуальным оптическим носителям.

Сохранение файлов протокола увеличивает уровень надежности записей, так как они не могут быть изменены пользователем с правами доступа root в клиенте LPAR, где они были сгенерированы. Несколько устройств виртуальных протоколов могут быть присоединены к одному и тому же LPAR клиента, и каждый протокол является отдельным файлом в каталоге `/dev`.

Защищенные протоколы позволяют объединять данные протоколов из нескольких LPAR клиента в одной файловой системе, доступной из VIOS. Поэтому, VIOS предоставляет одно расположение в системе для анализа и архивации протоколов. Администратор LPAR клиента может настроить приложения и операционную систему AIX на запись данных в устройства виртуальных протоколов, подобно записи данных в локальные файлы. Подсистема Audit AIX может быть настроена для перенаправления контрольных записей в виртуальные протоколы и другие службы AIX, такие как syslog, и работать с их существующей конфигурацией для перенаправления данных в виртуальные протоколы.

Для того чтобы настроить виртуальный протокол, администратор VIOS должен указать имя виртуального протокола со следующими отдельными компонентами:

- Имя клиента
- Имя протокола

Для имен двух компонентов администратор VIOS может установить любые значения, но имя клиента обычно совпадает для всех виртуальных протоколов, присоединенных к данному LPAR (например, имя хоста LPAR). Имя протокола используется для определения назначения протокола (например, audit или syslog).

В AIX LPAR каждое устройство виртуального протокола представлено двумя функционально эквивалентными файлами в файловой системе `/dev`. Первый файл назван после устройства, например, `/dev/vlog0`, а второй файл имеет имя, полученное соединением префикса `vl` с именем протокола и номером устройства. Например, если устройство виртуального протокола `vlog0` имеет имя протокола `audit`, он присутствует в файловой системе `/dev` как `vlog0` и `vlaudit0`.

Информация, связанная с данной:

Создание виртуальных протоколов

Обнаружение устройств виртуальных протоколов

После создания администратором VIOS устройств виртуальных протоколов и присоединения их к LPAR клиента, необходимо обновить конфигурацию устройства LPAR клиента, чтобы устройства стали видимы.

Администратор LPAR клиента обновляет параметры одним из следующих методов:

- Перезагрузка LPAR клиента
- Выполнение команды **cfgmgr**

Выполнение команды **lsdev** для просмотра устройств виртуальных протоколов. Устройства по умолчанию имеют префикс `vlog`. Пример вывода команды **lsdev** в AIX LPAR, в котором находятся два устройства виртуальных протоколов:

```
lsdev
vlog0  Virtual Log Device
vlog1  Virtual Log Device
```

Проверьте свойства отдельных устройств виртуальных протоколов с помощью команды `lsattr -El <имя устройства>`, которая имеет вывод, подобный следующему:

```
lsattr -El vlog0
PCM                         Path Control Module            False
client_name    dev-lpar-05 Client Name                     False
device_name    vlsyslog0   Device Name                     False
log_name       syslog      Log Name                        False
max_log_size   4194304     Maximum Size of Log Data File  False
max_state_size 2097152     Maximum Size of Log State File False
pvid           none        Physical Volume Identifier     False
```

Этот вывод показывает имя клиента, имя устройства и объем данных протокола, которые могут быть сохранены в VIOS.

Виртуальный протокол хранит два типа данных протокола:

- Данные протокола: необработанные данные протокола, генерируемые приложениями в AIX LPAR.
- Данные состояния: информация о времени настройки, открытия, закрытия устройств, а также других операций, использованных для анализа протокола.

Администратор VIOS указывает объем **данных протокола** и **данных состояния**, которые могут быть сохранены для каждого виртуального протокола, и этот объем задается атрибутами `max_log_size` и `max_state_size`. Когда объем сохраненных данных превышает заданное ограничение, более ранние данные перезаписываются. Администратор VIOS должен обеспечить периодический сбор и архивацию данных протокола для их сохранения.

Установка Защищенных протоколов

Можно установить функцию Защищенные протоколы PowerSC с помощью интерфейса командной строки или инструмента SMIT.

Предварительными требованиями для функции Защищенные протоколы являются VIOS 2.2.1.0 или выше и IBM AIX 6 с технологическим пакетом обслуживания 7 или IBM AIX 7 с технологическим пакетом обслуживания 1.

Имя файла для установки функции Защищенные протоколы — `powerscStd.vlog`, который включен в установочный компакт-диск PowerSC Standard Edition.

Для того чтобы установить функцию Защищенные протоколы:

| 1. Убедитесь в том, что запущен VIOS версии 2.2.1.0 или более поздней версии.
| 2. Вставите установочный компакт-диск PowerSC или загрузите его образ.
| 3. Используйте команду **installp** или инструмент SMIT для установки набора файлов `powerscStd.vlog`.

| **Информация, связанная с данной**:

| “Установка PowerSC Standard Edition 1.1.3” на стр. 3
| Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Настройка Trusted Logging

В статье описана процедура настройки Trusted Logging в подсистеме контроля AIX Audit и утилиты syslog.

Настройка подсистемы контроля AIX

В дополнение к записи протокола в локальной файловой системе подсистему контроля AIX можно настроить для записи двоичных данных в виртуальное устройство протокола.

Примечание: Перед настройкой подсистемы контроля AIX необходимо выполнить процедуру, описанную в разделе “Обнаружение устройств виртуальных протоколов” на стр. 18.

Для настройки подсистемы контроля AIX выполните следующие действия:

1. Настройте подсистему контроля AIX для ведения протокола данных в двоичном режиме (`auditbin`).
2. Активируйте функцию ведения надежных протоколов для контроля AIX путем редактирования файла конфигурации `/etc/security/audit/config`.
3. Добавьте параметр `virtual_log = /dev/vlog0` в раздел `bin:`.

   Примечание: Инструкция нужна, если администратору LPAR требуется записать данные `auditbin` в `/dev/vlog0`.
4. Перезапустите подсистему контроля AIX в следующей последовательности:

```
audit shutdown
audit start
```

Кроме записи протоколов в локальной файловой системе контрольные записи можно сохранить в Сервер виртуального ввода-вывода (VIOS) в указанных виртуальных устройствах протокола. Сохранение протоколов управляется существующими параметрами `bin1` и `bin2` в разделе `bin:` файла конфигурации `/etc/security/audit/config`.

Информация, связанная с данной:

Подсистема контроля

Настройка syslog

С помощью добавления правил в файл `/etc/syslog.conf` syslog можно настроить для записи сообщений в виртуальные протоколы.

Примечание: Перед настройкой файла `/etc/syslog.conf` необходимо выполнить процедуру, описанную в разделе “Обнаружение устройств виртуальных протоколов” на стр. 18.

Можно изменить файл `/etc/syslog.conf` для получения сообщений протокола, основанных на следующих критериях:

- Утилита
- Приоритет

При использовании виртуальных протоколов для сообщений syslog необходимо настроить файл `/etc/syslog.conf` в соответствии с правилами записи требуемых сообщений в соответствующий виртуальный протокол в каталоге `/dev`.

Например для отправки сообщений уровня отладки, созданных любой утилитой, в виртуальный протокол `vlog0` добавьте в файл `/etc/syslog.conf` следующую строку:

```
*.debug /dev/vlog0
```

Примечание: Не применяйте утилиты циклической смены протоколов, доступные в демоне `syslogd`, для команд, выполняющих прямую запись данных в виртуальные протоколы. Файлы в файловой системе `/dev` не являются обычными файлами и их нельзя переименовывать и перемещать. Администратор VIOS должен настроить циклическую смену виртуальных протоколов в VIOS.

После изменения конфигурации демон `syslogd` необходимо перезапустить с помощью следующей команды:

```
refresh -s syslogd
```

Информация, связанная с данной:

Демон syslogd

Запись данных в устройства виртуальных протоколов

Произвольные данные можно записать в устройство виртуального протокола, открыв соответствующий файл в каталоге `/dev` и записав в него данные. Виртуальный протокол может быть открыт одним процессом в один момент времени.

Например:

Для записи сообщений в устройства виртуальных протоколов с помощью команды **echo** введите следующую команду:

```
 echo "Log Message" > /dev/vlog0
```

Для сохранения файлов в устройствах виртуальных протоколов с помощью команды **cat** введите следующую команду:

```
cat /etc/passwd > /dev/vlog0
```

Максимальный размер отдельной записи ограничен 32 Кб, и программы, которые пытаются записать больше данных в одной операции записи, получают ошибку ввода/вывода (EIO). Утилиты интерфейса командной строки (CLI), такие как команда **cat**, автоматически разбивают передачу на операции записи по 32 Кб.

Надежное сетевое соединение и управление исправлениями

Надежное сетевое соединение (TNC) является компонентом группы надежных вычислений (TCG), которая предоставляет спецификации для проверки целостности конечной точки. TNC определяет открытую архитектуру решения, которая помогает администраторам применять стратегии для эффективного управления доступом к сетевой инфраструктуре.

Концепции структуры Надежное сетевое соединение

В этом разделе описаны компоненты, настройка защищенного соединения и система управления исправлениями в структуре Надежное сетевое соединение (TNC).

Компоненты Надежного сетевого соединения

В этом разделе описаны компоненты структуры Надежное сетевое соединение (TNC).

Модель TNC состоит из следующих компонентов:

Сервер структуры Надежное сетевое соединение:

Сервер структуры Надежное сетевое соединение (TNC) определяет клиентов, которые добавлены в сеть, и инициирует на них проверку.

Клиент TNC предоставляет требуемую информацию об уровне набора файлов на сервер для проверки. Сервер определяет, находится ли клиент на уровне, настроенном администратором. Если клиент не совместим, сервер TNC уведомляет администратора о необходимости исправления.

Сервер TNC инициирует проверки на клиентах, которые пытаются получить доступ к сети. Сервер TNC загружает набор верификаторов измерения целостности (IMV), которые могут потребовать измерения целостности от клиентов и проверить их. AIX имеет IMV по умолчанию, который проверяет набор файлов и уровень исправления защиты в системах. Сервер TNC является структурой, которая загружает множество модулей IMV и управляет ими. Для проверки клиента он использует IMV, чтобы запросить информацию от клиентов, и проверяет их.

Управление исправлениями:

Сервер структуры Надежное сетевое соединение (TNC) интегрирован с SUMA для предоставления решения по управлению исправлениями.

AIX SUMA загружает последние пакеты обновления и исправления защиты, доступные в IBM ECC и Fix Central. TNC и демон управления исправлениями передает последнюю обновленную информацию на сервер TNC, который служит в качестве набора файлов контрольной версии для проверки клиентов.

Демон **tncpmd** должен быть настроен для управления загрузками Ассистента по управлению служебными обновлениями (SUMA) и передачи информации набора файлов на сервер TNC. Этот демон должен быть расположен в системе, подключенной к Интернет, чтобы иметь возможность автоматически загружать обновления. Для использования сервера управления исправлениями TNC без подключения к Интернет можно зарегистрировать пользовательское хранилище исправлений на сервере управления исправлениями TNC.

Примечание: Сервер TNC и демон **tncpmd** могут быть расположены в одной системе.

Клиент структуры Надежное сетевое соединение:

Клиент структуры Надежное сетевое соединение (TNC) предоставляет информацию, требуемую сервером TNC для проверки.

Сервер определяет, находится ли клиент на уровне, настроенном администратором. Если клиент не совместим, сервер TNC уведомляет администратора о необходимости обновления.

Клиент TNC загружает IMC при запуске и использует IMC для сбора требуемой информации.

Определитель IP структуры Надежное сетевое соединение:

Сервер структуры Надежное сетевое соединение (TNC) может автоматически инициировать проверку на клиентах, входящих в сеть. Определитель IP, который выполняется в разделе Сервер виртуального ввода-вывода (VIOS), обнаруживает новых клиентов, обслуживаемых VIOS, и отправляет их IP-адреса на сервер TNC. Сервер TNC проверят клиента в соответствии с определенной стратегией.

Защищенная связь в структуре Надежное сетевое соединение

Демоны TNC связываются по зашифрованным каналам, предоставленным TLS или SSL (Secure Sockets Layer).

Защищенная связь обеспечивает идентификацию и защиту данных и команд, передаваемых по сети. Каждая система должна иметь собственный ключ и сертификат, которые генерируются при выполнении команды инициализации для компонентов. Этот процесс полностью прозрачен для администратора и требует от него минимум действий.

Для проверки нового клиента его сертификат должен быть импортирован в базу данных сервера. Первоначально сертификат помечается как ненадежный, а затем администратор использует команду **psconf** для просмотра и пометки сертификата как надежного, введя следующую команду:

```
psconf certadd -i<ip> -t<TRUSTED|UNTRUSTED>
```

Для использования других ключа и сертификата команда **psconf** предоставляет опцию для импорта сертификата.

Для импорта сертификата с сервера введите следующую команду:

```
psconf import  -S -k<key filename> -f<key filename>
```

Для импорта сертификата с клиента введите следующую команду:

```
psconf import -C -k<key filename> -f<key filename>
```

Протокол структуры Надежное сетевое соединение

Протокол структуры Надежное сетевое соединение (TNC) используется со структурой TNC для поддержки целостности сети.

TNC предоставляет спецификации для проверки целостности конечных точек. Доступ к конечным точкам предоставляется на основании показателей целостности важных компонентов, которые могут повлиять на операционную среду. Структура TNC позволяет администраторам отслеживать целостность систем в сети. TNC интегрирован с инфраструктурой поставки исправлений AIX для компоновки полного решения по управлению исправлениями.

Спецификации TNC должны удовлетворять требованиям архитектуры систем AIX и семейство POWER. Компоненты TNC предназначены для предоставления полного решения по управлению исправлениями в операционной системе AIX. Эта конфигурация позволяет администраторам эффективно управлять конфигурациями программного обеспечения в развертываниях AIX. Она предоставляет инструменты для проверки уровней исправлений систем и генерации отчетов о клиентах, которые не совместимы. Кроме того, управление исправлениями упрощает процесс загрузки и установки исправлений.

Модули IMC и IMV

Сервер или клиент структуры Надежное сетевое соединение (TNC) внутренне использует модули Коллектор измерений целостности (IMC) и Верификатор измерений целостности (IMV) для проверки сервера.

Эта структура позволяет загружать несколько модулей IMC и IMV на сервер и клиенты. Модуль, который выполняет и проверку уровня операционной системы и набора файлов, по умолчанию поставляется с операционной системой AIX. Для доступа к модулям, поставляемым с операционной системой AIX, используйте один из следующих путей:

- `/usr/lib/security/tnc/libfileset_imc.a`: Собирает из системы клиента данные об уровне OS и установленного набора файлов и отправляет их в IMV (сервер TNC) для проверки.
- `/usr/lib/security/tnc/libfileset_imv.a`: Запрашивает от клиента информацию об уровне OS и наборе файлов и сравнивает ее с контрольной информацией. Кроме того, обновляет состояние клиента в базе данных сервера TNC. Для просмотра состояния введите следующую команду:

  ```
  psconf list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
  ```

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Установка Trusted Network Connect

Для установки компонентов Trusted Network Connect (TNC) необходимо выполнить следующие действия.

Для настройки и использования компонентов TNC выполните следующие действия:

1. Определите IP-адреса систем для настройки сервера TNC, сервера Trusted Network Connect and Patch Management (TNCPM) и компонента указателя IP TNC для Сервер виртуального ввода-вывода (VIOS).

Примечание: Сервер TNC нельзя настроить для работы в качестве клиента TNC.

2. Настройте сервер управления сетевой установкой (NIM). Система, настроенная как сервер, является главным узлом NIM, наборы файлов `sets:bos.sysmgt.nim.master` должны быть установлены в системе клиента.
3. Настройте сервер TNCPM. Конфигурация может быть выполнена в системе NIM. Сервер TNCPM использует SUMA для загрузки исправлений с веб-сайтов IBM Fix Central и ECC. Для загрузки обновлений система должна быть подключена к сети Интернет. Для настройки сервера TNCPM введите следующую команду:

   ```
   pmconf mktncpm [pmport=<порт>]tncserver=<хост:порт>
   ```

   Например:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```

4. Настройте стратегии на сервере TNC. Создание стратегий для проверки клиентов описано в разделе “Создание стратегий для клиента Trusted Network Connect” на стр. 27.
5. Настройте компонент указателя IP TNC в VIOS. Эта конфигурация VIOS запускает проверку на клиентах, подключенных к сети. Для настройки указателя введите следующую команду:

   ```
   psconf mkipref tncport=<порт> tncserver=<ip:порт>
   ```

   Например:

   ```
   psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
   ```

   Примечание: Значения порта сервера и порта TNC, который является портом клиента, должны совпадать.
6. Настройте клиентов с помощью следующей команды:

   ```
   psconf mkclient tncport=<порт> tncserver=<ip-адрес-сервера>:<порт>
   ```

   Например:

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Информация, связанная с данной:

“Установка PowerSC Standard Edition 1.1.3” на стр. 3
Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Установка с NIM

IBM Fix Central

Электронный справочный центр Passport Advantage

Настройка Trusted Network Connect и управления исправлениями

Trusted Network Connect (TNC) необходимо настроить для работы в качестве демона управления исправлениями. Для создания комплексного решения управления исправлениями сервер TNC интегрируется с SUMA.

Настройка сервера Trusted Network Connect

В разделе описаны действия по настройке сервера TNC.

Для настройки сервера TNC в файле `/etc/tnccs.conf` должны быть указано значение, похожее на следующее:

```
component = SERVER
```

Для настройки системы в качестве сервера выполните следующую команду:

```
psconf mkserver tncport=<порт> pmserver=<ip|имя-хоста[,ip2|имя-хоста2..]:порт>
[recheck_interval=<время-в-минутах>]
```

Например:

```
psconf mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

Примечание: Порт `tncport` и порт `pmserver` должны иметь разные значения. Если не указано значение параметра `recheck_interval`, то используется значение по умолчанию (1440 минут).

Для порта `tncport` по умолчанию используется значение 42830 минут, а для порта `pmserver` - 38240 минут.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Настройка клиента Trusted Network Connect

В статье описаны этапы настройки клиента Trusted Network Connect (TNC) и параметры конфигурации, необходимые для настройки.

Для настройки клиента TNC в файле `/etc/tnccs.conf` должны быть указано значение, похожее на следующее:

```
component = CLIENT
```

Для настройки системы в качестве клиента выполните следующую команду:

```
psconf mkclient tncport=<порт> tncserver=<ip:порт>
```

Например:

```
psconf mkclient tncport=10000 tncserver=1.1.1.1:10000
```

Примечание: Значения порта сервера и клиентского порта `tncport` должны быть одинаковыми.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Настройка сервера управления исправлениями

Приведены этапы настройки системы в качестве сервера управления исправлениями.

Сервер управления исправлениями TNC необходимо настроить на сервере NIM для возможности обновления клиентов TNC.

Для инициализации хранилищ исправлений с целью управления исправлениями TNC введите следующую команду:

```
pmconf init -i <интервал загрузки> -l <список TL> [-A] [-P <каталог загрузки>][-x <интервал ifix>]
[-K <ключ ifix>]
```

Пример команды **pmconf**:

```
pmconf init -i 1440 -l 6100-07,7100-01
```

Команда **init** загружает последний пакет исправлений для каждого технологического уровня и предоставляет доступ к нему серверу TNC. Обновленные пакеты исправлений позволяют серверу TNC выполнить проверку контрольных версий клиентов TNC, а серверу управления исправлениями TNC установить обновления для клиентов TNC. Флаг **-A** позволяет принять все лицензионные соглашения при выполнении обновления клиентов. По умолчанию хранилища исправлений, загружаемые сервером управления исправлениями TNC, находятся в файле `/var/tnc/tncpm/fix_repository`. Для назначения другого каталога укажите флаг **-P**.

Для обеспечения автоматической загрузки IBM Security Advisory и промежуточных исправлений можно указать интервал промежуточных исправлений. Эта функция предоставляет автоматическое уведомление о новых промежуточных исправлениях безопасности и связанных идентификаторах CVE. Перед регистрацией

| в TNC выполняется проверки всех рекомендаций защиты и промежуточных исправлений. Общий ключ,
| связанный с уязвимостью IBM AIX и требуемый для автоматической загрузки промежуточных исправлений,
| доступен на веб-сайте Защита IBM AIX. Автоматическая загрузка пакетов обновлений и промежуточных
| исправлений запрещена, если значения интервалов для них равно 0.

Можно также обновить регистрацию пакета обновлений и промежуточного исправления вручную. Для регистрации вручную IBM Security Advisory с соответствующими промежуточными исправлениями введите следующую команду:

```
pmconf add -y <файл advisory> -v <файл сигнатуры>  -e <файл tar ifix>
```

| Для регистрации автономного промежуточного исправления вручную выполните следующую команду:

```
| pmconf add -p <SP> -e <файл ifix>
```

Для регистрации нового технологического уровня и загрузки его последнего пакета обновлений введите следующую команду:

```
pmconf add -l <Список TL>
```

Для загрузки пакета обновлений, не являющегося текущей версией, либо для загрузки технологического уровня, который будет использоваться для проверки и обновления клиентов, введите следующую команду:

```
pmconf add -l <список TL> -d
pmconf add -s <Список SP>
```

Для регистрации пакета обновлений или хранилища исправлений технологического уровня, существующего в системе, введите следующую команду:

```
pmconf add -s <SP> -p <пользовательское-хранилище-исправлений>
pmconf add -l <TL> -p <пользовательское-хранилище-исправлений>
```

Для настройки системы в качестве сервера управления исправлениями введите следующую команду:

```
pmconf mktncpm [pmport=<порт>] tncserver=ip_list[:порт]
```

Пример:

```
pmconf mktncpm pmport=20000 tncserver=1.1.1.1:100000
```

Сервер управления исправлениями TNC всегда поддерживает работу с APAR защиты. Для настройки сервера управления исправлениями TNC для возможности управлениями другими типами APAR введите следующую команду:

```
pmconf add -t <список-типов-APAR>
```

В предыдущем примере <список-типов-APAR> - это разделенный запятыми список, содержащий следующие типы APAR:

- HIPER
- PE
- Enhancement

Сервер управления исправлениями TNC поддерживает работу с **syslog** для загрузки пакета обновлений, технологического уровня и обновлений клиентов. Утилита - `user`, а приоритет - это `info`. Пример: `user.info`.

Сервер управления исправлениями TNC ведет протокол всех обновлений клиентов в каталоге `/var/tnc/tncpm/log/update/<ip>/<системное-время>`.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Информация, связанная с данной:

Защита IBM AIX

Настройка почтовых уведомлений сервера Trusted Network Connect

В статье описана процедура настройки уведомлений по электронной почте для сервера Trusted Network Connect (TNC).

Сервер TNC просматривает уровень исправления клиента и при обнаружении его несогласованности отправляет администратору сообщение электронной почты с результатами и требуемым исправлением.

Для настройки адреса электронной почты администратора введите следующую команду:

```
psconf add -e <ИД-электронной-почты>[ipgroup=[±]G1, G2 ..]
```

Например:

```
psconf add -e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

В предыдущем примере сообщение электронной почты для группы IP *vayugrp1* и *vayugrp2* отправляется на адрес электронной почты abc@ibm.com.

Для отправки сообщения на глобальный адрес электронной почты для группы IP, не имеющей связанного с ней адреса электронной почты, выполните следующую команду:

```
psconf add -e <адрес-электронной-почты>
```

Например:

```
psconf add -e abc@ibm.com
```

В предыдущем примере, если у группы IP нет связанного с ней адреса электронной почты, то сообщение будет отправлено на адрес abc@ibm.com. Он играет роль глобального адреса электронной почты.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Настройка указателя IP в VIOS

В статье описывается настройка указателя IP в Сервер виртуального ввода-вывода (VIOS) для автоматического начала проверки.

Примечание: Перед настройкой указателя IP необходимо настроить расширение ядра SVM в виртуальном сервере ввода-вывода.

Для настройки указателя IP TNC в файле `/etc/tnccs.conf` должен быть задан параметр, похожий на следующий: `component = IPREF`.

Для настройки системы в качестве клиента выполните следующую команду:

```
psconf mkipref tncport=<порт> tncserver=<ip:порт>
```

Например:

```
psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
```

Значения порта `tncserver` и клиентского порта `tncport` должны быть одинаковыми.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Управление Trusted Network Connect и управление исправлениями

В статье описано управление Trusted Network Connect (TNC) для выполнения таких задач, как добавление клиентов, стратегий, протоколов, результатов проверки, обновление клиентов и сертификатов, относящихся к TNC.

Просмотр протоколов сервера структуры Надежное сетевое соединение

В этом разделе описано, как просмотреть протоколы сервера структуры Надежное сетевое соединение (TNC).

Сервер TNC вносит в протокол результаты проверки всех клиентов. Для просмотра протокола выполните команду **psconf**:

```
psconf list -H -i <ip |ALL>
```

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Создание стратегий для клиента Trusted Network Connect

В статье описана настройка стратегий, относящихся к клиенту Trusted Network Connect (TNC).

Консоль `psconf` предоставляет интерфейс для управления стратегиями TNC. С каждым клиентом или группой клиентов можно связать стратегию.

Можно создать следующие стратегии:

- Группа IP содержит несколько IP-адресов клиентов.
- Каждый IP-адрес клиента может принадлежать только одной группе.
- Группа IP связана с группой стратегий.
- Группа стратегий содержит различные виды стратегий. Например, стратегию набора файлов, определяющую, что должно относиться к уровню операционной системы клиента (т. е., выпуск, технологический уровень и пакет обновлений). В группе стратегий может быть несколько стратегий наборов файлов, при этом уровень клиента, указывающего на эту стратегию, должен совпадать с одной из стратегий наборов файлов.

Способы создания группы IP, группы стратегий и стратегий наборов файлов показаны в следующих командах.

Для создания группы IP введите следующую команду:

```
psconf add -G <имя-группы-ip> ip=[±]<ip1,ip2,ip3 ...>
```

Например:

```
psconf add -G myipgrp ip=1.1.1.1,2.2.2.2
```

Примечание: Для группы необходимо указать хотя бы один IP-адрес. Несколько IP-адресов должны быть разделены запятыми.

Для создания стратегии набора файлов введите следующую команду:

```
psconf add -F <имя-стратегии-fs> <rel00-TL-SP>
```

Например:

```
psconf add -F myfspol  6100-02-03 aparlist=IY0001,IY0002
```

Примечание: Информация о компоновке должна быть указана в формате `<rel00-TL-sp>`.

Для создания стратегии и присвоения группы IP введите следующую команду:

```
psconf add -P <имя-стратегии> ipgroup=[±] <ipgrp1, ipgrp2 ...]
```

Например:

```
psconf add -P mypol ipgroup=myipgrp,myipgrp1
```

Для присвоения стратегии набора файлов стратегии введите следующую команду:

```
psconf add -P <имя-стратегии> fspolicy=[±]<fspol1, fspol2 ...>
```

Например:

```
psconf add -P mypol fspolicy=myfspol,myfspol1
```

Примечание: Если указано несколько стратегий наборов файлов, система применяет наиболее соответствующую клиенту. Например, для клиента с `6100-02-01` и стратегиями наборов файлов `7100-03-04` и `6100-02-03` на клиенте будет применена стратегия `6100-02-03`.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Запуск проверки для клиента структуры Надежное сетевое соединение

В этом разделе описано, как проверить клиента структуры Надежное сетевое соединение (TNC).

Используйте один из следующих методов для проверки клиента:

- Демон определителя IP в Сервер виртуального ввода-вывода (VIOS) отправляет IP клиента на сервер TNC: клиент LPAR запрашивает IP и пытается получить доступ к сети. Демон определителя IP в VIOS обнаруживает новые IP-адреса и направляет из на сервер TNC: сервер TNC инициирует проверку при получении нового IP-адреса.
- Сервер TNC периодически проверяет клиента: администратор может добавить IP клиентов, которые должны проверяться, в базу данных стратегии TNC. Сервер TNC проверяет клиентов, которые находятся в базе данных. Повторная проверка выполняется автоматически через регулярные интервалы времени, заданные значением атрибута `recheck_interval` в файле конфигурации `/etc/tnccs.conf`.
- Администратор вручную инициирует проверку клиента: администратор может вручную инициировать проверку, чтобы проверить добавлен ли клиент в сеть, выполнив следующую команду:

  ```
  tncconsole verify -i
  <ip>
  ```

Примечание: Для ресурсов, которые не подключены к VIOS, клиенты могут быть проверены и обновлены при их добавлении вручную на сервер TNC.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Просмотр результатов проверки структуры Надежное сетевое соединение

В этом разделе описано, как просмотреть результаты проверки клиента структуры Надежное сетевое соединение (TNC).

Для просмотра результатов проверки клиентов в сети введите следующую команду:

```
psconf list -s ALL -i ALL
```

Эта команда показывает всех клиентов, которые находятся в состоянии **IGNORED**, **COMPLIANT** или **FAILED**.

- **IGNORED**: IP клиента игнорируется в списке IP (то есть, клиент может быть исключен из проверки).
- **COMPLIANT**: Клиент прошел проверку (то есть, клиент совместим со стратегией).
- **FAILED**: Клиент не прошел проверку (то есть, клиент не совместим со стратегией, и требуется действие администрирования).

Для того чтобы определить причину неполадки, выполните команду **psconf** с IP клиента:

```
psconf list -s ALL -i <ip>
```

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Обновление клиента структуры Надежное сетевое соединение

Сервер структуры Надежное сетевое соединение (TNC) проверяет клиента и обновляет базу данных с помощью состояния клиента и результата проверки. Администратор может просмотреть результаты и выполнить действие для обновления клиента.

Для того чтобы обновить клиента на предыдущем шаге, введите следующую команду:

```
psconf update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

Например:

```
psconf update -i 4.4.4.4 -r 6100-02-03 -a IY0004
```

Команда **psconf** обновляет клиента с помощью компоновки и установок APAR, если они существуют.

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

Управление стратегиями управления исправлениями

Команда **pmconf** позволяет настроить стратегии управления исправлениями.

Стратегии управления исправлениями предоставляют такую информацию, как IP-адрес сервера TNC и интервал для инициализации обновления SUMA.

Для управления стратегией управления исправлениями введите следующую команду:

```
pmconf mktncpm [pmport=<порт>] tncserver=<хост:порт>
```

Например:

```
pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000
```

Примечание: Порты `pmport` и `tncserver` должны быть разными.

Ссылки, связанные с данной:

“Команда pmconf” на стр. 35

Импорт сертификатов Trusted Network Connect

В статье описана процедура импорта сертификата и безопасная передача данных по сети.

Демоны Trusted Network Connect (TNC) устанавливают соединение по защищенным каналам, организованным с помощью протоколов TLS или SSL. Этот демон гарантирует защищенную и идентифицированную передачу данных и команд по сети. Каждая система имеет собственный ключ и сертификат, созданные во время выполнения команды инициализации компонентов. Этот процесс является прозрачным для администратора и требует от него меньшего участия. Во время первоначальной проверки клиента его сертификат импортируется в базу данных сервера. Изначально сертификат помечается как ненадежный, затем администратор просматривает с помощью команды **psconf** просматривает его и помечает как надежный. Для этого используется следующая команда:

```
psconf certadd -i <ip> -t <TRUSTED|UNTRUSTED>
```

Если администратору требуется использовать другой ключ и сертификат, то команда **psconf** предоставляет возможность их импорта.

Для импорта сертификата с сервера введите следующую команду:

| `psconf import -S -k <имя-файла ключа> -f <имя-файла>`

| Для импорта сертификата с клиента введите следующую команду:

| `psconf import -C -k <имя-файла ключа> -f <имя-файла>`

Ссылки, связанные с данной:

“Команда psconf” на стр. 39

| Создание отчетов о сервере TNC

| Сервер структуры Надежное сетевое соединение (TNC) поддерживает как формат значений через запятую (CSV), так и текстовый формат вывода для своих отчетов по уязвимости и открытости (CVE), IBM Security Advisory, стратегиям сервера TNC, исправлениям защиты клиента TNC и зарегистрированным пакетам обновления и временным исправлениям.

| Отчет CVE показывает все уязвимости и открытости для зарегистрированных пакетов обновления. Для того чтобы показать результаты этого отчета, введите следующую команду:

| `psconf report -v {CVEid|ALL} -o {TEXT|CSV}`

| Отчет по IBM Security Advisory показывает известные уязвимости защиты в установленном программном обеспечении IBM. Для того чтобы показать результаты этого отчета, введите следующую команду:

| `psconf report -A <advisoryname>`

| Отчет по стратегиям сервера TNC показывает стратегии защиты, применяемые на сервере TNC. Для того чтобы показать результаты этого отчета, введите следующую команду:

| `psconf report -P {policyname|ALL} -o {TEXT|CSV}`

| Отчет по исправлениям клиента TNC показывает установленные и отсутствующие временные исправления для клиента TNC. Для того чтобы показать результаты этого отчета, введите следующую команду:

| `psconf report -i {ip|ALL} -o {TEXT|CSV}`

| Можно также выполнить отчет, который генерирует список зарегистрированных пакетов обновления, связанных отчетов APAR и временных исправлений. Для того чтобы показать результаты этого отчета, введите следующую команду:

| `psconf report -B {buildinfo|ALL} -o {TEXT|CSV}`

| **Ссылки, связанные с данной**:

| “Команда psconf” на стр. 39

Устранение неполадок Надежного сетевого соединения и правления исправлениями

Здесь описаны возможные причины неполадок и действия по их устранению в TNC и системе управления исправлениями.

Для того чтобы устранить неполадки TNC и системы управления исправлениями, проверьте параметры конфигурации, перечисленные в следующей таблице.

Таблица 3. Устранение неполадок параметров конфигурации для TNC и системы управления исправлениями

Неполадка	Исправление
Сервер TNC не запущен или не отвечает	Выполните следующую процедуру: 1. Определите, запущен ли демон сервера TNC, введя команду: `ps -eaf | grep tnccsd` 2. Если он не запущен, удалите файл `/var/tnc/.tncsock`. 3. Перезапустите сервер. Если неполадка сохранится, проверьте файл конфигурации `/etc/tnccs.conf` для записи `component = SERVER` на сервере TNC.
Сервер управления исправлениями TNC не запущен или не отвечает	• Определите, запущен ли демон сервера управления исправлениями TNC, введя следующую команду: `ps -eaf | grep tncpmd` • Проверьте файл конфигурации `/etc/tnccs.conf` для записи `component = TNCPM` на сервере управления исправлениями TNC.
Клиент TNC не запущен или не отвечает	• Определите, запущен ли демон клиента TNC, введя следующую команду: `ps -eaf | grep tnccsd` • Проверьте файл конфигурации `/etc/tnccs.conf` для записи `component = CLIENT` на клиенте TNC.
Ссылающаяся на IP TNC программа не запущена в Сервер виртуального ввода-вывода (VIOS)	• Определите, запущен ли демон определителя IP TNC программы, введя следующую команду: `ps -eaf | grep tnccsd` • Проверьте файл конфигурации `/etc/tnccs.conf` для записи `component = IPREF` в VIOS.
Невозможно настроить систему в качестве и сервера, и клиента TNC	Сервер и клиент TNC не могут одновременно выполняться в одной системе.
Демоны запущены, но проверка не выполняется	Включите сообщения протокола для демонов. Установите протокол `level=info` в файле `/etc/tnccs.conf`. Затем можно проанализировать сообщения протокола.

Команды PowerSC Standard Edition

PowerSC Standard Edition предоставляет команды, позволяющие установить связь с компонентом Trusted Firewall и Trusted Network Connect с помощью командной строки.

Команда chvfilt

Назначение

Изменяет значения существующего правила фильтрации в виртуальных LAN.

Синтаксис

chvfilt [**-v <4|6>**] **-n fid** [**-a <D|P>**] [**-z <svlan>**] [**-Z <dvlan>**] [**-s <исх-адрес>**] [**-d <целевой-адрес>**] [**-o <src_port_op>**] [**-p <исходный-порт>**] [**-O <dst_port_op>**] [**-P <целевой-порт>**] [**-c <протокол>**]

Описание

Команда **chvfilt** позволяет изменить определение правила фильтрации виртуальной LAN в таблице правил фильтрации.

Флаги

-a Задает действие. Допустимые значения:

- D (Deny): блокирует трафик
- P (Permit): включает трафик

-c указывает различные протоколы, к которым применимо правило фильтрации. Допустимые значения:
- udp
- icmp
- icmpv6
- tcp
- любой

-d Задает целевой адрес в формате IPv4 или IPv6.

-m Задает маску исходного адреса.

-M Задает маску целевого адреса.

-n Задает ИД фильтра в правиле, который необходимо изменить.

-o Указывает исходный порт или операцию типа ICMP. Допустимые значения:
- lt
- gt
- eq
- любой

-O Задает целевой порт или операцию кода ICMP. Допустимые значения:
- lt
- gt
- eq
- любой

-p Задает исходный порт или тип ICMP.

-P Задает целевой порт или код ICMP.

-s Задает исходный адрес в формате v4 или v6.

-v Задает версию IP в таблице правил фильтрации. Допустимые значения: 4 и 6.

-z Задает ИД виртуальной LAN в исходном логическом разделе.

-Z Задает ИД виртуальной LAN в целевом логическом разделе.

Код возврата

Команда возвращает следующие коды:

0 Успешное выполнение.

>0 Произошла ошибка.

Примеры

1. Для изменения действующего правила фильтрации, существующего в ядре, введите следующую команду:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Если правило фильтрации (n=2) не существует в ядре, вывод будет следующим:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   Система отображает вывод следующим образом:
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

Команда genvfilt

Назначение

Добавляет правило фильтрации для VLAN между логическими разделами одного сервера IBM Power Systems.

Синтаксис

genvfilt -v <4|6> -a <D|P> -z <svlan> -Z <dvlan> [**-s <исходный-адрес>**] [**-d <целевой-адрес>**] [**-o <src_port_op>**] [**-p <исходный-порт>**] [**-O <dst_port_op>**] [**-P <целевой-порт>**] [**-c <протокол>**]

Описание

Команда **genvfilt** добавляет правило фильтрации для VLAN между логическими разделами (LPAR) одного сервера IBM Power Systems.

Флаги

-a Задает действие. Допустимые значения:
- D (Deny): блокирует трафик
- P (Permit): включает трафик

-c указывает различные протоколы, к которым применимо правило фильтрации. Допустимые значения:
- udp
- icmp
- icmpv6
- tcp
- любой

-d Задает целевой адрес в формате v4 или v6.

-m Задает маску исходного адреса

-M Задает маску целевого адреса.

-o Указывает исходный порт или операцию типа ICMP. Допустимые значения:
- lt
- gt
- eq
- любой

-O Задает целевой порт или операцию кода ICMP. Допустимые значения:
- lt
- gt
- eq
- любой

-p Задает исходный порт или тип ICMP.

-P Задает целевой порт или код ICMP.

-s Задает исходный адрес в формате IPv4 или IPv6.

-v Задает версию IP в таблице правил фильтрации. Допустимые значения: 4 и 6.

-z Задает ИД виртуальной LAN в исходном LPAR. Допустимые значения: от 1 до 4096.

-Z Задает ИД виртуальной LAN в целевом LPAR. Допустимые значения: от 1 до 4096.

Код возврата

Команда возвращает следующие коды:

0 Успешное выполнение.

>0 Произошла ошибка.

Примеры

1. Для добавления правила фильтра, разрешающего передачу данных TCP от исходного ИД VLAN 100 к целевому ИД VLAN 200 на указанные порты, введите следующую команду:

   ```
   genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
   ```

Ссылки, связанные с данной:

"Команда mkvfilt"

"Команда vlantfw" на стр. 44

Команда lsvfilt
Назначение

Выводит список правил фильтрации в виртуальных LAN из таблицы фильтров.

Синтаксис

lsvfilt [**-a**]

Описание

Команда **lsvfilt** позволяет вывести список правил фильтрации в виртуальных LAN и их состояния.

Флаги

-a Выводит список только активных правил фильтрации.

Код возврата

Команда возвращает следующие коды:

0 Успешное выполнение.

>0 Произошла ошибка.

Примеры

1. Для вывода списка активных правил фильтрации в ядре введите следующую команду:

   ```
   lsvfilt -a
   ```

Понятия, связанные с данным:

"Деактивация правил" на стр. 16
Можно деактивировать правила, которые разрешают маршрутизацию между VLAN в функции Надежный брандмауэр.

Команда mkvfilt
Назначение

Активирует правила фильтрации в виртуальных LAN, определенные в команде **genvfilt**.

Синтаксис

mkvfilt -u

Описание

Команда **mkvfilt** активирует правила фильтрации в виртуальных LAN, определенные в команде **genvfilt**.

Флаги

-u Активирует правила фильтрации в таблице правил фильтрации.

Код возврата

Команда возвращает следующие коды:

0 Успешное выполнение.

>0 Произошла ошибка.

Примеры

1. Для активации правил фильтрации в ядре введите следующую команду:

   ```
   mkvfilt -u
   ```

Ссылки, связанные с данной:

“Команда genvfilt” на стр. 33

Команда pmconf

Назначение

Создание отчетов и управление сервером TNCPM путем регистрации технологических уровней и серверов TNC для получения новейших исправлений и создания отчетов о состоянии TNCPM.

Примечание: Для возможности загрузки метаданных пакета исправлений сервер TNCPM должен запускаться только в AIX версии 7.1 с технологическим уровнем 7100-02.

Синтаксис

pmconf mktncpm [**pmport=**<*порт*>] **tncserver=***ip* | имя-хоста **:** *порт*

pmconf rmtncpm

pmconf start

pmconf stop

| **pmconf init -i** <*интервал загрузки*> **-l** <*Список TL*> **-A** [**-P** <*путь загрузки*>] [**-x** <*ifix интервал*>] [**-K** <*ifix*
| *ключ*>]

pmconf add -l *Список-TL*

pmconf add -p <*Список SP*> [**-U** <*пользовательский путь SP*>]

| **pmconf add -p** <*SP*> **-e** <*файл ifix*>

| **pmconf add -y** <*файл advisory*> **-v** <*файл сигнатуры*> **-e** <*файл tar ifix*>

pmconf delete -l *Список-TL*

pmconf delete -p <*Список SP*>

pmconf delete -p <*SP*>**-e** *Файл ifix*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *имя-файла-сертификата* **-k** *имя-файла ключей*

pmconf export -f *имя-файла*

pmconf modify -i <*интервал загрузки*>

pmconf modify -P <*путь загрузки*>

pmconf modify -g <*yes или no для принятия всех лицензий*>

pmconf modify -t <*Список типов APAR*>

pmconf modify -x <*интервал ifix*>

pmconf modify -K <*ключ ifix*>

pmconf delete -l <*Список TL*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *значение*

Описание

Функции команды **pmconf**:

Управление хранилищем исправлений
Регистрирует или отменяет регистрацию технологических уровней; отменяет регистрацию серверов TNC. TNCPM создает хранилище исправлений для каждого технологического уровня, в котором содержатся последние исправления, информация **lslpp** (например сведения об установленных наборах файлов или обновлениях наборов файлов), а также сведения об исправлении защиты для этого технологического уровня.

Создание отчетности
Создает отчеты о состоянии TNCPM.

С помощью команды **pmconf** можно выполнить следующие операции:

Элемент	Описание
add	Регистрирует с помощью TNCPM новый технологический уровень.
chtncpm	Изменяет атрибуты в файле tnccs.conf. Для вступления изменений в силу на сервере TNCPM требуется явно указать команду **start**.
delete	Отменяет регистрацию технологического уровня с помощью TNCPM.
history	Отображает хронологию обновления и загрузки.
список	Отображает информацию о TNCPM.
log	Задает уровень протокола для компонентов TNC.
mktncpm	Создает сервер TNCPM.
modify	Изменяет атрибуты tncpm.conf.
rmtncpm	Удаляет сервер TNCPM.
start	Запускает сервер TNCPM.
stop	Останавливает сервер TNCPM.

Флаги

Элемент	Описание
-A	Принимает все лицензионные соглашения при выполнении обновления клиентов.
-a <файл advisory>	Указывает файл рекомендаций, соответствующий параметру **ifix**. Если файл рекомендаций не указан, то параметр **ifix** не рассматривается как адрес CVE промежуточного исправления.
-e <файл ifix>	Задает промежуточные исправления, добавленные в TNCPM.
-i *интервал-загрузки*	Задает интервал проверки сервером TNCPM наличия новых пакетов исправлений для зарегистрированных технологических уровней. Интервал - это целочисленное значение в минутах или в виде следующего формата: **d** (дни): **h** (часы): **m** (минуты).
-K <ключ ifix>	Задает общий ключ IBM AIX Product Security Incident Response Tool (PSIRT), используемый для идентификации загруженных рекомендованных и промежуточных исправлений. Этот общий ключ можно загрузить с сервера общих ключей PGP с помощью ИД **0x28BFAA12**.
-p *Список-SP*	Задает список пакетов обновлений для загрузки. Список - разделенный запятыми список в формате REL00-TL-SP (например, `6100-01-04` - это пакет обновлений 04 для технологического уровня 01 и версии 6.1). При использовании флага -U укажите только один SP.
-t *список-типов-APAR*	Задает типы APAR, поддерживаемые в TNCPM для обновления клиентов и списка серверов TNC. APAR защиты поддерживаются всегда. Список-типов-APAR - это разделенный запятыми список следующих типов: HIPER, FileNet Process Engine, Enhancement.
-P *путь-к-хранилищу-исправлений*	Задает каталог загрузки для хранилищ исправлений, которые будут загружены TNCPM. Каталог по умолчанию: **/var/tnc/tncpm/fix_repository**.
-U *пользовательское-хранилище-исправлений*	Задает путь к пользовательскому хранилищу исправлений. Укажите выпуск, технологический уровень и пакет обновлений, связанные с хранилищем исправлений, которое используется для проверки и обновлений клиентов.
-s	Создает отчет о зарегистрированных пакетах обновлений.
-l *SP*	Создает отчет со сведениями **lslpp** для пакета обновлений. *SP* указывается в формате REL00-TL-SP (например `6100-01-04` представляет пакет обновлений 04 для технологического уровня 01 и версии 6.1).
-u	Создает отчет о хронологии обновления клиента.
-d	Создает отчет о хронологии загрузки пакетов обновлений.
-C	Создает отчет для сертификата сервера.
-a *SP*	Создает отчет об информации APAR защиты для пакета обновлений. *SP* указывается в формате REL00-TL-SP (например `6100-01-04` представляет пакет обновлений 04 для технологического уровня 01 и версии 6.1).
-f *имя-файла*	Указывает имя файла сертификата.
-k *имя-файла-ключа*	Задает файл, из которого требуется прочитать ключ сертификата в случае операции импорта.

-c	Отображает пользовательские атрибуты в виде записей, разделенных двоеточием, например:
	`# имя: атрибут1: атрибут2: ...`
	`стратегия: значение1: значение2: ...`

-v <*файл сигнатуры*>	Указывает файл сигнатуры для рекомендации по уязвимостям IBM AIX.
-y <*файл advisory*>	Задает файл рекомендаций по уязвимостям IBM AIX.
-q	Подавляет вывод информации заголовка.
-x <*интервал ifix*>	Указывает интервал (в минутах) для проверки наличия и загрузки новых промежуточных исправлений. При значении 0 автоматическая загрузка промежуточного исправления и выдача уведомления отключена. Значение по умолчанию: 24 часа.

Код возврата

Команда возвращает следующие коды:

Элемент	Описание
0	Команда выполнена успешно, все запрошенные изменения внесены.
>0	Произошла ошибка. Напечатанное сообщение об ошибке содержит дополнительную информацию о типе неполадки.

Примеры

1. Для инициализации TNCPM введите следующую команду:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Для создания демона TNCPM введите следующую команду:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Для запуска сервера выполните следующую команду:
   ```
   pmconf start
   ```
4. Для останова сервера выполните следующую команду:
   ```
   pmconf stop
   ```
5. Для регистрации нового технологического уровня с помощью TNCPM введите следующую команду:
   ```
   pmconf add -l 6100-01
   ```
6. Для отмены регистрации технологического уровня в TNCPM введите следующую команду:
   ```
   pmconf delete -l 6100-01
   ```
7. Для отмены регистрации сервера TNC с IP-адресом 11.11.11.11 в TNCPM введите следующую команду:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Для регистрации более новой версии пакета обновлений в TNCPM введите следующую команду:
   ```
   pmconf add -s 6100-01-04
   ```
9. Для отмены регистрации более ранней версии пакета обновлений в TNCPM введите следующую команду:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Для создания отчета о хранилищах исправлений для каждого зарегистрированного технологического уровня выполните следующую команду:
    ```
    pmconf list -s
    ```
11. Для создания отчета о зарегистрированном технологическом уровне **lslpp** введите следующую команду:
    ```
    pmconf list -l 6100-01-02
    ```
12. Для создания отчета о хронологии обновлений введите следующую команду:
    ```
    pmconf hist -u
    ```
13. Для создания отчета о хронологии загрузок введите следующую команду:
    ```
    pmconf hist -d
    ```
14. Для создания отчета о сертификате сервера введите следующую команду:
    ```
    pmconf list -C
    ```
15. Для создания отчета с информацией о APAR защиты пакета обновлений введите следующую команду:
    ```
    pmconf list -a 6100-01-02
    ```
16. Для импорта сертификата сервера введите следующую команду:
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Для экспорта сертификата сервера введите следующую команду:
    ```
    pmconf export -f /tmp/server.txt
    ```

Команда psconf

Назначение

Создание отчетов и управление сервером Trusted Network Connect (TNC), клиентом TNC, IPRef TNC и SUMA. Она управляет стратегиями управления наборами файлов и исправлениями по отношению к целостности конечных точек (сервер и клиент) во время или после сетевого соединения для защиты сети от угроз и атак.

Синтаксис

Операции сервера TNC:

psconf mkserver [**tncport=**<*порт*>] **pmserver=**<*хост*:*порт*> [tsserver=<хост>] [**recheck_interval=**<*время-в-минутах*> | **d** (дни) : **h** (часы) : **m** (минуты)] [**dbpath** = <*пользовательский каталог*>]

psconf { **rmserver** | **status** }

psconf { **start** | **stop** | **restart** } **server**

psconf chserver attribute = *значение*

psconf add -F <*имя-стратегии-FS*> -r <*информация-о-компоновке*> [**apargrp=** [**±**]<*apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-]<*ifixgrp1,ifixgrp2...>*]

psconf add { **-G** <*имя-ipgroup*> **ip=**[**±**]<*хост1, хост2...*> | {**-A**<*группа-apar*> [**список-apar**=[**±**]*apar1, apar2...* | {**-V** <*группа-ifix*> [*список-ifix*=[+|-]*ifix1,ifix2...*]}

psconf add -P <*имя-стратегии*> { **fspolicy=**[**±**]<*f1,f2...*> | **ipgroup=**[**±**]<*g1,g2...*> }

psconf add -e *emailid* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [**±**]<*g1,g2...*>]

psconf add -I ip= [**±**]<*хост1, хост2...*>

psconf delete { **-F** <*имя-стратегии-FS*> | **-G** <*имя-ipgroup*> | **-P** <*имя-стратегии*> | **-A** <*группа-apar*> | **-V** <*группа-ifix*>}

psconf delete -H -i <*хост* | **ALL**> **-D** <*гггг-мм-дд*>

psconf certadd -i <*хост*> **-t <TRUSTED | UNTRUSTED>**

psconf certdel -i <*хост*>

psconf verify -i <*хост*> | **-G** <*ipgroup*>

psconf update [-p] {-i< *хост* >| **-G** <*ipgroup*> [**-r** <*информация-о-компоновке*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1*, *ifix2*,...>}

psconf log loglevel=<info | error | none>

psconf import -C -i <*хост*> **-f** <*имя-файла*> | **–d** <*имя-файла базы данных для импорта*>

psconf { **import -k** <*имя-файла-ключей*> | **export**} **-S -f** <*имя-файла*>

psconf list { **-S** | **-G** < *имя-ipgroup* | **ALL** > | **-F** < *имя-стратегии-FS* | **ALL** > | **-P** < *имя-стратегии* | **ALL** > | **-r** < *информация-о-компоновке* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *группа-apar* | **ALL** > | **-V** <*группа-ifix*>} [**-c**] [**-q**]

psconf list { **-H** | **-s** <**COMPLIANT** | **IGNORE** | **FAILED** | **ALL**> } **-i** <*хост* | **ALL**> [**-c**] [**-q**]

psconf export -d <*путь к каталогу экспорта*>

psconf report -v <CVEid|ALL> -o <TEXT|CSV>

psconf report -A <имя-advisory>

psconf report -P <имя-стратегии|ALL> -o <TEXT|CSV>

psconf report -i <ip|ALL> -o <TEXT|CSV>

psconf report -B <информация-о-компоновке|ALL> -o <TEXT|CSV>

Операции клиента TNC:

psconf mkclient [**tncport=**<*порт*>] **tncserver=**<*хост:порт*>

psconf mkclient tncport=<*порт*> -T

psconf { **rmclient** | **status** }

psconf {**start** | **stop** | **restart** } **client**

psconf chclient attribute = *значение*

psconf list { **-C** | **-S** }

psconf export { **-C** | **-S** } **-f** <*имя-файла*>

psconf import { **-S** | **-C -k** <*имя-файла-ключей*> } **-f** <*имя-файла*>

Операции IPRef TNC:

psconf mkipref [**tncport=**<*порт*>] **tncserver=**<хост:порт>

psconf { **rmipref** | **status**}

psconf { **start** | **stop** | **restart**} ipref

psconf chipref attribute = *значение*

psconf { **import -k** <*имя-файла-ключей*> | **export**} **-R -f** <*имя-файла*>

psconf list -R

Описание

Технология TNC - это открытая основанная на стандартах архитектура для идентификации конечных точек, измерения целостности платформы и интеграции систем защиты. Архитектура TNC проверяет конечные точки (серверы и сетевые клиенты) на согласованность со стратегиями защиты перед их применением в защищенной сети. IPRef TNC уведомляет сервер TNC о любых новых IP-адресах, обнаруженных на виртуальном сервере ввода-вывода (VIOS).

SUMA позволяет освободить системных администраторов от необходимости вручную загружать обновления с веб-сайта. В ней предусмотрены разнообразные параметры, позволяющие системному администратору настроить интерфейс для автоматической загрузки обновлений с веб-сайта рассылки обновлений.

Команда **psconf** управляет сетевым сервером и клиентом путем добавления или удаления стратегий защиты, проверки клиентов на надежность, создания отчетов и обновления сервера и клиента.

С помощью команды **psconf** можно выполнить следующие операции:

Элемент	Описание
add	Добавляет стратегию, клиента или сведения об электронной почте на сервер TNC.
apargrp	Задает имена групп APAR в составе стратегии набора файлов, которые используются для проверки клиентов TNC.
aparlist	Задает список APAR, входящих в состав группы APAR.
certadd	Помечает сертификат как надежный или ненадежный.
certdel	Удаляет информацию о клиенте.
chclient	Изменяет атрибуты в файле `tnccs.conf`. Для вступления изменений в силу на клиенте TNC требуется явно указать команду **start**. Синтаксис поля attribute=value должен совпадать с синтаксисом в команде **mkclient**.
chipref	Изменяет атрибуты в файле `tnccs.conf`. Для вступления изменений в силу в IPRef требуется явно указать команду **start**. Синтаксис поля attribute=value должен совпадать с синтаксисом в команде **mkipref**.
chserver	Изменяет атрибуты в файле `tnccs.conf`. Для вступления изменений в силу на сервере TNC требуется явно указать команду **start**. Синтаксис поля attribute=value должен совпадать с синтаксисом в команде **mkserver**. **Примечание:** С помощью команды **chserver** нельзя изменить атрибут **dbpath**. Для его изменения необходимо запустить команду **mkserver**.
dbpath	Задает расположение базы данных TNC. Значение по умолчанию: `/var/tnc`.
delete	Удаляет стратегию или информацию о клиенте.
export	Выполняет экспорт сертификата клиента или сервера или базы данных на сервере TNC.
fspolicy	Задает стратегию набора файлов выпуска, технологического уровня и пакета обновлений, используемых для проверки клиентов TNC.
import	Выполняет импорт сертификата клиента или сервера или базы данных на сервере TNC.
ipgroup	Задает группу IP, в которой содержится несколько IP-адресов клиентов или имен хостов.
список	Отображает информацию о сервере TNC, клиенте TNC или SUMA.
log	Задает уровень протокола для компонентов TNC.
mkclient	Настраивает клиент TNC.
mkipref	Настраивает IPRef TNC.
mkserver	Настраивает сервер TNC.
pmport	Задает номер принимающего запросы порта для сервера **pmserver**. Значение по умолчанию - 38240.
pmserver	Задает имя хоста или IP-адрес команды **suma**, которая загружает последние пакеты обновлений и исправления защиты, доступные на веб-сайте IBM® ECC и IBM Fix Central.
recheck_interval	Задает для сервера TNC интервал (в минутах или в формате d (дни) : h (часы) : m (минуты)) между проверками клиентов TNC. **Примечание:** Значение **recheck_interval=0** означает, что планировщик не будет выполнять периодическую проверку клиентов, а зарегистрированные клиенты будут проверяться автоматически при запуске. В таких случаях клиенты могут быть проверены вручную.
report	Создает отчет с расширением файла .txt или .csv.
restart	Перезапускает клиент TNC, сервер TNC или IPRef TNC.
rmclient	Удаляет конфигурацию клиента TNC.
rmipref	Удаляет конфигурацию IPRef TNC.
rmserver	Удаляет конфигурацию сервера TNC.
start	Запускает клиент TNC, сервер TNC или IPRef TNC.
status	Показывает состояние конфигурации TNC.
stop	Останавливает клиент TNC, сервер TNC или IPRef TNC.
tncport	Задает номер принимающего запросы порта для сервера TNC. Значение по умолчанию - 42830.
tncserver	Задает сервер TNC, проверяющий или обновляющий клиентов TNC.
tssserver	Задает IP-адрес или имя хоста сервера Trusted Surveyor.
update	Устанавливает исправления на клиента.
verify	Запускает проверку клиента вручную.

Флаги

Элемент	Описание
-A <имя-advisory>	Задает рекомендованное имя для отчета.
-B <информация-о-компоновке>	Указывает информацию о компоновке для подготовки к отчету об исправлении.

-c	Отображает пользовательские атрибуты в виде записей, разделенных двоеточием, например:
	`# имя: атрибут1: атрибут2: ...`
	`стратегия: значение1: значение2: ...`

-C	Указывает, что операция предназначена для компонента клиента.
-d *расположение файла базы данных/путь к каталогу базы данных*	Задает путь к файлу для импорта базы данных или каталог для экспорта базы данных.
-D *гггг-мм-дд*	Задает дату конкретной записи клиента в хронологии протокола, где *гггг* - год, *мм* - месяц и *дд* - день.
-e *ИД-электронной-почты* **ipgroup=**[**±**]*g1, g2...*	Задает ИД электронной почты, после которого следует разделенный запятыми список имен групп IP.
-E | FAIL | COMPLIANT | ALL |	Указывает событие, для которого необходимо отправить сообщение электронной почты на настроенный ИД электронной почты. FAIL - сообщения отправляются, если состояние проверки клиента - FAILED. COMPLIANT- сообщения отправляются, если состояние проверки клиента - COMPLAINT. ALL - сообщения отправляются для любых состояний проверки клиента.
-f *имя-файла*	Задает файл, из которого необходимо прочитать сертификат в случае операции импорта, или расположение, в которое должен быть записан сертификат при операции экспорта.
-F *стратегия-fs информация-о-компоновке*	Задает имя стратегии файловой системы, после которой следует информация о компоновке. Информация о компоновке может быть предоставлена в следующем формате: `6100-04-01`, где `6100` - это версия 6.1, `04` - уровень обслуживания и `01` - пакет обновлений.
-G *имя-группы-ip* **ip=**[**±**]*ip1, ip2...*	Задает имя группы IP, за которым следует разделенный запятыми список IP-адресов.
-H	Выводит протокол хронологии.
-i *хост*	Указывает IP-адрес или имя хоста.
-I ip=[**±**]*ip1, ip2...* | [±] хост1,хост2...	Указывает IP-адрес или имя хоста, которое должно быть проигнорировано при проверке.
-k *имя-файла*	Задает файл, из которого требуется прочитать ключ сертификата в случае операции импорта.
-p	Выполняет предварительный просмотр обновления клиента TNC.
-P <имя-стратегии>	Указывает имя стратегии для подготовки отчета о стратегиях клиента.
-q	Подавляет вывод информации заголовка.
-r *информация-о-компоновке*	Создает отчет на основе информации о компоновке. Информация о компоновке может быть предоставлена в следующем формате: `6100-04-01`, где `6100` - это версия 6.1, `04` - уровень обслуживания и `01` - пакет обновлений.
-R	Указывает, что операция предназначена для компонента IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Отображает клиента по состоянию: **COMPLIANT** Показывает активные клиенты. **IGNORE** Показывает клиентов, исключенных из любых проверок. **FAILED** Показывает клиентов, не прошедших проверку для настроенной стратегии. **Все** Показывает всех клиентов независимо от состояния.
-S <хост>	Указывает имя хоста для подготовки отчета об исправлениях защиты клиента.
-t TRUSTED | UNTRUSTED	Помечает указанного клиента как надежного или ненадежного. **Примечание:** Проверить сервер или клиента на надежность могут только системные администраторы.
-T	Указывает, что клиент может принимать запросы от любого сервера TS с действующим сертификатом.
-u	Удаляет промежуточное исправление, установленное на клиенте TNC.
-v	Указывает разделенный запятыми список промежуточных исправлений.
-V	Задает имя группы промежуточных исправлений.

Код возврата

Команда возвращает следующие коды:

Элемент	Описание
0	Команда выполнена успешно, все запрошенные изменения внесены.
>0	Произошла ошибка. Напечатанное сообщение об ошибке содержит дополнительную информацию о типе неполадки.

Примеры

1. Для запуска сервера TNC введите следующую команду:
   ```
   psconf start server
   ```
2. Для добавления стратегии файловой системы с именем `71D_latest` для компоновки `7100-04-02` введите следующую команду:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Для удаления стратегии файловой системы с именем `71D_old` выполните следующую команду:
   ```
   psconf delete -F 71D_old
   ```
4. Для проверки, что клиент с IP-адресом `11.11.11.11` является **надежным**, введите следующую команду:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Для удаления клиента с IP-адресом `11.11.11.11` из сервера введите следующую команду:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Для проверки информации о клиенте с IP-адресом `11.11.11.11` введите следующую команду:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Для отображения информации о клиенте с IP-адресом `11.11.11.11` введите следующую команду:
   ```
   psconf list -i 11.11.11.11
   ```
8. Для создания отчета о клиентах с состоянием **COMPLAINT** введите следующую команду:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Для создания отчета о компоновке `7100-04-02` введите следующую команду:
   ```
   psconf list -r 7100-04-02
   ```
10. Для отображения хронологии соединений клиента с IP-адресом `11.11.11.11` введите следующую команду:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Для удаления из хронологии протокола записей о клиенте с IP-адресом `11.11.11.11`, созданных до 2 февраля 2009 года, введите следующую команду:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Для импорта с сервера клиентского сертификата для клиента с IP-адресом `11.11.11.11` введите следующую команду:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Для экспорта серверного сертификата из клиента введите следующую команду:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Для обновления клиента с IP-адресом `11.11.11.11` до соответствующего уровня с сервера выполните следующую команду:
    ```
    psconf update -i 11.11.11.11
    ```
15. Для отображения состояний клиентов введите следующую команду:
    ```
    psconf status
    ```
16. Для отображения клиентского сертификата введите следующую команду:
    ```
    psconf list -C
    ```
17. Для запуска клиента введите следующую команду:
    ```
    psconf start client
    ```

Security

Вниманию пользователей RBAC и Trusted AIX:

Данная команда может выполнять привилегированные операции. Такие операции могут выполнять только пользователи с привилегированными правами доступа. Дополнительная информация о правах доступа и привилегиях приведена в разделе База данных привилегированных команд в документе Защита. Список привилегий и прав доступа, связанных с этой командой, приведен в команде **lssecattr** или подкоманде **getcmdattr**

Команда rmvfilt

Назначение

Удаляет правила фильтрации между виртуальными LAN из таблицы фильтров.

Синтаксис

rmvfilt -n [**fid|all>**]

Описание

Команда **rmvfilt** используется для удаления правил фильтрации между виртуальными LAN из таблицы фильтров.

Флаги

-n Указывает ИД правила фильтрации, которое будет удалено. Опция **all** используется для удаления всех правил фильтрации.

Код завершения

Эта команда возвращает следующие значения завершения:

0 Успешное завершение.

>0 Произошла ошибка.

Примеры

1. Для удаления или деактивации всех правил фильтрации в ядре введите следующую команду:

   ```
   rmvfilt -n all
   ```

Понятия, связанные с данным:

“Деактивация правил” на стр. 16
Можно деактивировать правила, которые разрешают маршрутизацию между VLAN в функции Надежный брандмауэр.

Команда vlantfw

Назначение

Показывает или очищает информацию о связывании IP и Media Access Control (MAC) и управляет функцией ведения протоколов.

Синтаксис

vlantfw -h | -s | -t | -d | -f | -G | -q | -D | -E | -F | -i | -l | -L | -m | -M | -N *integer*

Описание

Команда **vlantfw** показывает или очищает записи связывания IP и MAC. Она также предоставляет возможность запустить или остановить средство регистрации Надежного брандмауэра.

Флаги

-d Показывает всю информацию о связывании IP.

-D Показывает все собранные данные о соединении.

-E Показывает данные о соединении между логическими разделами (LPAR) в различных комплексах центральных процессоров.

-f Удаляет всю информацию о связывании IP.

-F Очищает кэш данных соединения.

-G Показывает правила фильтрации, которые могут быть настроены для внутренней маршрутизации потока данных с помощью Надежного брандмауэра.

-I Показывает данные соединения между LPAR, которые связаны с различными ИД VLAN, но совместно используют одни и те же комплексы центральных процессоров.

-l Запускает средство регистрации Надежного брандмауэра.

-L Останавливает средство регистрации Надежного брандмауэра и перенаправляет содержимое файла трассировки в файл `/home/padmin/svm/svm.log`.

-m Включает отслеживание Надежного брандмауэра.

-M Выключает отслеживание Надежного брандмауэра.

-q Запрашивает состояние защищенной виртуальной системы.

-s Запускает Надежный брандмауэр.

-t Останавливает Надежный брандмауэр.

Параметры

-N *целое число*
Показывает правило фильтрации, которое соответствует указанному целому числу.

Код завершения

Эта команда возвращает следующие значения завершения:

0 Успешное завершение.

>0 Произошла ошибка.

Примеры

1. Для того чтобы показать все привязки IP, введите следующую команду:
   ```
   vlantfw -d
   ```
2. Для того чтобы удалить все привязки IP, введите следующую команду:
   ```
   vlantfw -f
   ```
3. Для того чтобы запустить функцию ведения протоколов Надежного брандмауэра, введите следующую команду:
   ```
   vlantfw -l
   ```
4. Для того чтобы проверить состояние защищенной виртуальной машины, введите следующую команду:
   ```
   vlantfw -q
   ```
5. Для того чтобы запустить надежный брандмауэр, введите следующую команду:

```
vlantfw -s
```

6. Для того чтобы остановить надежный брандмауэр, введите следующую команду:

```
vlantfw -t
```

7. Для того чтобы показать соответствующие правила, которые можно использовать для генерации фильтров, направляющих поток данных в комплекс центрального процессора, введите следующую команду:

```
vlantfw -G
```

Ссылки, связанные с данной:

“Команда genvfilt” на стр. 33

Примечания

Эта информация была разработана для продуктов и услуг, предлагаемых на территории США.

Компания IBM может не предоставлять в других странах продукты и услуги, обсуждаемые в данном документе. Информацию о продуктах и услугах, распространяемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылки на продукты, программы или услуги IBM не означают, что можно использовать только указанные продукты, программы или услуги IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако ответственность за проверку действия любых продуктов, программ и услуг других компаний лежит на пользователе.

Компания IBM может обладать заявками на патенты или патентами на предметы обсуждения в данном документе. Обладание данным документом не предоставляет вам лицензии на эти патенты. Запросы на получение лицензии можно отправлять в письменном виде по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Для отправки запроса на лицензию, связанную с информацией, представляемой с помощью двухбайтовых символов (DBCS), обратитесь в местное отделение компании IBM по интеллектуальной собственности или отправьте запрос по адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 государствах освобождение от явных и подразумеваемых гарантий запрещено в некоторых сделках, поэтому это заявление может к вам не относиться.

Эта информация может содержать технические неточности или типографические ошибки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях этой книги. Компания IBM может вносить усовершенствования и изменения в продукты и программы, описанные в данном издании, в любое время без уведомления.

Любые ссылки на Веб-сайты других компаний приведены в данной публикации исключительно для удобства пользователей и не могут рассматриваться как рекомендация пользоваться этими веб-сайтами. Все материалы, опубликованные на этих сайтах, не относятся к материалам по данному продукту фирмы IBM, и ответственность за их использование ложится на пользователя.

IBM может использовать и распространять любую предоставленную вами информацию по собственному усмотрению 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) двустороннего использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Такая информация может быть предоставлена на определенных условиях, а в некоторых случаях - и за дополнительную плату.

Лицензионная программа, описанная в данном документе, и все лицензионные материалы для нее предоставляются компанией IBM на условиях соглашения с заказчиками IBM, международного соглашения о предоставлении лицензии на программу IBM или эквивалентного соглашения между сторонами.

Все данные о производительности, приведенные в настоящей документации, были получены в управляемой среде. В связи с этим результаты, полученные в других операционных средах, могут значительно отличаться от приведенных данных. Некоторые измерения могли быть выполнены в системах, находящихся в процессе разработки, поэтому нет гарантии, что в общедоступных системах будут получены аналогичные показатели. Более того, некоторые показатели могли быть получены с помощью экстраполяции. Фактические результаты могу отличаться от указанных. Пользователи настоящей документации должны проверять данные, относящиеся к их конкретной среде.

Информация о продуктах других компаний была получена от поставщиков этих продуктов, их опубликованных материалов или других общедоступных источников. Компания IBM не проверяла эти продукты и не может подтвердить правильность их работы, совместимость или другие заявленные характеристики продуктов других компаний. По вопросам о возможностях продуктов других компаний следует обращаться к поставщикам этих продуктов.

Любые заявления относительно будущих проектов или намерений IBM могут быть изменены или аннулированы без предварительного уведомления и являются исключительно декларациями общего характера о целях.

Все указанные цены IBM являются рекомендуемыми розничными ценами IBM на данный момент и могут быть изменены без предварительного уведомления. Цены дилеров могут быть другими.

Данная информация предназначена исключительно для целей планирования. Приведенная здесь информация может быть изменена до того, как описанные в ней продукты станут доступными.

Эта информация содержит примеры данных и отчеты, применяемые в повседневных деловых операциях. Для большего сходства с реальностью примеры содержат имена людей, названия компаний, товарных знаков и продуктов. Все эти имена и названия являются вымышленными и все сходства с реальными именами и адресами реальных предприятий случайны.

ЛИЦЕНЗИЯ НА АВТОРСКИЕ ПРАВА:

Настоящая документация содержит примеры исходного кода программ, иллюстрирующие приемы программирования в различных операционных системах. Вы имеете право копировать, изменять и распространять эти примеры программ в любой форме без уплаты вознаграждения фирме IBM в целях разработки, применения, сбыта или распространения прикладных программ, соответствующих интерфейсу прикладных программ операционной системы, для которой предназначены эти примеры. Эти примеры не были тщательно и всесторонне протестированы. В связи с этим IBM не может гарантировать их надежность,

удобство обслуживания и отсутствие ошибок. Примеры программ предоставляются "КАК ЕСТЬ", без каких-либо гарантий. Ни при каких обстоятельствах IBM не несет ответственности за возможный ущерб, вызванный использованием этих примеров программ.

Каждая копия, часть или модификация приведенных примеров программ должна содержать следующее сообщение об авторских правах:

© (название вашей компании) (год). Некоторые фрагменты исходного кода получены из примеров программ фирмы IBM Corp. © Copyright IBM Corp. _год или годы_.

В электронной версии этой информации могут отсутствовать фотографии и цветные иллюстрации.

Замечания о правилах работы с личными данными

Продукты IBM Software, включая решения программного обеспечения как услуг, (“Предложения программного обеспечения”) могут использовать cookie или другие технологии для сбора информации об использовании продукта в целях усовершенствования пользовательского интерфейса, для приспособления взаимодействий к конечному пользователю или для других целей. Во многих случаях Предложениями программного обеспечения собирается информация, в которой невозможно опознать персональные данные. Некоторые из наших Предложений программного обеспечения могут позволить вам собирать опознаваемую персональную информацию. Если это Предложение программного обеспечения использует cookie для сбора опознаваемой персональной информации, то специфическая информация об этом использовании cookie в предложении приведена далее.

Это Предложение программного обеспечения не использует cookie или другие технологии для сбора опознаваемой персональной информации.

Если конфигурации, развернутые для этого Предложения программного обеспечения предоставляют вам как клиенту возможность собирать опознаваемую персональную информацию о конечных пользователях посредством cookie и других технологий, вы должны самостоятельно проконсультироваться с юристом о всех законах, применимых к такому сбору данных, включая требования к уведомлению и согласию.

Более подробная информация об использовании различных технологий, включая cookie, для этих целей, приведена в Политике конфиденциальности IBM (http://www.ibm.com/privacy) и Заявлении IBM о конфиденциальности в Интернет (http://www.ibm.com/privacy/details), а также в разделах “Cookies, Web Beacons and Other Technologies” и “IBM Software Products and Software-as-a-Service Privacy Statement” на странице http://www.ibm.com/software/info/product-privacy.

Товарные знаки

IBM, эмблема IBM и ibm.com являются товарными знаками или зарегистрированными товарными знаками International Business Machines Corp. во всем мире. Названия других продуктов и услуг могут быть товарными знаками IBM и других компаний. Текущий список товарных знаков IBM опубликован на веб-странице Copyright and trademark information по следующему адресу: www.ibm.com/legal/copytrade.shtml.

Linux является зарегистрированным товарным знаком Линуса Торвальдса в США и других странах.

Java и все основанные на Java названия и эмблемы являются товарными знаками или зарегистрированными товарными знаками Oracle и/или дочерних компаний.

Индекс

P

C

T

У

Напечатано в Дании