IBM PowerSC

Standard Edition

версии 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

версии 1.1.6

PowerSC Standard Edition

Примечание

Перед началом работы с этим изданием и описанным в нем продуктом ознакомьтесь с информацией, приведенной в разделе “Примечания” на стр. 191.

Это издание применимо к IBM PowerSC Standard Edition версии 1.1.6 и ко всем последующим выпускам и модификациям, если в новых изданиях не указано иное.

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.

Новое в PowerSC Standard Edition

Здесь приведена новая и значительно измененная информация в наборе разделов для PowerSC Standard Edition версии 1.1.6.

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

Сентябрь 2017 г.

В GUI PowerSC добавлены следующие компоненты:

- Добавлена верхнеуровневая сводная панель Защита и соответствие, содержащая общий обзор всей информации о состоянии соответствия и актуальной целостности файлов.
- Добавлена интеграция с администраторами виртуализации, такими как PowerVC, через Open Stack, что обеспечивает автоматизированный и безопасный поиск конечных точек. Кроме того, интеграция поддерживает облачную среду с визуализацией защиты с момента создания VM.
- Добавлены средства создания отчетов для поддержки контроля. Обзорные и подробные отчеты о соответствии и целостности файлов теперь можно создавать в виде файлов CSV, вложенных в сообщения в формате HTML. Можно запланировать как немедленную, так и ежедневную рассылку этих отчетов.
- Enhanced Profile Editor расширяет ваши возможности по настройке правил и профайлов соответствия. Правила теперь можно брать из различных источников и редактировать в GUI.
- Добавлена интеграция с администраторами информации о событиях, относящихся к защите, таких как QRadar. Благодаря записям Syslog о значимых событиях, относящихся к соответствию и целостности файлов, интеграция стала легко осуществимой.
- Улучшенные функции UNDO позволяют упростить выполнение сложной задачи отмены примененного профайла. В PowerSC 1.1.6 достигнут значительный прогресс в обеспечении незаметности применения UNDO к профайлу PCI.
- Улучшена масштабируемость GUI для соответствия. Сервер GUI горизонтально масштабируем, и каждый экземпляр может поддерживать до тысячи и более конечных точек.

Добавлены следующие функции TNCPM:

- Появился прокси-сервер, предоставляющий дополнительный уровень защиты за счет изоляции TNCPM от Интернета.
- Интеграция временных исправлений (ifix) в TNCPM теперь полностью автоматизирована. TNCPM может отслеживать и исправлять любые уязвимости, относящиеся к операционной системе, без вмешательства пользователя.
- Загрузка пакетов с открытым исходным текстом теперь интегрирована в TNCPM, что оптимизирует поток операций над объектами с открытым исходным текстом.

Добавлена следующая функция для расширения возможностей соответствия:

- Добавлена опция отчета, предоставляющая сведения о правилах, включенных в применяемый профайл.

Файлы PDF PowerSC Standard Edition

Документация по PowerSC Standard Edition поставляется в виде файлов PDF.

- PowerSC Standard Edititon
- Информация о выпусках PowerSC Standard Edition

Концепции PowerSC Standard Edition

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 соответствия требованиям, надежную загрузку, надежный брандмауэр, надежное ведение протоколов, а также надежное сетевое соединение 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 • Акт о преемственности и подотчетности медицинского страхования (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
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 • AIX 7.2 • VIOS версии 2.2.1.4 или более поздней	• POWER6 • POWER7 • POWER8 • Сервер виртуального ввода-вывода версии 6.1S или более поздней

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

Компоненты	**Описание**	**Поддерживаемая операционная система**	**Поддерживаемое аппаратное обеспечение**
Trusted Logging	Протоколы AIX централизованно собираются на виртуальном сервере ввода-вывода (VIOS) в режиме реального 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 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Надежное сетевое соединение 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 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Клиент структуры Надежное сетевое соединение	Клиенту TNC необходим один из компонентов, перечисленных с операционной системой.	• 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 • Система консоли SUMA для AIX версии 7.2.1 в среде SUMA для управления исправлениями	

Установка PowerSC Standard Edition

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

Для PowerSC Standard Edition и GUI (графический пользовательский интерфейс) PowerSC доступны следующие наборы файлов:

- `powerscStd.ice`: устанавливается в системах AIX, для которых требуется функция автоматизации защиты и соответствия PowerSC Standard Edition. Программе соответствия требуется по крайней мере 5 Мб дисковой памяти в файловой системе "/".
- `powerscStd.vtpm`: устанавливается в системах AIX, для которых требуется функция защищенной загрузки в PowerSC Standard Edition. Набор файлов powerscStd.vtpm можно получить из базового носителя AIX или из https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm.
- `powerscStd.vlog`: устанавливается в системах AIX, для которых требуется функция защищенного ведения протокола в PowerSC Standard Edition.
- `powerscStd.tnc_pm`: устанавливается в AIX версии 7.1 TL4 или выше, с системой консоли SUMA в среде SUMA, для управления исправлениями в версии 7.2.1.0. Для защищенной передачи временных исправлений из IBM Security Site необходимо установить Curl 7.52.1-1 в TNC Patch Manager.
- `powerscStd.svm`: устанавливается в системах AIX для использования функций маршрутизации PowerSC Standard Edition.
- `powerscStd.rtc`: устанавливается в системы AIX, которым требуется режим соответствия требованиям реального времени PowerSC Standard Edition.
- `powerscStd.uiAgent.rte`: устанавливается в системах AIX, которые будут работать под управлением GUI (графический пользовательский интерфейс) PowerSC. Для установки powerscStd.uiAgent.rte 116 необходимо установить набор файлов powerscStd.ice 115 или выше.
- `powerscStd.uiServer.rte`: устанавливается в системах AIX, настроенных для запуска сервера GUI (графический пользовательский интерфейс) PowerSC.

PowerSC Standard Edition и GUI (графический пользовательский интерфейс) PowerSC 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**.

Дополнительная информация об установке GUI (графический пользовательский интерфейс) PowerSC приведена в разделе “Установка GUI PowerSC” на стр. 146.

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” на стр. 5
В обзоре PowerSC Standard Edition описаны функции, компоненты и поддержка оборудования, относящиеся к компоненту PowerSC Standard Edition.

“Установка функции Надежная загрузка” на стр. 113
Для установки функции Надежная загрузка требуются некоторые конфигурации аппаратного и программного обеспечения.

Задачи, связанные с данной:

“Установка Надежного брандмауэра” на стр. 121
Установка Надежного брандмауэра PowerSC подобна установке любой другой функции PowerSC.

“Установка Защищенных протоколов” на стр. 128
Можно установить функцию Защищенные протоколы PowerSC с помощью интерфейса командной строки или инструмента SMIT.

“Настройка компонентов TNC” на стр. 134
Каждый из компонентов TNC требует некоторой настройки для работы в конкретной среде.

Автоматизация защиты и согласования

AIX Profile Manager позволяет управлять заранее определенными профайлами защиты и согласования. PowerSC Real Time Compliance постоянно отслеживает включенные системы AIX для гарантии их согласованной и защищенной настройки.

Профайлы XML автоматизируют рекомендованную конфигурацию системы AIX IBM для соответствия стандарту защиты данных платежных карт, закону Сарбейнса-Оксли либо указаниям министерства обороны по технической реализации защиты UNIX и Акту о преемственности и подотчетности медицинского страхования (HIPAA). Организации, следующие стандартам защиты, должны использовать заранее определенные параметры без опасности систем.

AIX Profile Manager работает как модуль IBM® Systems Director, упрощающий применение, отслеживание и контроль параметров защиты, как для операционных систем AIX, так и для систем VIOS (Сервер виртуального ввода-вывода). Для использования функции соответствия требованиям защиты необходимо установить приложение PowerSC в управляемой системе AIX, отвечающей стандартам соответствия. Функция Автоматизация защиты и согласования входит в состав PowerSC Standard Edition.

В управляемых системах AIX необходимо установить пакет установки PowerSC Standard Edition 5765-PSE. Пакет установки устанавливает набор файлов `powerscStd.ice`, который можно внедрить в систему с помощью команды AIX Profile Manager или **pscxpert**. PowerSC с согласованием IBM Compliance Expert Express (ICEE) позволяет управлять профайлами XML и улучшать их. Профайлы XML управляются с помощью AIX Profile Manager.

Примечание: Перед применением профайла защиты установите в системе все приложения.

Понятия автоматизации обеспечения соответствия и защиты

Функция обеспечения соответствия и защиты PowerSC - это автоматизированный способ настройки и контроля систем AIX в соответствии с указаниями министерства обороны США (DoD) по технической реализации защиты (STIG), стандартом защиты информации в сфере платежных карт (PCI DSS), законом Сарбейна-Оксли и согласованием COBIT (SOX/COBIT), а также с Актом о преемственности и подотчетности медицинского страхования (HIPAA).

PowerSC помогает автоматизировать настройку и мониторинг систем, которые должны соответствовать версии 1.2, 2.0 или 3.0 стандарта защиты данных в сфере платежных карт (PCI DSS). Поэтому функция обеспечения согласования и защиты PowerSC является точным и законченным методом автоматизации настройки защиты, применяемым для соответствия ИТ требованиям DoD UNIX STIG, PCI DSS, закону Сарбейна-Оксли и COBIT (SOX/COBIT), а также Акту о преемственности и подотчетности медицинского страхования (HIPAA).

Примечание: Обеспечение соответствия и защита PowerSC изменяет существующие профайлы XML, используемые в издании IBM Compliance Expert express (ICEE). Профайлы XML PowerSC Standard Edition можно использовать с командой **pscxpert** аналогично ICEE.

Поставляемые в составе PowerSC Standard Edition заранее настроенные профайлы обеспечения соответствия требованиям законодательства снижают административную нагрузку интерпретации документации о соответствии требованиям и внедрения стандартов в качестве параметров конфигурации конкретных систем. Эта технология уменьшает стоимость контроля и настройки соответствия требования законодательства путем автоматизации процессов. IBMPowerSC Standard Edition разработана для помощи в эффективном управлении требованиями к системе, связанными с соответствием внешним стандартам, что может снизить стоимость и повысить соответствие требованиям законодательства.

Соответствие требованиям STIG Министерства обороны США.

Министерство обороны США требует высокий уровень защиты компьютерных систем. Уровень защиты и качества, установленный Министерством обороны США, соответствует качеству и клиентской базе AIX на сервере Power Systems.

Для достижения указанных целей защиты защищенная операционная система, такая как AIX, должна быть правильно настроена. Директивой 8500.1 Министерство обороны США признало необходимость в конфигурациях защиты для всех операционных систем. Данная директива устанавливает стратегию и возлагает ответственность за руководство настройкой защиты на Агентство защиты информации Министерства обороны США (DISA).

DISA разработала принципы и рекомендации и опубликовало руководство по технической реализации защиты UNIX (STIG), в котором описывается среда, отвечающая или превосходящая требования к защите систем Министерства обороны США, работающих на уровне важности MAC II, который содержит важную информацию. Министерство обороны США имеет строгие требования к безопасности ИТ и составило подробный список значений параметров конфигурации, гарантирующих безопасную работу системы. Есть возможность воспользоваться необходимыми рекомендациями экспертов. PowerSC Standard Edition помогает автоматизировать процесс настройки параметров в соответствии с требованиями Министерства обороны США.

Примечание: Все файлы пользовательских сценариев для обеспечения соответствия требованиям Министерства обороны США находятся в каталоге `/etc/security/pscexpert/dodv2`.

PowerSC Standard Edition поддерживает требования версии 1, выпуск 2, STIG Министерства обороны США для AIX. Требования и инструкции по обеспечению их соблюдения приведены в следующих таблицах.

Таблица 2. Общие требования Министерства обороны США

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00020	2	Требуется реализация программного обеспечения защищенной компьютерной базы AIX.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
AIX00040	2	Должна использоваться команда **securetcpip**.	**Расположение** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
AIX00060	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00080	1	Атрибут `SYSTEM` не должен быть *none* ни у какой учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/SYSattr` **Действие, обеспечивающее соответствие** Гарантирует, что значение указанного атрибута не *none*. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
AIX00200	2	Система не должна пропускать направленные широковещательные рассылки через брандмауэр.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `direct_broadcast` значение *0*.
AIX00210	2	Система должна обеспечивать защиту от атак ICMP на соединения TCP.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `tcp_icmpsecure` значение *1*.
AIX00220	2	Система должна обеспечивать защиту стека TCP от атак посредством сброса соединения, синхронизации (SYN) и внедрения данных.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Гарантирует, что сетевой параметр `tcp_tcpsecure` равен *7*.
AIX00230	2	Система должна обеспечивать защиту от атак посредством фрагментации пакетов IP.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ip_nfrag` значение *200*.
AIX00300	1,2,3	В системе не должно быть активной службы `bootp`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает указанную службу.
AIX00310	2	Файлы `/etc/ftpaccess.ctl` должны существовать.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Действие, обеспечивающее соответствие** Гарантирует существование файла.
GEN000020	2	Система должна требовать идентификацию при запуске в однопользовательском режиме.	**Расположение** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Действие, обеспечивающее соответствие** Гарантирует, что учетная запись root для всех загрузочных разделов имеет пароль в файле `/etc/security/passwd`. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000100	1	Версия операционной системы должна быть поддерживаемой.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cat1` **Действие, обеспечивающее соответствие** Показывает результаты указанных тестов правил.

GEN000120	2	Должно быть установлено большинство текущих обновлений и исправлений защиты системы.	**Расположение**
			`/usr/sbin/instfix -i`
			`/etc/security/pscexpert/dodv2/dodv2cat1`
			Действие, обеспечивающее соответствие
			Настройте это с помощью функции TNC.

GEN000140	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.
GEN000220	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.
GEN000240	2	Системные часы должны быть синхронизированы с авторитетным источником времени Министерства обороны США.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Гарантирует соответствие системных часов требованиям.
GEN000241	2	Системные часы должны регулярно синхронизироваться, не реже раза в сутки.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Гарантирует соответствие системных часов требованиям.
GEN000242	2	Система должна иметь не менее двух источников времени для синхронизации часов.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2netrules` **Действие, обеспечивающее соответствие** Гарантирует использование нескольких источников времени для синхронизации часов.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000280	2	Должен быть запрещен прямой вход в следующие типы учетных записей: • application • default • shared • utility	**Расположение** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Действие, обеспечивающее соответствие** Запрещает прямой вход в указанные учетные записи.
GEN000290	2	Система не должна иметь лишних учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Действие, обеспечивающее соответствие** Гарантирует отсутствие ненужных учетных записей.
GEN000300 (связан с GEN000320, GEN000380, GEN000880)	2	Все учетные записи в системе должны иметь уникальное имя пользователя или учетной записи и уникальный пароль пользователя или учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует, что все учетные записи отвечают указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000320 (связан с GEN000300, GEN000380, GEN000880)	2	Все учетные записи в системе должны иметь уникальное имя пользователя или учетной записи и уникальный пароль пользователя или учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует, что все учетные записи отвечают указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000340	2	ИД пользователей (UID) и ИД групп (GID), зарезервированные для системных учетных записей, не должны присваиваться несистемным учетным записям или группам.	**Расположение** `/etc/security/pscexpert/dodv2/account` **Действие, обеспечивающее соответствие** Этот параметр автоматически включается для выполнения данного правила.
GEN000360	2	ИД пользователей (UID) и ИД групп (GID), зарезервированные для системных учетных записей, не должны присваиваться несистемным учетным записям или группам.	**Расположение** `/etc/security/pscexpert/dodv2/account` **Действие, обеспечивающее соответствие** Этот параметр автоматически включается для выполнения данного правила.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000380 (связан с GEN000300, GEN000320, GEN000880)	2	Все учетные записи в системе должны иметь уникальное имя пользователя или учетной записи и уникальный пароль пользователя или учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует, что все учетные записи отвечают указанным требованиям.
GEN000400	2	Текст Министерства обороны США, показываемый при входе, должен показываться сразу перед или как часть приглашения консольного входа.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Действие, обеспечивающее соответствие** Показывает требуемый текст.
GEN000402	2	Текст Министерства обороны США, показываемый при входе в систему, должен показываться сразу перед или как часть приглашения входа в графическую среду рабочего стола.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Действие, обеспечивающее соответствие** Задает текст Министерства обороны США, показываемый при входе в систему.
GEN000410	2	Служба FTPS или FTP в системе должна быть настроена для показа текста Министерства обороны США при входе.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Действие, обеспечивающее соответствие** Показывает текст Министерства обороны США при входе на сервер FTP.
GEN000440	2	Должны записываться успешные и неуспешные попытки входа в систему и выхода из системы.	**Расположение** `/etc/security/pscexpert/dodv2/loginout` **Действие, обеспечивающее соответствие** Включает ведение требуемых протоколов.
GEN000452	2	Система должна показывать дату и время предыдущего успешного входа в учетную запись при каждом входе в систему.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Показывает требуемую информацию.
GEN000460	2	Это правило отключает учетную запись после 3 неудачных попыток входа в систему подряд.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Задает ограничение на количество попыток входа в систему.
GEN000480	2	Это правило устанавливает 4-секундную задержку входа в систему.	**Расположение** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Действие, обеспечивающее соответствие** Устанавливает требуемую задержку входа в систему.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000540	2	Это правило гарантирует, что глобальные системные файлы конфигурации паролей настроены в соответствии с требованиями к паролям.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Задает требуемые параметры паролей.
GEN000560	1	Все учетные записи в системе должны иметь допустимые пароли.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует наличие паролей у учетных записей.
GEN000580	2	Это правило гарантирует, что все пароли содержат не менее 14 символов.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Задает минимальную длину пароля 14 символов.
GEN000585	2	Система должна использовать утвержденный FIPS 140-2 криптографический алгоритм хэширования для генерации хэшей паролей учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/fipspasswd` **Действие, обеспечивающее соответствие** Гарантирует, что для хэшей паролей используется утвержденный алгоритм хэширования.
GEN000590	2	Система должна использовать утвержденный FIPS 140-2 криптографический алгоритм хэширования для генерации хэшей паролей учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/fipspasswd` **Действие, обеспечивающее соответствие** Гарантирует, что для хэшей паролей используется утвержденный алгоритм хэширования.
GEN000595	2	Использовать утвержденный FIPS 140-2 алгоритм хэширования при генерации хэшей паролей, хранящихся в системе.	**Расположение** `/etc/security/pscexpert/dodv2/fipspasswd` **Действие, обеспечивающее соответствие** Гарантирует, что для хэшей паролей используется утвержденный алгоритм хэширования.
GEN000640	2	Это правило требует наличия хотя бы одного неалфавитного символа в пароле	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Указывает, что пароль должен содержать не менее 1 неалфавитного символа.
GEN000680	2	Это правило гарантирует, что пароли содержат не более 3 одинаковых символов подряд	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Указывает, что пароль должен содержать не более 3 повторяющихся символов.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000700	2	Это правило гарантирует, что глобальные системные файлы конфигурации паролей настроены в соответствии с требованиями к паролям.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Гарантирует, что файлы конфигурации паролей соответствуют требованиям.

GEN000740	2	Пароли всех неинтерактивных учетных записей и учетных записей автоматической обработки должны быть заблокированы (GEN000280). Прямой вход в систему должен быть запрещен для общих учетных записей, учетных записей по умолчанию, учетных записей приложений и служебных учетных записей. (GEN002640) Системные учетные записи по умолчанию следует выключить или удалить.	**Расположение**
			`/etc/security/pscexpert/dodv2/loginout`
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			Действие, обеспечивающее соответствие
			Этот параметр включается автоматически.

GEN000740	2	Пароли всех учетных записей для автоматической обработки и неинтерактивных учетных записей следует менять не реже раза в год или блокировать их.	**Расположение** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Действие, обеспечивающее соответствие** Гарантирует, что указанные пароли меняются раз в год или блокируются.
GEN000750	2	Это правило требует, чтобы новые пароли содержали не менее 4 символов, которых не было в прежнем пароле.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Задает минимальное количество новых символов в новом пароле, равное 4.
GEN000760	2	Учетные записи должны блокироваться после 35 дней отсутствия активности.	**Расположение** `/etc/security/pscexpert/dodv2/disableacctdod` **Действие, обеспечивающее соответствие** Блокирует учетные записи после 35 дней отсутствия активности.
GEN000790	2	Система не должна допускать использование словарных слов в качестве паролей.	**Расположение** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Действие, обеспечивающее соответствие** Гарантирует стойкость устанавливаемого пароля по умолчанию.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000800	2	Это правило запрещает повторное использование последних 5 паролей.	**Расположение** `/etc/security/pscexpert/dodv2/chusrattrdod` **Действие, обеспечивающее соответствие** Гарантирует, что новый пароль не совпадает с последними 5 паролями.
GEN000880 (связан с GEN000300, GEN000320, GEN000380)	2	Все учетные записи в системе должны иметь уникальное имя пользователя или учетной записи и уникальный пароль пользователя или учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует, что все учетные записи отвечают указанным требованиям.
GEN000900	3	Домашний каталог пользователя root не должен находиться в корневом каталоге (/).	**Расположение** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанному требованию. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000940	2	Путь поиска исполняемых файлов учетной записи root должен иметь значение по умолчанию, установленное вендором, и должен содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000945	2	Путь поиска библиотек учетной записи root должен иметь системное значение по умолчанию и должен содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000950	2	Список заранее загружаемых библиотек учетной записи root должен быть пустым.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000960 (связан с GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	В пути поиска исполняемых файлов учетной записи root не должно быть каталогов, доступных на запись всем пользователям.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000980	2	Система должна запрещать прямой вход в учетную запись пользователя root, за исключением системной консоли.	**Расположение** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN001000	2	Консоли удаленного доступа должны быть выключены и защищены от несанкционированного доступа.	**Расположение** `/etc/security/pscexpert/dodv2/remoteconsole` **Действие, обеспечивающее соответствие** Гарантирует, что указанные консоли выключены.
GEN001020	2	Учетная запись пользователя root не должна использоваться для прямого входа в систему.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Отключает прямой вход в учетную запись пользователя root.
GEN001060	2	Система должна вести протокол успешных и неуспешных попыток доступа к учетной записи пользователя root.	**Расположение** `/etc/security/pscexpert/dodv2/loginout` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN001100	1	Пароли пользователя root ни при каких обстоятельствах не должны передаваться через сеть в текстовой форме.	**Расположение** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN001120	2	Система должна запрещать вход пользователя root через протокол SSH.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Выключает вход пользователя root через SSH.
GEN001440	3	У всех интерактивных пользователей должен быть указан домашний каталог в файле `/etc/passwd`.	**Расположение** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Действие, обеспечивающее соответствие** Гарантирует, что все интерактивные пользователи имеют указанный каталог.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001475	2	Файл /etc/group не должен содержать хэшей паролей групп.	**Расположение** /etc/security/pscexpert/dodv2/passwdhash **Действие, обеспечивающее соответствие** Гарантирует отсутствие хэшей паролей групп в указанном файле. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла DoDv2_to_AIXDefault.xml. Этот параметр необходимо изменить вручную.
GEN001600	2	Пути поиска исполняемых файлов сценариев управления выполнением должны содержать только абсолютные пути.	**Расположение** /etc/security/pscexpert/dodv2/fixpathvars **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла DoDv2_to_AIXDefault.xml. Этот параметр необходимо изменить вручную.
GEN001605	2	Пути поиска библиотек сценариев управления выполнением должны содержать только абсолютные пути.	**Расположение** /etc/security/pscexpert/dodv2/fixpathvars **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла DoDv2_to_AIXDefault.xml. Этот параметр необходимо изменить вручную.
GEN001610	2	Списки заранее загружаемых библиотек сценариев управления выполнением должны содержать только абсолютные пути.	**Расположение** /etc/security/pscexpert/dodv2/fixpathvars **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла DoDv2_to_AIXDefault.xml. Этот параметр необходимо изменить вручную.
GEN001840	2	Пути поиска исполняемых файлов всех глобальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** /etc/security/pscexpert/dodv2/fixpathvars **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла DoDv2_to_AIXDefault.xml. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001845	2	Пути поиска библиотек всех глобальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001850	2	Списки заранее загружаемых библиотек всех глобальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001900	2	Пути поиска исполняемых файлов всех локальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001901	2	Пути поиска библиотек всех локальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001902	2	Списки заранее загружаемых библиотек всех локальных файлов инициализации должны содержать только абсолютные пути.	**Расположение** `/etc/security/pscexpert/dodv2/fixpathvars` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001940	2	Файлы инициализации пользователя не должны запускать программ, доступных на запись всем пользователям.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN001980	2	Файлы `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` или `/etc/group` не должны содержать знака плюса (+) без определения записей для сетевых групп NIS+.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2netrules` **Действие, обеспечивающее соответствие** Гарантирует, что указанные файлы соответствуют указанным требованиям.
GEN002000	2	В системе не должно быть файлов `.netrc`.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2netrules` **Действие, обеспечивающее соответствие** Гарантирует отсутствие указанных файлов в системе. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN002020	2	Все файлы `.rhosts`, `.shosts` и `hosts.equiv` должны содержать только надежные пары хост-пользователь.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2netrules` **Действие, обеспечивающее соответствие** Гарантирует, что указанные файлы соответствуют данному требованию.
GEN002040	1	Это правило выключает файлы `.rhosts`, `.shosts` и `hosts.equiv` и файлы `shosts.equiv`.	**Расположение** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Действие, обеспечивающее соответствие** Выключает указанные файлы.
GEN002120	1,2	Это правило проверяет и настраивает оболочки пользователей.	**Расположение** `/etc/security/pscexpert/dodv2/usershells` **Действие, обеспечивающее соответствие** Создает требуемые оболочки. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN002140	1,2	Все оболочки, указанные в файле `/etc/passwd`, должны быть перечислены в файле `/etc/shells`, за исключением оболочек, которые указаны для предотвращения входа в систему.	**Расположение** `/etc/security/pscexpert/dodv2/usershells` **Действие, обеспечивающее соответствие** Гарантирует, что оболочки указаны в правильных файлах. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN002280	2	Доступ на запись к файлам устройств и каталогам должен быть только у пользователей с системной учетной записью и у пользователей, которым такие права дал вендор.	**Расположение** `/etc/security/pscexpert/dodv2/wwdevfiles` **Действие, обеспечивающее соответствие** Показывает файлы устройств, каталоги и другие файлы из необщедоступных каталогов системы, которые доступны всем пользователям на запись.
GEN002300	2	Файлы устройств, используемые для резервного копирования, должны быть доступны на чтение и (или) запись только пользователю root и пользователю backup.	**Расположение** `/etc/security/pscexpert/dodv2/wwdevfiles` **Действие, обеспечивающее соответствие** Показывает файлы устройств, каталоги и другие файлы из необщедоступных каталогов системы, которые доступны всем пользователям на запись.
GEN002400	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах. **Примечание:** Сравнивает два последних еженедельных протокола, которые создаются в каталоге `/var/security/pscexpert`, на предмет наличия несанкционированной активности.
GEN002420	2	Съемные носители данных, удаленные файловые системы и прочие файловые системы, которые не содержат одобренных файлов `setuid`, должны монтироваться с параметром *nosuid*.	**Расположение** `/etc/security/pscexpert/dodv2/fsmntoptions` **Действие, обеспечивающее соответствие** Гарантирует, что удаленные файловые системы монтируются с указанными параметрами. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN002430	2	Съемные носители данных, удаленные файловые системы и прочие файловые системы, которые не содержат одобренных файлов устройств, должны монтироваться с параметром *nodev*.	**Расположение** `/etc/security/pscexpert/dodv2/fsmntoptions` **Действие, обеспечивающее соответствие** Гарантирует, что удаленные файловые системы монтируются с указанными параметрами. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

GEN002480	2	Доступ на запись всем пользователям должен быть разрешен только для общедоступных каталогов, и файлы, доступные всем пользователям на запись, должны находиться только в общедоступных каталогах.	**Расположение**
			`/etc/security/pscexpert/dodv2/wwdevfiles`
			`/etc/security/pscexpert/dodv2/fpmdodfiles`
			Действие, обеспечивающее соответствие
			Сообщает, когда файлы в необщедоступных каталогах доступны на запись всем пользователям.

GEN002640	2	Системные учетные записи по умолчанию следует выключить или удалить.	**Расположение**
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			`/etc/security/pscexpert/dodv2/loginout`
			Действие, обеспечивающее соответствие
			Выключает системные учетные записи по умолчанию.

GEN002660	2	Должен быть включен контроль.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Включает команду `dodaudit`, активирующую контроль.
GEN002720	2	Система контроля должна быть настроена для отслеживания неудачных попыток доступа к файлам и программам.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002740	2	Система контроля должна быть настроена для отслеживания удаления файлов.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002750	3	Система контроля должна быть настроена для отслеживания создания учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002751	3	Система контроля должна быть настроена для отслеживания изменения учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN002752	3	Система контроля должна быть настроена для отслеживания отключенных учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002753	3	Система контроля должна быть настроена для отслеживания удаления учетных записей.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002760	2	Система контроля должна быть настроена для отслеживания всех административных операций, привилегированных операций и операций, связанных с защитой.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002800	2	Система контроля должна быть настроена для отслеживания входа в систему, выхода из системы и открытия сеанса.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002820	2	Система контроля должна быть настроена для отслеживания любых изменений прав доступа подсистемы избирательного контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002825	2	Система контроля должна быть настроена для отслеживания загрузки и выгрузки динамических модулей ядра.	**Расположение** `/etc/security/pscexpert/dodv2/dodaudit` **Действие, обеспечивающее соответствие** Автоматически включает указанный режим контроля.
GEN002860	2	Требуется ежедневная ротация протоколов контроля.	**Расположение** `/etc/security/pscexpert/dodv2/rotateauditdod` **Действие, обеспечивающее соответствие** Гарантирует выполнение ротации протоколов контроля.
GEN002960	2	Доступ к утилите `cron` должен контролироваться с помощью файла `cron.allow` и (или) файла `cron.deny`.	**Расположение** `/etc/security/pscexpert/dodv2/limitsysacc` **Действие, обеспечивающее соответствие** Гарантирует включение ограничений.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003000 (связан с GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	Утилита `cron` не должна запускать программы, которые доступны на запись группе или всем пользователям.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует включение ограничений. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003020 (связан с GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	Утилита `cron` не должна запускать программы, находящиеся в каталогах, доступных на запись всем пользователям, или в их подкаталогах.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Запрещает пользователям, не входящим в группу владельца, доступ на запись к каталогам программы `cron`. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003060	2	Системные учетные записи по умолчанию (за исключением root) должны отсутствовать в файле `cron.allow` или должны быть добавлены в файл `cron.deny`, если файл `cron.allow` отсутствует.	**Расположение** `cron.allow` или `cron.deny` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003160 (связан с GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	Должен вестись протокол работы утилиты `cron`.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003280	2	Доступ к утилите `at` должен контролироваться файлами `at.allow` и `at.deny`.	**Расположение** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003300	2	Файл `at.deny` не должен быть пустым, если существует.	**Расположение** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003320	2	Системные учетные записи по умолчанию, кроме root, должны отсутствовать в файле `at.allow` или должны быть добавлены в файл `at.deny`, если файл `at.allow` отсутствует.	**Расположение** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003360 (связан с GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	Демон `at` не должен запускать программы, которые доступны на запись группе или всем пользователям.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_ AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003380 (связан с GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	Демон `at` не должен запускать программы, находящиеся в каталогах, доступных на запись всем пользователям, или в их подкаталогах.	**Расположение** `/etc/security/pscexpert/dodv2/rmwwpaths` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_ AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003510	2	Создание дампов памяти ядра должно быть выключено, если в них нет необходимости.	**Расположение** `/etc/security/pscexpert/dodv2/coredumpdev` **Действие, обеспечивающее соответствие** Выключает создание дампов памяти ядра.
GEN003540	2	В системе должны использоваться неисполняемые программные стеки.	**Расположение** `/etc/security/pscexpert/dodv2/sedconfigdod` **Действие, обеспечивающее соответствие** Включает принудительное использование неисполняемых программных стеков.
GEN003600	2	Система не должна пересылать пакеты с фиксированным маршрутом IPv4.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipsrcforward` значение *0*.
GEN003601	2	Должны быть заданы соответствующие размеры очередей ожидающих соединений TCP.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `clean_partial_ conns` значение *1*.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003603	2	Система не должна отвечать на эхо-запросы ICMPv4, отправленные с широковещательного адреса.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `bcastping` значение *0*.
GEN003604	2	Система не должна отвечать на запросы времени ICMP, отправленные с широковещательного адреса.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `bcastping` значение *0*.
GEN003605	2	Система не должна применять обратную маршрутизацию отправителя к ответам TCP.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `nonlocsrcroute` значение *0*.
GEN003606	2	Система должна запрещать локальным приложениям генерировать пакеты с фиксированным маршрутом.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipsrcroutesend` значение *0*.
GEN003607	2	Система не должна принимать пакеты IPv4 с фиксированным маршрутом.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Выключает прием пакетов IPv4 с фиксированным маршрутом.
GEN003609	2	Система должна игнорировать сообщения перенаправления ICMP IPv4.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipignoreredirects` значение *1*.
GEN003610	2	Система не должна отправлять сообщения перенаправления ICMP IPv4.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipsendredirects` значение *0*.
GEN003612	2	Система должна быть настроена для использования SYN-cookie TCP в случае SYN-флуда TCP.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `clean_partial _conns` значение *1*.
GEN003640	2	Корневая файловая система должна использовать журнал или обеспечивать целостность другим способом.	**Расположение** `/etc/security/pscexpert/dodv2/chkjournal` **Действие, обеспечивающее соответствие** Включает журнал в корневой файловой системе.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003660	2	Система должна вести протокол данных идентификации и информационных данных.	**Расположение** `/etc/security/pscexpert/dodv2/chsyslogdod` **Действие, обеспечивающее соответствие** Включает ведение протокола данных `auth` и `info`.
GEN003700	2	Демоны `inetd` и `xinetd` должны быть выключены или удалены, если не используются сетевыми службами.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003810	2	Службы `portmap` и `rpcbind` не должны выполняться без необходимости.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003815	2	Службы `portmap` и `rpcbind` не должны устанавливаться без необходимости.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003820-3860	1,2,3	Демоны `rsh`, `rexexec` и `telnet` и служба `rlogind` не должны выполняться.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN003865	2	Не должно быть установленных инструментов анализа сети.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN003900	2	Файл `hosts.lpd` (или эквивалентный) не должен содержать знака плюса (+).	**Расположение** `/etc/security/pscexpert/dodv2/printers` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN004220	1	В административных учетных записях не должен запускаться веб-браузер, за исключением случаев, когда он нужен для администрирования локальных служб.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cat1` **Действие, обеспечивающее соответствие** Показывает результаты указанных тестов правил.
GEN004460	2	Это правило включает ведение протокола данных `auth` и `info`.	**Расположение** `/etc/security/pscexpert/dodv2/chsyslogdod` **Действие, обеспечивающее соответствие** Включает ведение протокола данных `auth` и `info`.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям

GEN004540	2	Это правило выключает команду справки `sendmail`.	**Расположение**
			`/etc/security/pscexpert/dodv2/sendmailhelp`
			`/etc/security/pscexpert/dodv2/dodv2cmntrows`
			Действие, обеспечивающее соответствие
			Выключает указанную команду.

GEN004580	2	Система не должна использовать файлы `.forward`.	**Расположение** `/etc/security/pscexpert/dodv2/forward` **Действие, обеспечивающее соответствие** Выключает указанные файлы. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004600	1	Служба `SMTP` должна быть самой последней версии.	**Расположение** `/etc/security/pscexpert/dodv2/SMTP_ver` **Действие, обеспечивающее соответствие** Гарантирует, что выполняется самая последняя версия указанной службы. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004620	2	У сервера `sendmail` должна быть выключена функция отладки.	**Расположение** `/etc/security/pscexpert/dodv2/SMTP_ver` **Действие, обеспечивающее соответствие** Выключает функцию отладки `sendmail`.
GEN004640	1	Служба `SMTP` не должна иметь активного псевдонима `uudecode`.	**Расположение** `/etc/security/pscexpert/dodv2/SMTPuucode` **Действие, обеспечивающее соответствие** Выключает псевдоним `uudecode` .
GEN004710	2	Передача электронной почты должна быть ограничена.	**Расположение** `/etc/security/pscexpert/dodv2/sendmaildod` **Действие, обеспечивающее соответствие** Ограничивает передачу электронной почты.
GEN004800	1,2,3	Незашифрованный FTP не должен использоваться в системе.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN004820	2	Анонимный доступ к FTP должен быть выключен в системе, если он не санкционирован.	**Расположение** `/etc/security/pscexpert/dodv2/anonuser` **Действие, обеспечивающее соответствие** Выключает анонимный доступ к FTP в системе. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004840	2	Если система - сервер FTP анонимного доступа, она должна быть изолирована в сети нейтральной области (DMZ).	**Расположение** `/etc/security/pscexpert/dodv2/anonuser` **Действие, обеспечивающее соответствие** Гарантирует, что сервер FTP анонимного доступа в системе находится в сети нейтральной зоны (DMZ).
GEN004880	2	Должен существовать файл `ftpusers`.	**Расположение** `/etc/security/pscexpert/dodv2/chdodftpusers` **Действие, обеспечивающее соответствие** Гарантирует наличие указанного файла в системе.
GEN004900	2	Файл `ftpusers` должен содержать имена учетных записей, которым запрещено использовать протокол FTP.	**Расположение** `/etc/security/pscexpert/dodv2/chdodftpusers` **Действие, обеспечивающее соответствие** Гарантирует наличие требуемых имен учетных записей в файле.
GEN005000	1	Учетные записи сервера FTP анонимного доступа не должны иметь функциональной оболочки.	**Расположение** `/etc/security/pscexpert/dodv2/usershells` **Действие, обеспечивающее соответствие** Удаляет оболочки из учетных записей сервера FTP анонимного доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN005080	1	Демон `TFTP` должен работать в защищенном режиме, в котором обеспечивается доступ только к одному каталогу в файловой системе хоста.	**Расположение** `/etc/security/pscexpert/dodv2/tftpdod` **Действие, обеспечивающее соответствие** Гарантирует, что демон соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005120	2	Демон TFTP должен быть настроен по спецификациям вендора, включая выделенную учетную запись пользователя TFTP, оболочку без входа в систему, например `/bin/false`, и домашний каталог, владельцем которого является пользователь TFTP.	**Расположение** `/etc/security/pscexpert/dodv2/tftpdod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005140	1,2,3	Любой активный демон TFTP должен быть санкционирован и одобрен в пакете аккредитации системы.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Гарантирует, что демон санкционирован.
GEN005160	1,2	Любой хост X Window System должен создавать файл `.Xauthority`.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2disableX` **Действие, обеспечивающее соответствие** Гарантирует создание указанного файла хостом.
GEN005200	1,2	Экспортированные дисплеи X Window System не должны быть общедоступными.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2disableX` **Действие, обеспечивающее соответствие** Выключает распространение указанных программ.
GEN005220	1,2	Должны использоваться файлы `.Xauthority` или `X*.hosts` (или эквивалентные) для ограничения доступа к серверу X Window System.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2disableX` **Действие, обеспечивающее соответствие** Гарантирует, что указанные файлы для ограничения доступа к серверу есть в системе.
GEN005240	1,2	Утилита .Xauthority должна разрешать доступ только к санкционированным хостам.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2disableX` **Действие, обеспечивающее соответствие** Гарантирует, что доступ ограничен только санкционированными хостами.
GEN005260	2	Это правило выключает соединения X Window System и администратор входа XServer.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Выключает требуемые соединения и администратор входа.
GEN005280	1,2,3	В системе не должно быть активной службы `UUCP`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005300	2	В сообществах SNMP должны быть изменены параметры по умолчанию.	**Расположение** `/etc/security/pscexpert/dodv2/chsnmp` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005305	2	Служба SNMP должна использовать SNMP не ниже версии 3.	**Расположение** `/etc/security/pscexpert/dodv2/chsnmp` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005306	2	Служба SNMP должна требовать применения FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/chsnmp` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005440	2	Система должна использовать удаленный сервер syslog (хост протокола).	**Расположение** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Действие, обеспечивающее соответствие** Гарантирует, что система использует удаленный сервер syslog.
GEN005450	2	Система должна использовать удаленный сервер syslog (хост протокола).	**Расположение** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Действие, обеспечивающее соответствие** Гарантирует, что система использует удаленный сервер syslog.
GEN005460	2	Система должна использовать удаленный сервер syslog (хост протокола).	**Расположение** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Действие, обеспечивающее соответствие** Гарантирует, что система использует удаленный сервер syslog.
GEN005480	2	Система должна использовать удаленный сервер syslog (хост протокола).	**Расположение** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Действие, обеспечивающее соответствие** Гарантирует, что система использует удаленный сервер syslog.
GEN005500	2	Демон SSH должен быть настроен для использования только протокола SSH версии 2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005501	2	Клиент SSH должен быть настроен для использования только протокола SSH версии 2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005504	2	Демон SSH должен работать только на сетевых адресах управления, если не санкционировано его использование для других целей.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005505	2	Демон SSH должен использовать только шифры, соответствующие требованиям стандартов FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005506	2	Демон SSH должен использовать только шифры, соответствующие требованиям стандартов FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005507	2	Демон SSH должен использовать только коды идентификации сообщений (MAC) с криптографическими алгоритмами хэширования, соответствующими требованиям стандартов FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005510	2	Демон SSH должен использовать только коды идентификации сообщений с шифрами, которые соответствуют требованиям стандартов FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005511	2	Демон SSH должен использовать только коды идентификации сообщений с шифрами, которые соответствуют требованиям стандартов FIPS 140-2.	**Расположение** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005512	2	Демон SSH должен использовать только коды идентификации сообщений (MAC) с криптографическими алгоритмами хэширования, соответствующими требованиям стандартов FIPS 140-2.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005521	2	Демон SSH должен ограничивать вход определенными пользователями или группами.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005536	2	Демон SSH должен выполнять строгую проверку файлов конфигурации домашнего каталога.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005537	2	Демон SSH должен использовать разделение прав доступа.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005538	2	Демон SSH не должен разрешать в rhosts идентификацию с помощью криптосистемы RSA.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005539	2	Демон SSH не должен разрешать сжатие или разрешать его только после успешной идентификации.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005550	2	В демоне SSH должен быть настроен текст Министерства обороны США, показываемый при входе в систему.	**Расположение** /etc/security/pscexpert/dodv2/sshDoDconfig **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005560	2	Определяет, настроен ли шлюз по умолчанию для IPv4.	**Расположение** `/etc/security/pscexpert/dodv2/chkgtway` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную. **Примечание:** Если система использует протокол IPv6, параметр *ipv6_enabled* в файле `/etc/security/pscexpert/ipv6.conf` должен иметь значение `yes`. Если система не использует IPv6, то параметр *ipv6_enabled* должен быть `no`.
GEN005570	2	Определяет, настроен ли шлюз по умолчанию для IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/chkgtway` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную. **Примечание:** Если система использует протокол IPv6, параметр *ipv6_enabled* в файле `/etc/security/pscexpert/ipv6.conf` должен иметь значение `yes`. Если система не использует IPv6, то параметр *ipv6_enabled* должен быть `no`.
GEN005590	2	Демоны протоколов маршрутизации разрешены только в том случае, если система выполняет роль маршрутизатора.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005590	2	Демоны протоколов маршрутизации разрешены только в том случае, если система выполняет роль маршрутизатора.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN005600	2	Пересылка пакетов IP должна быть выключена для IPv4, если система не является маршрутизатором.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipforwarding` значение *0*.
GEN005610	2	В системе должна быть выключена пересылка пакетов IP для IPv6, если система не является маршрутизатором IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ip6forwarding` значение *1*.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005820	2	UID (ИД пользователя) и GID (ИД группы) для анонимного доступа в NFS не должны обладать правами доступа.	**Расположение** `/etc/security/pscexpert/dodv2/nfsoptions` **Действие, обеспечивающее соответствие** Гарантирует, что указанные ИД не имеют прав доступа.
GEN005840	2	Сервер NFS должен ограничивать доступ к файловым системам локальными хостами.	**Расположение** `/etc/security/pscexpert/dodv2/nfsoptions` **Действие, обеспечивающее соответствие** Настраивает сервер NFS для ограничения доступа локальными хостами.
GEN005880	2	Сервер NFS не должен разрешать удаленный доступ пользователя root.	**Расположение** `/etc/security/pscexpert/dodv2/nfsoptions` **Действие, обеспечивающее соответствие** Выключает удаленный доступ пользователя root на сервере NFS.
GEN005900	2	Должен быть указан параметр *nosuid* во всех операциях монтирования клиентов NFS.	**Расположение** `/etc/security/pscexpert/dodv2/nosuid` **Действие, обеспечивающее соответствие** Указывает параметр *nosuid* во всех операциях монтирования клиентов NFS.
GEN006060	2	В системе не должна выполняться служба `Samba` без необходимости.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN006380	1	Система не должна использовать UDP для NIS или NIS+.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cat1` **Действие, обеспечивающее соответствие** Показывает результаты указанных тестов правил.
GEN006400	2	Протокол NIS запрещен.	**Расположение** `/etc/security/pscexpert/dodv2/nisplus` **Действие, обеспечивающее соответствие** Выключает указанный протокол. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006420	2	Карты NIS должны быть защищены трудно угадываемыми именами доменов.	**Расположение** `/etc/security/pscexpert/dodv2/nisplus` **Действие, обеспечивающее соответствие** Гарантирует, что имена доменов трудно определить.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN006460	2	Все серверы NIS+ должны работать на уровне защиты 2.	**Расположение** `/etc/security/pscexpert/dodv2/nisplus` **Действие, обеспечивающее соответствие** Гарантирует, что сервер работает на указанном минимальном уровне защиты. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006480	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.
GEN006560	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.
GEN006580	2	Система должна использовать программу контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/checktcpd` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN006600	2	Системная программа контроля доступа должна вести протокол всех попыток доступа к системе.	**Расположение** `/etc/security/pscexpert/dodv2/chsyslogdod` **Действие, обеспечивающее соответствие** Гарантирует ведение протокола доступа.
GEN006620	2	Системная программа контроля доступа должна быть настроена для разрешения или запрещения доступа системы к определенным хостам.	**Расположение** `/etc/security/pscexpert/dodv2/chetchostsdod` **Действие, обеспечивающее соответствие** Указывает требуемые значения в файлах `hosts.deny` и `hosts.allow`.
GEN007020	2	Протокол SCTP (протокол передачи с управлением потоком) должен быть выключен.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2netrules` **Действие, обеспечивающее соответствие** Выключает указанный протокол.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN007700	2	Обработчик протокола IPv6 не должен быть подключен к сетевому стеку без необходимости.	**Расположение** `/etc/security/pscexpert/dodv2/rminet6` **Действие, обеспечивающее соответствие** Отключает обработчик протокола IPv6 от сетевого стека, если обработчик не указан в файле `/etc/ipv6.conf`. **Примечание:** Если система использует протокол IPv6, параметр *ipv6_enabled* в файле `/etc/security/pscexpert/ipv6.conf` должен иметь значение `yes`. Если система не использует IPv6, то параметр *ipv6_enabled* должен быть `no`.
GEN007780	2	В системе должны быть выключены туннели `6to4`.	**Расположение** `/etc/security/pscexpert/dodv2/rmiface` **Действие, обеспечивающее соответствие** Выключает указанные туннели. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN007820	2	В системе не должно быть настроенных IP-туннелей.	**Расположение** `/etc/security/pscexpert/dodv2/rmtunnel` **Действие, обеспечивающее соответствие** Выключает IP-туннели. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN007840	2	Клиент `DHCP` должен быть выключен, если не используется.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN007850	2	Клиент `DHCP` не должен отправлять динамические обновления DNS.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2services` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN007860	2	Система должна игнорировать сообщения перенаправления ICMP IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipignoreredirects` значение *1*.
GEN007880	2	Система не должна отправлять перенаправления ICMP IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipsendredirects` значение *0*.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN007900	2	Система должна использовать соответствующий фильтр обратного пути для сетевого потока данных IPv6, если система использует IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN007920	2	Система не должна пересылать пакеты с фиксированным маршрутом IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ip6srcrouteforward` значение *0*.
GEN007940: GEN003607	2	Система не должна принимать пакеты IPv4 или IPv6 с фиксированным маршрутом.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `ipsrcrouterecv` значение *0*.
GEN007950	2	Система не должна отвечать на эхо-запросы ICMPv6, отправленные с широковещательного адреса.	**Расположение** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Действие, обеспечивающее соответствие** Присваивает параметру сети `bcastping` значение *0*.
GEN008000	2	Если в системе используется LDAP для идентификации или хранения информации учетных записей, то сертификаты, используемые для идентификации на сервере LDAP, должны браться из PKI Министерства обороны США или должны быть получены другим одобренным Министерством обороны США способом.	**Расположение** `/etc/security/pscexpert/dodv2/ldap_config` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN008020	2	Если в системе используется LDAP для идентификации или хранения информации учетных записей, то соединение TLS с LDAP должно требовать от сервера сертификат с действительной цепочкой доверия.	**Расположение** `/etc/security/pscexpert/dodv2/ldap_config` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN008050	2	Если система использует LDAP для идентификации или хранения информации учетных записей, то файл `/etc/ldap.conf` (или эквивалентный) не должен содержать паролей.	**Расположение** `/etc/security/pscexpert/dodv2/ldap_config` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN008380	2	Система должна еженедельно проверяться на наличие несанкционированных файлов `setuid` и несанкционированных изменений санкционированных файлов `setuid`.	**Расположение** `/etc/security/pscexpert/dodv2/trust` **Действие, обеспечивающее соответствие** Выполняет еженедельную проверку на предмет изменений в указанных файлах.
GEN008520	2	Система должна использовать локальный брандмауэр, защищающий хост от сканирования портов. Брандмауэр закрывает уязвимые порты на 5 минут для защиты от сканирования портов.	**Расположение** `/etc/security/pscexpert/dodv2/ipsecshunports` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям.
GEN008540	2	В локальном брандмауэре системы должна быть реализована стратегия *deny-all*, *allow-by-exception*.	**Расположение** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Действие, обеспечивающее соответствие** Гарантирует, что система соответствует указанным требованиям. **Примечание:** Можно добавить дополнительные правила фильтрации в файл `/etc/security/aixpert/bin/filter.txt`. Эти правила интегрируются сценарием `ipsecshunhosthls.sh` во время применения профайла. Записи должны быть в следующем формате: *номер-порта*`:`*IP-адрес*`:` *действие* где допустимые значения *действия* - `Allow` или `Deny`.
GEN008600	1	Система должна быть настроена для запуска только из конфигурации загрузки системы.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cat1` **Действие, обеспечивающее соответствие** Гарантирует, что для запуска системы используется только конфигурация загрузки системы.
GEN008640	1	Система не должна использовать съемные носители данных в качестве загрузочных.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cat1` **Действие, обеспечивающее соответствие** Гарантирует, что система не загружается со съемного носителя данных.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN009140	1,2,3	В системе не должно быть активной службы `chargen`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009160	1,2,3	В системе не должно быть активной службы `Демон службы управления календарем` (CMSD).	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009180	1,2,3	В системе не должно быть активной службы `Сервер базы данных ToolTalk` (ttdbserver).	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009190	1,2,3	В системе не должно быть активной службы `comsat`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009200-9330	1,2,3	В системе не должно быть других активных служб и демонов.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009210	2	В системе не должно быть активной службы `discard`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009220	2	В системе не должно быть активной службы `dtspc`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009230	2	В системе не должно быть активной службы `echo`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN009240	2	В системе не должно быть активной службы `Протокол доступа к сообщениям Интернета (IMAP)`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009250	2	В системе не должно быть активной службы `Почтовый протокол (POP3)`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009260	2	В системе не должно быть активных служб talk и `ntalk`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009270	2	В системе не должно быть активной службы `netstat` в процессе inetd.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009280	2	В системе не должно быть активной службы `PCNFS`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009290	2	В системе не должно быть активной службы `systat`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009300	2	Служба `inetd time` должна быть выключена в системном демоне `inetd`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009310	2	В системе не должно быть активной службы `rusersd`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.

Таблица 2. Общие требования Министерства обороны США (продолжение)

ИД контрольной точки STIG Министерства обороны	Категория правил STIG	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN009320	2	В системе не должно быть активной службы `sprayd`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009330	2	В системе не должно быть активной службы `rstatd`.	**Расположение** `/etc/security/pscexpert/dodv2/inetdservices` **Действие, обеспечивающее соответствие** Выключает требуемые демоны и службы путем добавления символов комментария в соответствующие записи файла `/etc/inetd.conf`.
GEN009340	2	Администраторы входа XServer не должны выполняться, если они не нужны для управления сеансами X11.	**Расположение** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Действие, обеспечивающее соответствие** Это правило выключает соединения X Window System и администратор входа XServer.

Таблица 3. Требования Министерства обороны США к владению файлами

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00085	Файлом `/etc/netsvc.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
AIX00090	Файлом `/etc/netsvc.conf` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
AIX00320	Файлом `/etc/ftpaccess.ctl` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
AIX00330	Файлом `/etc/ftpaccess.ctl` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000250	Файлом конфигурации синхронизации времени, например `/etc/ntp.conf`, должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN000251	Файлом конфигурации синхронизации времени, например `/etc/ntp.conf`, должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN001160	Все файлы и каталоги должны иметь правильных владельцев.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что все файлы и каталоги имеют правильного владельца.
GEN001170	Все файлы и каталоги должны иметь правильную группу-владельца.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что все файлы и каталоги имеют правильного владельца.
GEN001220	Все системные файлы, программы и каталоги должны принадлежать системной учетной записи.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что системные файлы, программы и каталоги принадлежат системной учетной записи.
GEN001240	Системные файлы, программы и каталоги должны принадлежать системной группе.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Все системные файлы, программы и каталоги должны принадлежать системной группе.
GEN001320	Файлами NIS/NIS+/yp должен владеть пользователь root, sys или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь root, sys или bin.
GEN001340	Файлами NIS/NIS+/yp должна владеть группа sys, bin, other или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа sys, bin, other или system.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001362	Файлом `/etc/resolv.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001363	Файлом `/etc/resolv.conf` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN001366	Файлом `/etc/hosts` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001367	Файлом `/etc/hosts` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN001371	Файлом `/etc/nsswitch.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001372	Файлом `/etc/nsswitch.conf` должна владеть группа root, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа root, bin, sys или system.
GEN001378	Файлом `/etc/passwd` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001379	Файлом `/etc/passwd` должна владеть группа bin, security, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, security, sys или system.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001391	Файлом `/etc/group` должен владеть пользователь root	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001392	Файлом `/etc/group` должна владеть группа bin, security, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, security, sys или system.
GEN001400	Файлом `/etc/security/passwd` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN001410	Файлом `/etc/security/passwd` должна владеть группа bin, security, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, security, sys или system.
GEN001500	Владельцами домашних каталогов всех интерактивных пользователей должны быть соответствующие пользователи.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что владельцами домашних каталогов всех интерактивных пользователей являются соответствующие пользователи.
GEN001520	Домашние каталоги всех интерактивных пользователей должны принадлежать основной группе владельца домашнего каталога.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что домашние каталоги всех интерактивных пользователей принадлежат основной группе владельца домашнего каталога.
GEN001540	Владельцем всех файлов и каталогов в домашних каталогах интерактивных пользователей должен быть владелец домашнего каталога.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что владельцем всех файлов и каталогов в домашних каталогах интерактивных пользователей является владелец домашнего каталога.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001550	Все файлы и каталоги в домашних каталогах пользователей должны принадлежать группе, членом которой является владелец домашнего каталога.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что все файлы и каталоги в домашних каталогах пользователей принадлежат группе, членом которой является владелец домашнего каталога.
GEN001660	Всеми файлами запуска системы должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь root.
GEN001680	Всеми файлами запуска системы должна владеть группа sys, bin, other или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа sys, bin, other или system.
GEN001740	Всеми глобальными файлами инициализации должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь root.
GEN001760	Всеми глобальными файлами инициализации должна владеть группа sys, bin, system или security.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа sys, bin, system или security.
GEN001820	Всеми файлами и каталогами - заготовками (обычно находятся в каталоге `/etc/skel`) должен владеть пользователь root или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами и каталогами владеет пользователь root или bin.
GEN001830	Всеми файлами-заготовками (обычно находятся в каталоге `/etc/skel`) должна владеть группа security.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа security.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001860	Всеми локальными файлами инициализации должен владеть пользователь user или root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь user или root.
GEN001870	Локальными файлами инициализации должна владеть основная группа пользователя user или группа root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что локальными файлами инициализации должна владеть основная группа пользователя user или группа root.

GEN002060	Все файлы `.rhosts`, `.shosts`, `.netrc` и `hosts.equiv` должны быть доступны только пользователю root или владельцу.	**Расположение**
		`/etc/security/pscexpert/dodv2/chowndodfiles`
		`/etc/security/pscexpert/dodv2/fpmdodfiles`
		Действие, обеспечивающее соответствие
		Гарантирует, что только пользователь root или владелец имеет доступ к указанным файлам.

GEN002100	Файл `.rhosts` не должен поддерживаться PAM (подключаемые модули идентификации).	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанный файл недоступен при использовании PAM.
GEN002200	Всеми файлами оболочек должен владеть пользователь root или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь root или bin.
GEN002210	Всеми файлами оболочек должна владеть группа root, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа root, bin, sys или system.
GEN002340	Звуковыми устройствами должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что всеми звуковыми устройствами владеет пользователь root.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN002360	Всеми звуковыми устройствами должна владеть группа root, sys, bin или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что всеми звуковыми устройствами владеет группа root, sys, bin или system.
GEN002520	Всеми общедоступными каталогами должен владеть пользователь root или учетная запись приложения.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что всеми общедоступными каталогами владеет пользователь root или учетная запись приложения.
GEN002540	Всеми общедоступными каталогами должна владеть группа system или группа приложения.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что всеми общедоступными каталогами владеет группа system или группа приложения.
GEN002680	Протоколами системного контроля должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет пользователь root.
GEN002690	Протоколами системного контроля должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа bin, sys или system.
GEN003020	Утилита `cron` не должна запускать программы, находящиеся в каталогах, доступных на запись всем пользователям, или в их подкаталогах.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Запрещает утилите `cron` запускать программы из каталогов, доступных на запись всем пользователям, и их подкаталогов.
GEN003040	Файлом `crontabs` должен владеть пользователь root или пользователь, создавший файл crontab.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл crontabs принадлежит пользователю root или пользователю, создавшему файл crontab.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003050	Файлами `crontab` должна владеть группа system, cron или основная группа пользователя, создавшего файл crontab.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы `crontab` принадлежат группе system, cron или основной группе пользователя, создавшего файл crontab.
GEN003110	Каталоги `cron` и `crontab` не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные каталоги не имеют расширенных списков контроля доступа.
GEN003120	Каталогами `cron` и `crontab` должен владеть пользователь root или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что каталоги cron и crontab принадлежат пользователю root или bin.
GEN003140	Каталогами `cron` и `crontab` должна владеть группа system, sys, bin или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные каталоги принадлежат группе system, sys, bin или cron.
GEN003160	Должно быть реализовано ведение протокола для cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что реализовано ведение протокола для cron.
GEN003240	Файлом `cron.allow` должен владеть пользователь root, bin или sys.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root, bin или sys.
GEN003250	Файлом `cron.allow` должна владеть группа system, bin, sys или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа system, bin, sys или cron.
GEN003260	Файлом `cron.deny` должен владеть пользователь root, bin или sys.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root, bin или sys.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003270	Файлом `cron.deny` должна владеть группа system, bin, sys или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа system, bin, sys или cron.
GEN003420	Каталогом `at` должен владеть пользователь root, bin, sys, daemon или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным каталогом владеет пользователь root, sys, daemon или cron.
GEN003430	Каталогом `at` должна владеть группа system, bin, sys или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным каталогом владеет группа system, bin, sys или cron.
GEN003460	Файлом `at.allow` должен владеть пользователь root, bin или sys.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root, bin или sys.
GEN003470	Файлом `at.allow` должна владеть группа system, bin, sys или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа system, bin, sys или cron.
GEN003480	Файлом `at.deny` должен владеть пользователь root, bin или sys.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root, bin или sys.
GEN003490	Файлом `at.deny` должна владеть группа system, bin, sys или cron.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа system, bin, sys или cron.
GEN003720	Файлом `inetd.conf`, файлом `xinetd.conf` и каталогом `xinetd.d` должен владеть пользователь root или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами и каталогом владеет пользователь root или bin.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003730	Файлом `inetd.conf`, файлом `xinetd.conf` и каталогом `xinetd.d` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами и каталогом владеет группа bin, sys или system.
GEN003760	Файлом `services` должен владеть пользователь root или bin.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root или bin.
GEN003770	Файлом `services` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN003920	Файлом `hosts.lpd` (или эквивалентным) должен владеть пользователь root, bin, sys или lp.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root, bin, sys или lp.
GEN003930	Файлом `hosts.lpd` (или эквивалентным) должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN003960	Командой **traceroute** должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что владелец команды - пользователь root.
GEN003980	Команда **traceroute** должна принадлежать группе sys, bin или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что командой владеет группа sys, bin или system.
GEN004360	Файлом `alias` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN004370	Файл `aliases` должен принадлежать группе sys, bin или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа sys, bin или system.
GEN004400	Файлы, выполняемые через почтовый файл `aliases`, должны принадлежать пользователю root и находиться в каталоге, которым владеет пользователь root и доступ на запись к которому есть только у пользователя root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы, выполняемые через почтовый файл `aliases`, принадлежат пользователю root и находятся в каталоге, которым владеет пользователь root и доступ на запись к которому есть только у пользователя root.
GEN004410	Файлами, выполняемыми через почтовый файл `aliases`, должна владеть группа root, bin, sys или other. Они также должны быть в каталоге, принадлежащем группе root, bin, sys или other.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлами, выполняемыми через почтовый файл `aliases`, владеет группа root, bin, sys или other. И находятся в каталоге, принадлежащем группе root, bin, sys или other.
GEN004480	Файлом протокола службы SMTP должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN004920	Файлом `ftpusers` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN004930	Файлом `ftpusers` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN005360	Файлом `snmpd.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005365	Файлом `snmpd.conf` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN005400	Файлом `/etc/syslog.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN005420	Файлом `/etc/syslog.conf` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN005610	В системе должна быть выключена пересылка пакетов IP для IPv6, если система не является маршрутизатором IPv6.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что пересылка пакетов IP для IPv6 выключена, если система не используется в качестве маршрутизатора IPv6.
GEN005740	Файлом конфигурации экспорта NFS должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN005750	Файлом конфигурации экспорта NFS должна владеть группа root, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа root, bin, sys или system.
GEN005800	Всеми системными файлами и каталогами, экспортируемыми NFS, должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005810	Всеми системными файлами и каталогами, экспортируемыми NFS, должна владеть группа root, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами и каталогами владеет группа root, bin, sys или system.
GEN006100	Файлом `/usr/lib/smb.conf` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN006120	Файлом `/usr/lib/smb.conf` должна владеть группа bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN006160	Файлом `/var/private/smbpasswd` должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN006180	Файлом `/var/private/smbpasswd` должна владеть группа sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа sys или system.
GEN006340	Файлами в каталоге `/etc/news` должен владеть пользователь root или news.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным каталогом владеет пользователь root или news.
GEN006360	Файлами в каталоге `/etc/news` должна владеть группа system или news.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанными файлами владеет группа system или news.
GEN008080	Если система использует LDAP для идентификации или хранения информации учетных записей, то файлом `/etc/ldap.conf` (или эквивалентным) должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.

Таблица 3. Требования Министерства обороны США к владению файлами (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN008100	Если система использует LDAP для идентификации или хранения информации учетных записей, то файлом `/etc/ldap.conf` (или эквивалентным) должна владеть группа security, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.
GEN008140	Если система использует LDAP для идентификации или хранения информации учетных записей, то файлом или каталогом центра сертификации для TLS должен владеть пользователь root.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет пользователь root.
GEN008160	Если система использует LDAP для идентификации или хранения информации учетных записей, то файлом или каталогом центра сертификации для TLS должна владеть группа root, bin, sys или system.	**Расположение** `/etc/security/pscexpert/dodv2/chowndodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанным файлом владеет группа bin, sys или system.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00100	Файл `/etc/netsvc.conf` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
AIX00340	Файл `/etc/ftpaccess.ctl` должен иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN000252	Файл конфигурации синхронизации времени, например `/etc/ntp.conf`, должен иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN000920	Домашний каталог учетной записи пользователя root (не /) должен иметь режим доступа 0700.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что каталог имеет указанный режим доступа или более ограничивающий.
GEN001140	Системные файлы и каталоги должны иметь равномерные права доступа.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует целостность прав доступа.
GEN001180	Все файлы демона сетевых служб должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001200	Все файлы системных команд должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001260	Файлы системных протоколов должны иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001280	Файлы справки должны иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001300	Файлы библиотек должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001360	Файлы NIS/NIS+/yp должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001364	Файл `/etc/resolv.conf` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001368	Файл `/etc/hosts` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001373	Файл `/etc/nsswitch.conf` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001380	Файл `/etc/passwd` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001393	Файл `/etc/group` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001420	Файл `/etc/security/passwd` должен иметь режим доступа 0400.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001480	Все домашние каталоги пользователей должны иметь режим доступа 0750 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN001560	Все файлы и каталоги, содержащиеся в домашних каталогах пользователей, должны иметь режим доступа 0750 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001580	Все сценарии управления выполнением должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001640	Сценарии управления выполнением не должны запускать программы и сценарии, доступные на запись всем пользователям.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Проверяет программы, такие как `cron`, на наличие программ и сценариев, доступных на запись всем пользователям.
GEN001720	Все глобальные файлы инициализации должны иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001800	Все файлы-заготовки, например файлы в каталоге `/etc/skel`, должны иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN001880	Все локальные файлы инициализации должны иметь режим доступа 0740 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	**Описание**	**Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям**
GEN002220	Все файлы оболочек должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN002320	Звуковые устройства должны иметь режим доступа 0660 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что звуковые устройства имеют указанный режим доступа или более ограничивающий.
GEN002560	Системное и пользовательское значение **umask** по умолчанию должно быть 077.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные параметры имеют значение *077*.
GEN002700	Файлы протокола системного контроля должны иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN002717	Исполняемые файлы инструментов системного контроля должны иметь режим доступа 0750 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN002980	Файл `cron.allow` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003080	Файлы crontab должны иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003090	Файлы `crontab` не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные файлы не имеют расширенных списков контроля доступа.
GEN003100	Каталоги cron и crontab должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные каталоги имеют указанный режим доступа или более ограничивающий.
GEN003180	Файл `cronlog` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003200	Файл `cron.deny` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003252	Файл `at.deny` должен иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003340	Файл `at.allow` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003400	Каталог `at` должен иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что каталог имеет указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003440	У заданий `at` значение параметра **`umask`** должно быть 077 или более ограничивающим.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что параметр имеет указанный режим доступа или более ограничивающий.
GEN003740	Файлы `inetd.conf` и `xinetd.conf` должны иметь режим доступа 0440 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN003780	Файл `services` должен иметь режим доступа 0444 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN003940	Файл `hosts.lpd` (или эквивалентный) должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN004000	Файл `traceroute` должен иметь режим доступа 0700 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN004380	Файл `alias` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN004420	Файлы, которые выполняются через почтовый файл `aliases`, должны иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fmpdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN004500	Файл протокола службы SMTP должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN004940	Файл `ftpusers` должен иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN005040	У всех пользователей FTP должно быть задано значение **umask** по умолчанию 077.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует правильное значение параметра.
GEN005100	Демон `TFTP` должен иметь режим доступа 0755 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что демон имеет указанный режим доступа или более ограничивающий.
GEN005180	Все файлы `.Xauthority` должны иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN005320	Файл `snmpd.conf` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN005340	Файлы Базы информации управления (MIB) должны иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005390	Файл `/etc/syslog.conf` должен иметь режим доступа 0640 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN005522	Файлы открытых ключей хоста SSH должны иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN005523	Файлы личных ключей хоста SSH должны иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файлы имеют указанный режим доступа или более ограничивающий.
GEN006140	Файл `/usr/lib/smb.conf` должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN006200	Файл `/var/private/smbpasswd` должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN006260	Файл `/etc/news/hosts.nntp` (или эквивалентный) должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN006280	Файл `/etc/news/hosts.nntp.nolimit` (или эквивалентный) должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.

Таблица 4. Стандарты Министерства обороны США для прав доступа к файлам (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN006300	Файл `/etc/news/nnrp.access` (или эквивалентный) должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN006320	Файл `/etc/news/passwd.nntp` (или эквивалентный) должен иметь режим доступа 0600 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN008060	Если система использует LDAP для идентификации или хранения информации учетных записей, то файл `/etc/ldap.conf` (или эквивалентный) должен иметь режим доступа 0644 или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что файл имеет указанный режим доступа или более ограничивающий.
GEN008180	Если система использует LDAP для идентификации или хранения информации учетных записей, то файл и (или) каталог центра сертификации для TLS должны иметь режим доступа 0644 (0755 для каталогов) или более ограничивающий.	**Расположение** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанный файл и (или) каталоги имеют указанный режим доступа или более ограничивающий.

Таблица 5. Требования Министерства обороны США к списку контроля доступа

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00110	Файл `/etc/netsvc.conf` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
AIX00350	Файл `/etc/ftpaccess.ctl` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000253	Файл конфигурации синхронизации времени, например `/etc/ntp.conf`, не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN000930	Домашний каталог пользователя root не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001190	Все файлы демона сетевых служб не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001210	Все файлы системных команд не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001270	Файлы системных протоколов не должны иметь расширенных списков контроля доступа, за исключением случаев, когда это необходимо для поддержки санкционированного программного обеспечения.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001310	Все файлы библиотек не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001361	Все файлы команд NIS/NIS+/yp не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001365	Файл `/etc/resolv.conf` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001369	Файл `/etc/hosts` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001374	Файл `/etc/nsswitch.conf` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001390	Файл `/etc/passwd` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001394	Файл `/etc/group` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001430	Файл `/etc/security/passwd` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001570	Все файлы и каталоги, содержащиеся в домашних каталогах пользователей, не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001590	Все сценарии управления выполнением не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN001730	Все глобальные файлы инициализации не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001810	Все файлы-заготовки не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN001890	Локальные файлы инициализации не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN002230	Все файлы оболочек не должны иметь расширенных списков контроля доступа	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN002330	Звуковые устройства не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN002710	Все файлы системного контроля не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN002990	Расширенные списки контроля доступа должны быть выключены для файлов `cron.allow` и `cron.deny`.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003090	Файлы crontab не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003110	Каталоги cron и crontab не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003190	Файлы протокола cron не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003210	Файл `cron.deny` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003245	Файл `at.allow` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003255	Файл `at.deny` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003410	Каталог `at` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003745	Файлы `inetd.conf` и `xinetd.conf` не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN003790	Файл служб не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN003950	Файл `hosts.lpd` (или эквивалентный) не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004010	Файл `traceroute` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004390	Файл `alias` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004430	Файлы, выполняющиеся через почтовый файл `aliases`, не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN004510	Файл протокола службы SMTP не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN004950	Файл `ftpusers` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN005190	Файлы `.Xauthority` не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN005350	Файлы Базы информации управления (MIB) не должны иметь расширенных списков контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN005375	Файл `snmpd.conf` не должен иметь расширенного списка контроля доступа	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN005395	Файл `/etc/syslog.conf` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006150	Файл `/usr/lib/smb.conf` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006210	Файл `/var/private/smbpasswd` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN006270	Файл `/etc/news/hosts.nntp` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006290	Файл `/etc/news/hosts.nntp.nolimit` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006310	Файл `/etc/news/nnrp.access` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN006330	Файл `/etc/news/passwd.nntp` не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Выключает указанный расширенный список контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Таблица 5. Требования Министерства обороны США к списку контроля доступа (продолжение)

ИД контрольной точки STIG Министерства обороны	Описание	Расположение сценария, где определено действие, и результаты действия, обеспечивающего соответствие требованиям
GEN008120	Если система использует LDAP для идентификации или хранения информации учетных записей, то файл `/etc/ldap.conf` (или эквивалентный) не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанные файлы не имеют расширенного списка контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.
GEN008200	Если система использует LDAP для идентификации или хранения информации учетных записей, то файл или каталог центра сертификации для TLS не должен иметь расширенного списка контроля доступа.	**Расположение** `/etc/security/pscexpert/dodv2/acldodfiles` **Действие, обеспечивающее соответствие** Гарантирует, что указанный каталог или файл не имеет расширенного списка контроля доступа. **Примечание:** Этот параметр автоматически не изменяется при восстановлении стратегии AIX по умолчанию с помощью файла `DoDv2_to_AIXDefault.xml`. Этот параметр необходимо изменить вручную.

Информация, связанная с данной:

Министерство обороны - соответствие STIG

Отрасль платежных карт - соответствие стандартам защиты данных

Стандарт защиты данных в сфере платежных карт (PCI - DSS) определяет категории защиты ИТ по 12 разделам, называемым 12 требованиями и процедурами оценки защиты.

12 требований и процедур оценки защиты ИТ-систем, определяемые PCI - DSS, содержат следующие элементы:

Требование 1: устанавливать и обслуживать конфигурацию брандмауэра для защиты данных владельца кредитной карточки.

Задокументированный список служб и портов, необходимых для бизнеса. Это требование реализуется путем отключения необязательных и незащищенных служб.

Требование 2: не использовать в качестве системных паролей и других параметров защиты значения, предоставленные поставщиком.

Всегда следует изменять предоставленные поставщиком значения по умолчанию перед установкой системы в сети. Этот требование реализуется путем отключения демона SNMP.

Требование 3: защищать сохраненные данные владельца кредитной карточки.

Это требование реализуется путем включения компонента EFS, предоставляемого операционной системой AIX.

Требование 4: зашифровать данные владельца кредитной карточки при передаче данных в открытых общедоступных сетях.

Это требование реализуется путем включения компонента IPSEC, предоставляемого операционной системой AIX.

Требование 5: использовать и регулярно обновлять антивирусное программное обеспечение.

Это требование реализуется путем использования программы стратегии защищенного выполнения. Защищенное выполнение - это рекомендованное антивирусное ПО, встроенное в операционную систему AIX. Для PCI требуется записывать протоколы программы защищенного выполнения путем включения управления событиями и сведениями о защите (SIEM) для отслеживания предупреждений. Программа защищенного выполнения, запущенная в режиме только для ведения протокола, не прекращает проверки при возникновении ошибки, вызванной несоответствием хеша.

Требование 6: разрабатывать и обслуживать защищенные системы и приложения.

Для реализации этого требования необходимо вручную установить требуемые исправления в систему. После приобретения PowerSC Standard Edition можно использовать компонент TNC.

Требование 7: ограничивать доступ к данным владельца кредитной карточки до известных бизнес-потребностей.

Можно реализовать жесткие меры по контролю за доступом, используя компонент RBAC для включения правил и ролей. RBAC не может работать в автоматическом режиме, так как для его активации требуется ввод администратора.

`RbacEnablement` проверяет систему для определения, существуют ли в системе свойства isso, so и sa для ролей. Если эти свойства не существуют, то сценарий их создает. Этот сценарий запускается также в составе проверок pscexpert в виде команды `pscxpert -c`.

Требование 8: присваивать уникальный ИД каждому пользователю, имеющему доступ к компьютеру.

Это требование реализуется путем включения профайлов PCI. К профайлу PCI применимы следующие правила:

- Изменение пользовательских паролей, по крайней мере, каждые 90 дней.
- Требование минимальной длины пароля в 7 символов.
- Использование пароля, содержащего и цифры, и буквенные символы.
- Запрет на использование пароля, совпадающего с предыдущими четырьмя паролями.
- Ограничение на число попыток доступа с последующей блокировкой ИД пользователя после шести неудачных попыток.
- Определение продолжительности блокировки, равной 30 минутам, либо до разблокировки ИД пользователя администратором.
- Требование повторного ввода пароля для повторной активации терминала после простоя в течение 15 минут или больше.

Требование 9: ограничить доступ к данным владельца кредитной карточки.

Для создания хранилищ конфиденциальных данных владельца кредитной карточки следует применять комнаты с ограниченным доступом.

Требование 10: отслеживать весь доступ к сетевым ресурсам и к данным владельца кредитной карточки.

Это требование реализуется включением автоматического протоколирования системных компонентов и ведения протоколов доступа к ним.

Требование 11: регулярно тестировать процессы и системы защиты.

Требование реализуется с помощью функции соответствия требованиям реального времени.

Требование 12: поддерживать стратегию защиты, включающую информационную безопасность для сотрудников и подрядчиков.

Активация модемов для производителей только при необходимости и немедленная деактивация модемов после использования. Это требование реализуется путем отключения удаленного входа в систему с правами пользователя root, активации администратором системы при необходимости и последующей деактивации при ее отсутствии.

PowerSC Standard Edition упрощает управление конфигурацией, требуемое для исполнения инструкций, определенных в PCI DSS версии 2.0 и PCI DSS версии 3.0. Однако полностью процесс автоматизировать нельзя.

Например, ограничение доступа к данным владельца кредитной карточки на основе бизнес-требований не может быть выполнено автоматически. Операционная система AIX предоставляет технологии надежной защиты, такие как ролевой контроль доступа (RBAC), однако, PowerSC Standard Edition не может автоматизировать эту конфигурацию, так как не может определить пользователей, которым требуется доступ, и пользователей, которым доступ не требуется. IBM Compliance Expert может автоматизировать конфигурацию других параметров защиты, соответствующих требованиям PCI.

Если профайл PCI применен к среде базы данных, то некоторые порты TCP и UDP, используемые программным стеком, будут отключены из-за ограничений. Для запуска приложения и рабочей нагрузки необходимо разрешить использование этих портов и отключить функцию защищенного выполнения. Для снятия ограничений портов и отключения функции защищенного выполнения выполните следующие команды:

```
trustchk -p TE=OFF
tcptr -delete 9091 65535
tcptr -delete 9090 9090
tcptr -delete 112 9089
tcptr -add 9091 65535 1024 1
```

Примечание: Все пользовательские файлы сценариев, предоставляемые для поддержки соответствия требованиям PCI - DSS, расположены в каталоге `/etc/security/pscexpert/bin`.

В следующей таблице показано, каким образом PowerSC Standard Edition соотносится с требованиями стандарта PCI DSS с помощью функций инструмента AIX Security Expert:

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
2.1	Всегда изменять поставляемые производителем значения по умолчанию перед установкой системы сети. Например, включать пароли, строки сообщества SNMP и отключать лишние учетные записи.	Задает минимальное число недель до возможности сменить пароль равным 0, присвоив параметру **minage** значение 0.	`/etc/security/pscexpert/bin/chusrattr`
PCI версии 2 8.5.9 **PCI версии 3** 8.2.4	Изменение пользовательских паролей, по крайней мере, каждые 90 дней.	Задает максимальное число недель допустимости пароля, равное 13 неделям, присвоив параметру **maxage** значение 13.	`/etc/security/pscexpert/bin/chusrattr`
2.1	Всегда изменять поставляемые производителем значения по умолчанию перед установкой системы сети. Например, включать пароли, строки сообщества SNMP и отключать лишние учетные записи.	Задает число недель, в течение которых учетная запись с устаревшим паролем сохраняется в системе, равным 8 неделям, присвоив параметру **maxexpired** значение 8.	`/etc/security/pscexpert/bin/chusrattr`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 8.5.10 **PCI версии 3** 8.2.3	Требование минимальной длины пароля в 7 символов.	Задает минимальную длину пароля равной 7 символам, присвоив параметру **minlen** значение 7.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.11 **PCI версии 3** 8.2.3	Использовать пароли, содержащие и цифровые, и буквенные символы.	Задает минимальное число буквенных символов в пароле равным 1. Это значение обеспечивает содержание в пароле буквенных символов за счет присвоения параметру **minalpha** значения 1.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.11 **PCI версии 3** 8.2.3	Использовать пароли, содержащие и цифровые, и буквенные символы.	Задает минимальное число небуквенных символов в пароле равным 1. Это значение гарантирует, что пароль содержит небуквенные символы, при присвоении параметру **minother** значения 1.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 2.1 **PCI версии 3** 8.2.2	Всегда изменять поставляемые производителем значения по умолчанию перед установкой системы сети. Например, включать пароли, строки сообщества SNMP и отключать лишние учетные записи.	Задает максимальное число повторов символа в пароле равным 8, присваивая параметру **maxrepeats** значения 8. Этот параметр означает, что символ в пароле может быть повторен неограниченное число раз, если это удовлетворяет другим ограничениям создания пароля.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.12 **PCI версии 3** 8.2.5	Запрет на использование пароля, совпадающего с предыдущими четырьмя паролями.	Задает число недель, после которого можно повторно использовать пароль, равным 52, путем присваивания параметру **histexpire** значения 52.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.12 **PCI версии 3** 8.2.5	Запрет на использование пароля, совпадающего с предыдущими четырьмя паролями.	Задает число предыдущих паролей, которые нельзя повторно использовать, равным 4, путем присвоения параметру **histsize** значения 4.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.13 **PCI версии 3** 8.1.6	Ограничение на число попыток доступа с последующей блокировкой ИД пользователя после шести неудачных попыток.	Задает число последовательных неудачных попыток входа в систему с последующим отключением учетной записи равным 6 для каждой учетной записи, отличной от root, путем присвоения параметру **loginentries** значения 6.	/etc/security/pscexpert/bin/chusrattr
PCI версии 2 8.5.13 **PCI версии 3** 8.1.6	Ограничение на число попыток доступа с последующей блокировкой ИД пользователя после шести неудачных попыток.	Задает число последовательных неудачных попыток входа в систему с последующим отключением порта равным 6 путем присвоения параметру **logindisable** значения 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 8.5.14 **PCI версии 3** 8.1.7	Определение продолжительности блокировки, равной 30 минутам, либо до разблокировки ИД пользователя администратором.	Задает продолжительность блокировки порта после отключения атрибутом *logindisable* равным 30 минутам, присвоив параметру **loginreenable** значения 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Активация технологий удаленного доступа для производителей и бизнес-партнеров только при необходимости с немедленным отключением после использования.	Отключает функцию удаленного доступа с правами пользователя root путем присвоения этому параметру значения false. Администратор системы может активировать эту функцию при необходимости, а затем деактивировать ее после выполнения задачи.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	Присвоение всем пользователям уникальных ИД перед предоставлением им доступа к системным компонентам или данным владельца кредитной карточки.	Включает функцию, гарантирующую для каждого пользователя уникальное имя пользователя перед его доступом к системным компонентам или данным владельца кредитной карточки, путем присвоения этой функции значения true.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Включить контроль системы.	Включает контроль двоичных файлов в системе.	/etc/security/pscexpert/bin/pciaudit
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая общую среду рабочего стола (CDE).	Отключает функцию CDE, если не настроен traceroute уровня 4 (LFT).	/etc/security/pscexpert/bin/comntrows
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон timed.	Завершает работу демона timed и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон rwhod.	Завершает работу демона rwhod и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 2.1 **PCI версии 3** 2.1.1	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая завершение работы демона SNMP.	Завершает работу демона SNMP и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 2.1 **PCI версии 3** 2.1.1	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая завершение работы демона SNMPMIBD.	Завершает работу демона SNMPMIBD и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
2.1	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая завершение работы демона AIXMIBD.	Завершает работу демона AIXMIBD и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
2.1	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая завершение работы демона HOSTMIBD.	Завершает работу демона HOSTMIBD и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон DPID2.	Завершает работу демона DPID2 и помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую демон.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 2.1 **PCI версии 3** 2.2.2	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая завершение работы сервера DHCP.	Завершает работу сервера DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая агент DHCP.	Останавливает и отключает промежуточный агент DHCP, а также помечает символом комментария соответствующую запись в файле /etc/rc.tcpip, автоматически запускающую агент.	/etc/security/pscexpert/bin/rctcpip
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон rshd.	Останавливает и отключает все экземпляры демона rshd и службы оболочки, а также помечает символом комментария соответствующие записи в файле /etc/inetd.conf, автоматически запускающие экземпляры.	/etc/security/pscexpert/bin/cominetdconf

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rlogind`.	Останавливает и отключает все экземпляры демона `rlogind` и службы rlogin. Также утилита AIX Security Expert помечает символом комментария соответствующие записи в файле `/etc/inetd.conf`, автоматически запускающие экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rexecd`.	Останавливает и отключает все экземпляры демона `rexecd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `comsat`.	Останавливает и отключает все экземпляры демона `comsat`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `fingerd`.	Останавливает и отключает все экземпляры демона `fingerd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `systat`.	Останавливает и отключает все экземпляры демона `systat`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
2.1	Изменить указанные производителем значения по умолчанию перед установкой системы в сети, включая отключение команды `netstat`.	Отключает команду `netstat` и помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`.	`/etc/security/pscexpert/bin/cominetdconf`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.3	Отключить ненужные и незащищенные службы, включая демон `tftp`.	Останавливает и отключает все экземпляры демона `tftp`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `talkd`.	Останавливает и отключает все экземпляры демона `talkd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rquotad`.	Останавливает и отключает все экземпляры демона `rquotad`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rstatd`.	Останавливает и отключает все экземпляры демона `rstatd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rusersd`.	Останавливает и отключает все экземпляры демона `rusersd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `rwalld`.	Останавливает и отключает все экземпляры демона `rwalld`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `sprayd`.	Останавливает и отключает все экземпляры демона `sprayd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая демон `pcnfsd`.	Останавливает и отключает все экземпляры демона `pcnfsd`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую экземпляры.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу `TCP echo`.	Останавливает и отключает все экземпляры службы `echo(tcp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу `TCP discard`.	Останавливает и отключает все экземпляры службы `discard(tcp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу `TCP chargen`.	Останавливает и отключает все экземпляры службы `chargen(tcp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу `TCP daytime`.	Останавливает и отключает все экземпляры службы `daytime(tcp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу TCP `time`.	Останавливает и отключает все экземпляры службы `timed(tcp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу UDP `echo`.	Останавливает и отключает все экземпляры службы `echo(udp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу UDP `discard`.	Останавливает и отключает все экземпляры службы `discard(udp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу UDP `chargen`.	Останавливает и отключает все экземпляры службы `chargen(udp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу UDP `daytime`.	Останавливает и отключает все экземпляры службы `daytime(udp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу UDP `time`.	Останавливает и отключает все экземпляры службы `timed(udp)`. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле `/etc/inetd.conf`, автоматически запускающую службу.	`/etc/security/pscexpert/bin/cominetdconf`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.3	Отключить ненужные и незащищенные службы, включая службу FTP.	Останавливает и отключает все экземпляры демона ftpd. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле /etc/inetd.conf, автоматически запускающую экземпляры.	/etc/security/pscexpert/bin/cominetdconf
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.3	Отключить ненужные и незащищенные службы, включая службу telnet.	Останавливает и отключает все экземпляры демона telnetd. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле /etc/inetd.conf, автоматически запускающую экземпляры.	/etc/security/pscexpert/bin/cominetdconf
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая dtspc.	Останавливает и отключает все экземпляры демона dtspc. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле /etc/inittab, автоматически запускающую демон, если LFT не настроен, а CDE отключен в файле /etc/inittab.	/etc/security/pscexpert/bin/cominetdconf
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу ttdbserver.	Останавливает и отключает все экземпляры службы ttdbserver. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле /etc/inetd.conf, автоматически запускающую службу.	/etc/security/pscexpert/bin/cominetdconf
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 2.2.2	Отключить ненужные и незащищенные службы, включая службу cmsd.	Останавливает и отключает все экземпляры службы cmsd. Также утилита AIX Security Expert помечает символом комментария соответствующую запись в файле /etc/inetd.conf, автоматически запускающую службу.	/etc/security/pscexpert/bin/cominetdconf
PCI версии 2 2.2.3 **PCI версии 3** 2.2.4	Настроить параметры защиты системы для предотвращения несанкционированного использования.	Удаляет команды SUID путем пометки символом комментария соответствующей записи в файле /etc/inetd.conf, автоматически разрешающей использование команд.	/etc/security/pscexpert/bin/rmsuidfrmrcmds
PCI версии 2 2.2.3 **PCI версии 3** 2.2.4	Настроить параметры защиты системы для предотвращения несанкционированного использования.	Включает самый нижний уровень защиты для администратора прав доступа к файлу.	/etc/security/pscexpert/bin/filepermgr

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 2.2.3 **PCI версии 3** 2.2.4	Настроить параметры защиты системы для предотвращения несанкционированного использования.	Изменяет в протоколе NFS параметры ограничения, удовлетворяющие требованиям безопасности PCI. Эти параметры ограничения включают запрет удаленного доступа с правами пользователя root, а также доступ с анонимным UID и GID.	`/etc/security/pscexpert/bin/nfsconfig`
PCI версии 2 2.2.2 **PCI версии 3** 2.2.3	Включать только необходимые и защищенные службы, протоколы, демоны и т. д., требуемые для правильной работы системы. Внедрять защищенные функции для всех обязательных служб, протоколов или демонов, которые должны быть защищены.	Отключает демоны `rlogind`, `rshd` и `tftpd`, которые не являются защищенными.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI версии 2 2.2.2 **PCI версии 3** 2.2.3	Включать только необходимые и защищенные службы, протоколы, демоны и т. д., требуемые для правильной работы системы. Внедрять защищенные функции для всех обязательных служб, протоколов или демонов, которые должны быть защищены.	Отключает демоны `rlogind`, `rshd` и `tftpd`, которые не являются защищенными.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI версии 2 2.2.2 **PCI версии 3** 2.2.3	Включать только необходимые и защищенные службы, протоколы, демоны и т. д., требуемые для правильной работы системы. Внедрять защищенные функции для всех обязательных служб, протоколов или демонов, которые должны быть защищены.	Отключает демоны `logind`, `rshd` и `tftpdpci_rmetchostsequiv`, которые не являются защищенными.	`/etc/security/pscexpert/bin/ rmetchostsequiv`
PCI версии 2 1.3.6 **PCI версии 3** 2.2.3	Реализовать проверку с фиксацией состояний или фильтрацию пакетов, при которой в сети разрешены только установленные соединения.	Включает сетевую опцию **`clean_partial_conns`** путем присвоения ей значения 1.	`/etc/security/pscexpert/bin/ntwkopts`
PCI версии 2 2.2.2 **PCI версии 3** 2.2.3	Реализовать проверку с фиксацией состояний или фильтрацию пакетов, при которой в сети разрешены только установленные соединения.	Включает защиту TCP путем присвоения сетевой опции **`tcp_tcpsecure`** значения 7. Этот параметр предоставляет защиту от атак данных, сброса (RST) и запроса соединения TCP (SYN).	`/etc/security/pscexpert/bin/ntwkopts`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
1.2	Защитить от неавторизованного доступа к неиспользуемым портам.	Настраивает систему на отключение хостов на 5 минут для предотвращения доступа к неиспользуемым портам из других систем.	`/etc/security/pscexpert/bin/ipsecshunhosthls` **Примечание:** Можно указать дополнительные правила фильтра в файле `/etc/security/aixpert/bin/filter.txt`. Эти правила будут интегрированы с помощью сценария `ipsecshunhosthls.sh` при применении профайла. Записи должны указываться в следующем формате: *номер-порта*`:`*ip-адрес*`:` *действие* , где для поля *действие* допустимы следующие значения: `Allow` и `Deny`.
1.2	Защитить хост от сканирования портов.	Настраивает систему на блокирование уязвимых портов на 5 минут для предотвращения сканирования портов.	`/etc/security/pscexpert/bin/ipsecshunports` **Примечание:** Можно указать дополнительные правила фильтра в файле `/etc/security/aixpert/bin/filter.txt`. Эти правила будут интегрированы с помощью сценария `ipsecshunhosthls.sh` при применении профайла. Записи должны указываться в следующем формате: *номер-порта*`:`*ip-адрес*`:` *действие* , где для поля *действие* допустимы следующие значения: `Allow` и `Deny`.
7.1.1	Ограничить права доступа для создания объекта.	Задает права доступа по умолчанию для создания объекта равными 22 путем присвоения параметру **umask** значения 22.	`/etc/security/pscexpert/bin/chusrattr`
7.1.1	Ограничить доступ к системе.	Гарантирует, что в файле `cron.allow` указан только один ИД пользователя root, и удаляет файл `cron.deny` из системы.	`/etc/security/pscexpert/bin/limitsysacc`
6.5.8	Удалить точку из пути к домашнему каталогу пользователя root.	Удаляет точки из переменной среды PATH в следующих файлах, расположенных в домашнем каталоге пользователя root: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathroot`
6.5.8	Удалить точку из пути к домашнему каталогу пользователя, отличного от root:	Удаляет точки из переменной среды *PATH* в следующих файлах в домашнем каталоге пользователя: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
2.2.3	Ограничить доступ к системе.	Добавляет возможности пользователя root и имя пользователя в файл `/etc/ftpusers`.	`/etc/security/pscexpert/bin/chetcftpusers`
2.1	Удалить гостевую учетную запись.	Удаляет гостевую учетную запись и ее файлы.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Запретить запуск программ в области материалов.	Включает функцию отключения работы со стеком (SED).	`/etc/security/pscexpert/bin/sedconfig`
8.2	Гарантирует сложность пароля для пользователя root.	Запускает проверку целостности пароля пользователя root для обеспечения его надежности.	`/etc/security/pscexpert/bin/chuserstanza`
PCI версии 2 8.5.15 **PCI версии 3** 8.1.8	Ограничить доступ к системе путем настройки времени простоя сеанса.	Задает ограничение на время простоя равным 15 минутам. Если простой сеанса превышает это время, потребуется повторно ввести пароль.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Ограничить доступ потока к информации владельца кредитной карточки.	Задает максимальное значение для правила регулирования потока TCP, снижающее вероятность отказа в обслуживании для портов.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Использовать защищенное соединение при переносе данных.	Включает автоматическое создание тоннеля IPSec между виртуальными серверами ввода-вывода во время миграции работающих разделов.	`/etc/security/pscexpert/bin/cfgsecmig`
1.3.5	Ограничить пакеты из неизвестных источников.	Разрешает пакеты из HMC.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Применять антивирусное программное обеспечение.	Обеспечивает целостность системы путем обнаружения и удаления известных типов вредоносного ПО, а также защиты от него.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI версии 2 Раздел 7 **PCI версии 3** Раздел 7	Обеспечивать доступ на основе необходимости.	Включает управление доступом на основе ролей (RBAC) путем создания следующих ролей с требуемыми правами доступа: системный оператор, системный администратор, администратор безопасности информационных систем.	`/etc/security/pscexpert/bin/EnableRbac`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Реализовать более защищенные функции для всех требуемых служб, протоколов или демонов, которые могут быть незащищенными.	Использует такие защищенные технологии, как SSH, S-FTP, SSL или IPsec VPN для защиты таких незащищенных служб, как NetBIOS, обмен файлами, Telnet и FTP. Настраивает также демон SSH для использования только протокола SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Клиент SSH должен быть настроен для использования только протокола SSHv2.	Настраивает клиент SSH для использования протокола SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен принимать запросы только от адресов сети управления, если ему не предоставлены права для других целей.	Обеспечивает применение демона SSH только для обработки запросов.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен быть настроен для использования только шифров FIPS 140-2	Гарантирует, что демон SSH использует только шифры FIPS 140-2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен быть настроен для использования только кодов аутентификации сообщений (MAC) с применением криптографических алгоритмов хеширования FIPS 140-2.	Гарантирует, что MAC используют утвержденные алгоритмы.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен ограничивать возможность входа в систему определенными пользователями или группами.	Ограничивает вход в систему определенными пользователями и группами.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	После входа в систему система должна отображать дату и время последнего успешного входа в систему для учетной записи.	Сохраняет информацию о последнем успешном входе в систему и отображает ее после следующего успешного входа.	`/etc/security/pscexpert/bin/sshPCIconfig`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен в строгом режиме выполнять проверку файлов конфигурации домашнего каталога.	Гарантирует правильные режимы файлов конфигурации в домашнем каталоге.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH должен использовать разделение прав доступа.	Обеспечивает для демона SSH правильное разделение прав доступа.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 2.3	Демон SSH не должен разрешать идентификацию RSA rhosts.	Отключает идентификацию RSA для rhosts при использовании демона SSH.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI версии 2 1.1.5 2.2.2 **PCI версии 3** 10.4	Проверять процессы и стандарты конфигурации на реализацию технологии синхронизации времени и соответствие требованиям PCI DSS 6.1 и 6.2.	Включает демон ntp.	`/etc/security/pscexpert/bin/rctcpip`
PCI версии 2 Не включен в профайл версии 2, добавлен в версию 3. **PCI версии 3** 8.1.5	Отключать неиспользуемую учетную запись пользователя.	Отключает учетные записи пользователей после 35 дней отсутствия активности.	`/etc/security/pscexpert/bin/disableacctpci`
PCI версии 3 2.2.3	Выключите Secure Sockets Layer (SSL) v3 и Transport Layer Security (TLS) v1.0 в приложениях.	Выключите SSLv3 и TLS v1.0 в конфигурации сервера POP3 (Pop3d) Courier.	`/etc/security/pscexpert/bin/disableSSL`
PCI версии 3 2.2.3	Выключите SSL v3 и TLS v1.0 в приложениях.	Выключите SSLV3 и TLS v1.0 в конфигурации сервера IMAP Courier (imapd).	`/etc/security/pscexpert/bin/disableSSL`
PCI версии 3 8.2.1	Выключите SSL v3 и TLS v1.0 в приложениях.	Проверьте, указан ли в файле конфигурации протокола сетевого времени (NTP) протокол TLS 1.1 или более поздней версии.	`/etc/security/pscexpert/bin/checkNTP`

Таблица 6. Параметры, связанные с соответствием требованиям стандартов PCI DSS версии 2.0 и версии 3.0 (продолжение)

Реализует следующие стандарты PCI DSS	Спецификация реализации	Реализация AIX Security Expert	Расположение сценария, изменяющего значение
PCI версии 3 2.2.3	Выключите SSL v3 и TLS v1.0 в приложениях.	Проверьте, указан ли в файле конфигурации демона протокола передачи файлов (FTPD) протокол TLS 1.1 или более поздней версии.	`/etc/security/pscexpert/bin/secureFTP`
PCI версии 3 2.2.3	Выключите SSL v3 и TLS v1.0 в приложениях.	Проверьте, указан ли в файле конфигурации протокола передачи файлов (FTP) протокол TLS 1.1 или более поздней версии.	`/etc/security/pscexpert/bin/secureFTP`
PCI версии 3 2.2.3	Выключите SSL v3 и TLS v1.0 в приложениях.	Выключите SSLv3 и TLS v1.0 в конфигурации sendmail.	`/etc/security/pscexpert/bin/sendmailPCIConfig`
PCI версии 3 2.2.3	Выключите SSL v3 и TLS v1.0 в приложениях.	Проверьте, применяется ли в AIX протокол SSL версии выше 1.0.2.	`/etc/security/pscexpert/bin/sslversion`
PCI версии 3 8.2.1	Принудительная двухфакторная идентификация.	Включите двухфакторную идентификацию, такую как SHA-256 или SHA-512.	`/etc/security/pscexpert/bin/pwdalgchk`

Информация, связанная с данной:

Отрасль платежных карт - соответствие стандартам защиты данных

Закон Сарбейна-Оксли и согласование с COBIT

Закон Сарбейнса-Оксли от 2002-го года принят на 107-м конгрессе США и касается контроля за общественными компаниями как субъектами законов безопасности и связанных вопросов для защиты интересов инвесторов.

Раздел SOX 404 содержит требования к оценке руководством внутренних средств контроля. Для большинства организаций внутренние средства контроля охватывают ИТ-системы, обрабатывающие финансовые данные компании и формирующие отчетность. Закон SOX предоставляет конкретную информацию по ИТ-отрасли и ИТ-безопасности. Многие аудиторы SOX надеются на стандарты, например COBIT, как на методы измерения и контроля управления и руководства ИТ. Опция конфигурации XML PowerSC Standard Edition SOX/COBIT предоставляет конфигурацию защиты для систем AIX и VIOS (Сервер виртуального ввода-вывода) для соответствия требованиям соответствия COBIT.

IBM Compliance Expert Express Edition работает в следующей версии операционной системы AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

Ответственность за согласованность с внешними стандартами лежит на системном администраторе AIX. Продукт IBM Compliance Expert Express Edition разработан для упрощения управления операционной системой и отчетами, необходимыми для соответствия стандартам.

Поставляемые в составе продукта IBM Compliance Expert Express Edition заранее настроенные профайлы соответствия снижают административную нагрузку по интерпретации документов о соответствии требованиям и внедрению этих стандартов в качестве конкретных параметров конфигурации системы.

Компоненты IBM Compliance Expert Express Edition разработаны для помощи в эффективном управлении требованиями к системе, связанными с соответствием внешним стандартам, что может снизить стоимость и повысить соответствие требованиям законодательства. Все внешние стандарты защиты включают аспекты,

отличные от параметров конфигурации системы. Применение IBM Compliance Expert Express Edition не может гарантировать соответствие стандартам. Программа Compliance Expert разработана для упрощения управления параметром конфигурации систем, что помогает администраторам сосредоточиться на других аспектах соответствия стандартам.

Информация, связанная с данной:

Соответствие COBIT

Акт о преемственности и подотчетности медицинского страхования (HIPAA)

Акт о преемственности и подотчетности медицинского страхования (HIPAA) - это профайл защиты, направленный на защиту электронно защищенной информации о состоянии здоровья (EPHI).

Правило безопасности HIPAA направлено на защиту информации EPHI и распространяется только на часть организаций в зависимости от их функций и особенностей использования информации EPHI.

Все организации, попадающие под действие HIPAA, чья деятельность близка к функциям некоторых госучреждений, должны выполнять правило безопасности HIPAA.

Согласно тексту Правила безопасности HIPAA оно защищает конфиденциальность, целостность и доступность информации EPHI.

Информация EPHI, которую попадающая под правило организация создает, получает, обрабатывает и передает, должна быть защищена от вероятных угроз, несанкционированного использования и утечки.

Требования, стандарты и спецификации по реализации Правила безопасности HIPAA применяются к следующих организациям:

- Медицинские учреждения
- Программы медицинского страхования
- Расчетные палаты медицинского страхования
- Спонсоры льготных рецептов и карт на лекарственные средства в рамках программы медицинского страхования пожилых людей

В следующей таблице собрана информация о нескольких разделах Правила безопасности HIPAA. Каждый раздел включает несколько стандартов и спецификаций реализации.

Примечание: Все файлы пользовательских сценариев для обеспечения соответствия HIPAA находятся в каталоге `/etc/security/pscexpert/bin`.

Таблица 7. Правила HIPAA и детали реализации

Разделы Правила безопасности HIPAA	Спецификация реализации	Реализация aixpert	Команды и возвращаемые значения
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Реализует процедуры регулярной проверки записей о работе информационной системы, таких как протоколы контроля, отчеты о доступе и отчеты об инцидентах защиты.	Определяет, включен ли контроль в системе.	**Команда**: **#audit query**. **Возвращаемое значение**: в случае успешного выполнения эта команда завершается со значением 0. В случае неуспешного выполнения команда завершается со значением 1.

Таблица 7. Правила HIPAA и детали реализации (продолжение)

Разделы Правила безопасности HIPAA	**Спецификация реализации**	**Реализация aixpert**	**Команды и возвращаемые значения**
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Реализует процедуры регулярной проверки записей о работе информационной системы, таких как протоколы контроля, отчеты о доступе и отчеты об инцидентах защиты.	Включает контроль в системе. Также настраивает набор записываемых событий.	**Команда**: **# audit start >/dev/null 2>&1**. **Возвращаемое значение**: в случае успешного выполнения эта команда завершается со значением 0. В случае неуспешного выполнения команда завершается со значением 1. Контролируются следующие события: **FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod, FILE_Fchown**
164.312 (a) (2) (iV)	Шифрование и расшифровка (A):Реализует механизм шифрования и расшифровки информации EPHI.	Определяет включена ли EFS (шифрованная файловая система) в системе.	**Команда**: **# efskeymgr -V >/dev/null 2>&1**. **Возвращаемое значение**: если EFS уже включена, эта команда завершается со значением 0. Если EFS не включена, эта команда завершается со значением 1.
164.312 (a) (2) (iii)	Автоматический выход из системы (A): Реализует электронные процедуры закрытия электронного сеанса после определенного периода отсутствия активности.	Настраивает выход из интерактивных процедур после 15 минут отсутствия активности.	**Команда**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Возвращаемое значение**: если команде не удается найти значение**TMOUT=15**, сценарий завершается со значением 1. В противном случае команда завершается со значением 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Гарантирует, что все пароли содержат не менее 14 символов.	**Команда**: **chsec -f /etc/security/user -s user -a minlen=8**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения сценарий завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Гарантирует, что все пароли содержат хотя бы две буквы (одна из них должна быть прописной).	**Команда**: **chsec -f /etc/security/user -s user -a minalpha=4**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.

Таблица 7. Правила HIPAA и детали реализации (продолжение)

Разделы Правила безопасности HIPAA	Спецификация реализации	Реализация aixpert	Команды и возвращаемые значения
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Указывает, что пароль должен содержать не менее 2 неалфавитных символов.	**Команда**: **#chsec -f /etc/security/user -s user -a minother=2**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Гарантирует отсутствие в паролях повторяющихся символов.	**Команда**: **#chsec -f /etc/security/user -s user -a maxrepeats=1**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Запрещает повторное использование последних 5 паролей.	**Команда**: **#chsec -f /etc/security/user -s user -a histsize=5**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает срок действия пароля 13 недель.	**Команда**: **#chsec -f /etc/security/user -s user -a maxage=8**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Отменяет временный (в неделях) запрет на изменение пароля.	**Команда**: **#chsec -f /etc/security/user -s user -a minage=2**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает 4-недельный срок смены пароля, после того как истек его срок действия, указанный пользователем в параметре **maxage**.	**Команда**: **#chsec -f /etc/security/user -s user -a maxexpired=4**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.

Таблица 7. Правила HIPAA и детали реализации (продолжение)

Разделы Правила безопасности HIPAA	**Спецификация реализации**	**Реализация aixpert**	**Команды и возвращаемые значения**
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Указывает, что минимум 4 символа не должны совпадать с прежним паролем.	**Команда**: **#chsec -f /etc/security/user -s user -a mindiff=4**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Указывает, что система должна выдать предупреждение о необходимости смены пароля через 5 дней.	**Команда**: **#chsec -f /etc/security/user -s user -a pwdwarntime=5**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Проверяет правильность определений пользователей и исправляет ошибки.	**Команда**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck -n ALL**. **Возвращаемое значение**: эта команда не возвращает значений. Команда ищет и исправляет ошибки.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Блокирует учетную запись после трех неудачных попыток входа подряд.	**Команда**: **#chsec -f /etc/security/user -s user -a loginretries=3**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Устанавливает 5-секундную задержку между неудачной попыткой входа и следующей.	**Команда**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает 10 неудачных попыток входа в систему через порт, после чего порт блокируется.	**Команда**: **chsec -f /etc/security/lastlog -s username -a unsuccessful_login_count=10**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.

Таблица 7. Правила HIPAA и детали реализации (продолжение)

Разделы Правила безопасности HIPAA	**Спецификация реализации**	**Реализация aixpert**	**Команды и возвращаемые значения**
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает 60-секундный интервал времени для неудачных попыток входа через порт, по истечении которого порт отключается.	**Команда**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает 30-минутный интервал времени, по истечении которого отключенный порт разблокируется.	**Команда**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Задает 30-секундный интервал времени для ввода пароля.	**Команда**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Возвращаемое значение**: в случае успешного выполнения этот сценарий завершается со значением 0. В случае неуспешного выполнения команда завершается с кодом ошибки 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Управление паролями (A):Реализует процедуры создания, изменения и защиты паролей.	Гарантирует блокировку учетных записей по истечении 35 дней отсутствия активности.	**Команда**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Возвращаемое значение**: если команде не удается присвоить параметру **account_locked** значение **true**, сценарий завершается со значением 1. В противном случае команда завершается со значением 0.
164.312 (c) (1)	Реализует стратегии и процедуры для защиты информации EPHI от внесения неверных изменений и уничтожения.	Включить стратегии защищенного выполнения (TE).	**Команда**: Включает **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON Например, trustchk -p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Возвращаемое значение**: в случае сбоя сценарий возвращает значение 1.

Таблица 7. Правила HIPAA и детали реализации (продолжение)

Разделы Правила безопасности HIPAA	Спецификация реализации	Реализация aixpert	Команды и возвращаемые значения
164.312 (e) (1)	Реализует технические меры защиты от несанкционированного доступа к информации EPHI, которая передается по сети электронных коммуникаций.	Определяет, установлены ли наборы файлов **ssh**. Если нет, выдается сообщение об ошибке.	**Команда**: **# lslpp -l | grep openssh > /dev/null 2>&1**. **Возвращаемое значение**: если код возврата этой команды равен 0, сценарий завершается со значением 0. Если наборы файлов ssh не установлены, сценарий выводит сообщение об ошибке `Установите наборы файлов ssh для защищенной передачи данных` и завершается со значением 1.

В следующей таблице собрана информация о нескольких функциях Правила безопасности HIPAA. Каждая функция включает несколько стандартов и спецификаций реализации.

Таблица 8. Функции HIPAA и детали реализации

Функции HIPAA	Спецификация реализации	Реализация aixpert	Команды и возвращаемые значения
Ведение протоколов ошибок	Объединяет ошибки из различных протоколов и отправляет администратору по электронной почте.	Определяет наличие аппаратных ошибок. Определяет наличие неисправимых ошибок по файлу **trcfile** в каталоге `/var/adm/ras/trcfile`. Отправляет ошибки по адресу **root@<имя-хоста>**.	**Команда**: **errpt -d H**. **Возвращаемое значение**: в случае успешного выполнения эта команда завершается со значением 0. В случае неуспешного выполнения команда завершается со значением 1.
Поддержка FPM	Изменяет права доступа к файлам.	Изменяет права доступа к файлам по списку прав доступа и файлов с помощью команды **fpm**.	**Команда**: **# fpm -1 <уровень> -f <файл-команд>**. **Возвращаемое значение**: в случае успешного выполнения эта команда завершается со значением 0. В случае неуспешного выполнения команда завершается со значением 1.
Поддержка ролевого контроля доступа	Создает пользователей **isso**, **so** и **sa** и назначает им соответствующие роли.	Предлагает создать пользователей **isso**, **so** и **sa**. Назначает роли пользователям.	**Команда**: **/etc/security/pscexpert/bin/RbacEnablement**.

Информация, связанная с данной:

Акт о преемственности и подотчетности медицинского страхования (HIPAA)

Соответствие требованиям NERC

NERC (Североамериканская корпорация по вопросам надежности энергоснабжения) является некоммерческой организацией, разрабатывающей стандарты для электроэнергетики. PowerSC Standard Edition содержит готовый профайл NERC, содержащий стандарты безопасности для защиты критически важных систем электроснабжения.

Профайл NERC соответствует стандартам CIP (защита объектов жизнеобеспечения).

Профайл NERC находится в файле `/etc/security/aixpert/custom/NERC.xml`. Требования CIP, применяемые к профайлу NERC, можно сбросить в состояние по умолчанию посредством применения профайла NERC_to_AIXDefault.xml, который находится в каталоге `/etc/security/aixpert/custom`. Этот процесс отличается от операции отмены профайла NERC.

В следующей таблице приведена информация о стандартах CIP, применяемых к операционной системе AIX, и о том, как PowerSC Standard Edition обрабатывает стандарты CIP:

Таблица 9. Стандарты CIP для PowerSC Standard Edition

Стандарт CIP	**Реализация AIX Security Expert**	**Расположение сценария, меняющего значение**
CIP-003-3 R5.1	Настраивает параметры защиты системы для предотвращения уязвимостей путем удаления атрибутов SUID и SGID из двоичных файлов.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Включает ролевой контроль доступа путем создания ролей оператора системы, администратора системы и администратора защиты информационной системы с требуемыми правами доступа.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Включает SSH для защищенного доступа.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5 CIP-007-5 R1.1	Выключает следующие ненужные и небезопасные службы: • демон **lpd** • Common Desktop Environment (CDE)	`/etc/security/pscexpert/bin/comntrows`
CIP-005-3a R2.5 CIP-007-5 R1.1	Выключает следующие ненужные и небезопасные службы: • демон **timed** • демон **NTP** • демон **rwhod** • демон **DPID2** • агент DHCP	`/etc/security/pscexpert/bin/rctcpip`

Таблица 9. Стандарты CIP для PowerSC Standard Edition (продолжение)

Стандарт CIP	Реализация AIX Security Expert	Расположение сценария, меняющего значение
CIP-005-3a R2.5 CIP-007-5 R1.1	Выключает следующие ненужные и небезопасные службы: • демон **comsat** • демон **dtspcd** • демон **fingerd** • демон **ftpd** • демон **rshd** • демон **rlogind** • демон **rexecd** • демон **systat** • демон **tfptd** • демон **talkd** • демон **rquotad** • демон **rstatd** • демон **rusersd** • демон **rwalld** • демон **sprayd** • демон **pcnfsd** • демон **telnet** • служба cmsd • служба ttdbserver • служба TCP echo • служба TCP discard • служба TCP chargen • служба TCP daytime • служба TCP time • служба UDP echo • служба UDP discard • служба UDP chargen • служба UDP daytime • служба UDP time	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5 CIP-007-5 R1.1	Включает применение запроса отказа в обслуживании для портов защиты.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Включает контроль двоичных файлов системы.	`/etc/security/pscexpert/bin/pciaudit`
CIP-007-3a R3 CIP-007-5 R2.1	Выводит сообщение о включении TNC.	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-3a R4 CIP-007-5 R3.3	Обеспечивает целостность системы посредством обнаружения и удаления известных типов вредоносных программ, а также защиты от таких программ.	`/etc/security/pscexpert/bin/manageITsecurity`
CIP-007-3a R5.2.1	Включает принудительную смену пароля при первом входе для всех незаблокированных учетных записей пользователей по умолчанию.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Блокирует все учетные записи пользователей по умолчанию.	`/etc/security/pscexpert/dodv2/lockacc_rlogin`

Таблица 9. Стандарты CIP для PowerSC Standard Edition (продолжение)

Стандарт CIP	Реализация AIX Security Expert	Расположение сценария, меняющего значение
CIP-007-3a R5.3.1	Задает минимальную длину паролей 6 символов.	/etc/security/pscexpert/bin/chusrattr
CIP-007-5 R5.5.1	Задает минимальную длину паролей 8 символов.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Указывает, что каждый пароль должен быть сочетанием букв, цифр и специальных символов.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Меняет каждый пароль ежегодно.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	Выводит сообщение о включении EFS (шифрованной файловой системы).	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-5 R5.7	Ограничение числа неудачных попыток идентификации.	/etc/security/pscexpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	Выводит сообщение о включении соответствия требованиям реального времени (RTC).	/etc/security/pscexpert/bin/GeneralMsg

Информация, связанная с данной:

Соответствие требованиям NERC

Управление автоматизацией защиты и согласования

В этом разделе описывается процесс планирования и развертывания профайлов автоматизации защиты и соответствия PowerSC в группе систем согласно принятым процедурам соответствия требования законодательства и управления в ИТ-отрасли.

В рамках соответствия и управления ИТ-отраслью системы с одинаковой рабочей нагрузкой и одинаковыми классами защиты должны управляться и изменяться согласованно. Для планирования и развертывания функции соответствия в системах выполните следующие действия:

Идентификация рабочих групп системы

В руководствах по соответствию и управлению ИТ-отраслью утверждается, что системы с одинаковыми рабочими нагрузками и классами защиты должны управляться и настраиваться согласованно. Поэтому необходимо определить все системы в аналогичной рабочей группе.

Использование тестовой системы для первоначальной настройки

Примените соответствующий профайл соответствия PowerSC к тестовой системе.

Рассмотрите следующие примеры применения профайлов соответствия в операционной системе AIX.

Пример 1: применение `DoD.xml`

```
% aixpert -f /etc/security/aixpert/custom/DoD.xml
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules

Input file=/etc/security/aixpert/custom/DoD.xml
```

В этом примере отсутствуют правила с ошибкой, т. е. `Failedrules=0`. Это означает, что все правила применены успешно, и можно начинать этап тестирования. При наличии ошибок будет сформирован подробный вывод.

Пример 2: применение PCI.xml с ошибкой

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85       Passedrules=84  Failedrules=1   Level=AllRules

Input file=/etc/security/aixpert/custom/PCI.xml
```

Ошибка правила pci_grpck должна быть устранена. Возможные причины ошибки:

- Правило не применено в среде и должно быть удалено.
- Существует ошибка в системе, которая должна быть устранена.

Изучение сбойного правила

В большинстве случаев применение профайла защиты и соответствия PowerSC выполняется без ошибок. Однако система может иметь невыполненные предварительные требования, связанные с установкой, и другие неполадки, требующие внимания администратора.

Пример поиска причины сбоя:

Откройте файл /etc/security/aixpert/custom/PCI.xml и найдите сбойное правило. В данном примере это правило pci_grpck. Командой **fgrep** найдите сбойное правило pci_grpck и просмотрите связанное правило XML.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Реализует пункты раздела 8.2 стандарта PCI,
Проверить определения групп: проверяет правильность определений групп и исправляет ошибки.
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
Определения системы групп пользователей и паролей</AIXPertGroup
</AIXPertEntry
```

В правиле pci_grpck можно видеть команду /usr/sbin/grpck.

Изменение сбойного правила

При применении профайла защиты и соответствия PowerSC могут возникнуть ошибки.

В системе могут быть не выполнены предварительные требования установки и другие неполадки, требующие внимания администратора. После определения команды, лежащей в основе сбойного правила, проверьте систему и найдите сбойную команду настройки. В системе может быть неполадка защиты. Также может оказаться, что определенное правило неприменимо к среде системы. В этом случае необходимо создать нестандартный профайл защиты.

Создание профайла собственной конфигурации защиты

Если правило неприменимо к определенной среде системы, большинство организаций, обеспечивающих соблюдение нормативных требований, допускают документированные исключения.

Для удаления правила и создания собственной стратегии защиты и файла конфигурации выполните следующие действия:

1. Скопируйте следующие файлы в один файл с именем /etc/security/aixpert/custom/*<имя-стратегии-защиты>*.xml:

   ```
   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
   ```

2. В файле *<имя-стратегии-защиты>*.xml удалите неприменимое правило от открывающего тега XML <AIXPertEntry name... до закрывающего тега </AIXPertEntry.

Можно вставить дополнительные правила настройки для защиты. Вставьте дополнительные правила в схему AIXPertSecurityHardening XML. Профайлы PowerSC нельзя изменять непосредственно, но можно настраивать.

Для большинства сред необходимо создать пользовательскую стратегию XML. Для передачи нестандартного профайла в другие системы необходимо защищенно скопировать измененную стратегию XML в систему, где требуется такая же конфигурация. Пользовательская стратегия XML передается в другие системы по защищенному протоколу, например SFTP, и сохраняется в каталоге /etc/security/aixpert/custom/*<имя-стратегии-защиты>.xml*/etc/security/aixpert/custom/

Войдите в систему, где должен быть создан нестандартный профайл, и выполните следующую команду:

```
pscxpert -f : /etc/security/aixpert/custom/<имя-стратегии-защиты>.xml
```

Тестирование приложений с помощью AIX Profile Manager

Конфигурации защиты могут влиять на работу приложений и порядок доступа к системе и управления ею. Важно тестировать приложения и методы управления системой перед развертыванием системы в рабочей среде.

Стандарты соответствия требованиям законодательства требуют более строгой конфигурации защиты, чем конфигурация по умолчанию. Для тестирования системы выполните следующие действия:

1. Выберите **Просмотр профайлов и управление ими** на правой панели страницы приветствия AIX Profile Manager.
2. Выберите профайл, используемый шаблоном для развертывания систем, которые будут отслеживаться.
3. Нажмите **Сравнить**.
4. Выберите управляемую группу или отдельные системы в группе и щелкните на **Добавить**, чтобы добавить их в список выбранных.
5. Нажмите **OK**.

Запустится операция сравнения.

Мониторинг систем для непрерывного соблюдения требований с помощью AIX Profile Manager

Конфигурации защиты могут влиять на работу приложений и порядок доступа к системе и управления ею. Важно вести мониторинг приложений и методов управления системой при развертывании системы в рабочей среде.

Для мониторинга системы AIX с помощью AIX Profile Manager выполните следующие действия:

1. Выберите **Просмотр профайлов и управление ими** на правой панели страницы приветствия AIX Profile Manager.
2. Выберите профайл, используемый шаблоном для развертывания систем, которые будут отслеживаться.
3. Нажмите **Сравнить**.
4. Выберите управляемую группу или отдельные системы в группе и добавьте их в список выбранных.
5. Нажмите **OK**.

Запустится операция сравнения.

Настройка автоматизации защиты и соответствия PowerSC

Описание процедуры настройки PowerSC для автоматизации защиты и соответствия из командной строки и с помощью AIX Profile Manager.

Настройка параметров соответствия требованиям PowerSC

Основы применения функции автоматизации защиты и соответствия PowerSC, тестирования конфигурации в тестовых системах и планирования и развертывания параметров. При применении конфигурации соответствия требованиям ее параметры меняют большое количество параметров конфигурации операционной системы.

Примечание: Некоторые стандарты и профайлы требуют отключения Telnet, поскольку в Telnet пароли передаются открытым текстом. Поэтому должен быть установлен, настроен и запущен Open SSH. Можно использовать и другие средства защищенного обмена данными с настраиваемой системой. Данные стандарты соответствия требуют отключения входа пользователя `root` в систему. Перед тем как продолжить применение изменений конфигурации, необходимо настроить одного или нескольких обычных пользователей (не root). Эта конфигурация не отключает пользователя root, и можно войти в систему от имени обычного пользователя и переключиться на пользователя root командой **su**. Проверьте соединение SSH с системой, войдите как обычный пользователь и выполните команду для переключения на пользователя `root`.

Для доступа к профайлам конфигурации Министерства обороны США, PCI, SOX и COBIT используйте следующий каталог:

- Профайлы в операционной системе AIX находятся в каталоге `/etc/security/aixpert/custom`.
- Профайлы в VIOS (Сервер виртуального ввода-вывода) помещаются в каталог `/etc/security/aixpert/core`.

Настройка соответствия требованиям PowerSC из командной строки

Реализация и проверка профайла соответствия с помощью команды **pscxpert** в системе AIX и команды **viosecure** в VIOS (Сервер виртуального ввода-вывода).

Для применения профайлов соответствия PowerSC в системе AIX введите одну из следующих команд, которая зависит от требуемого уровня стандарта защиты.

Таблица 10. Команды PowerSC для AIX

Команда	Стандарт
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*Руководство по технической реализации защиты UNIX от Министерства обороны США*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Акт о преемственности и подотчетности медицинского страхования*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Стандарт безопасности данных в сфере платежных карт*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Закон Сарбейнза - Оксли (2002). Управление ИТ по COBIT*

Для применения профайлов соответствия PowerSC в системе VIOS введите одну из следующих команд для требуемого уровня стандарта защиты.

Таблица 11. Команды PowerSC для VIOS (Сервер виртуального ввода-вывода)

Команда	Стандарт
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*Руководство по технической реализации защиты UNIX от Министерства обороны США*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Акт о преемственности и подотчетности медицинского страхования*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Стандарт безопасности данных в сфере платежных карт*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Закон Сарбейнза - Оксли (2002). Управление ИТ по COBIT*

Для выполнения команды **pscxpert** в системе AIX и команды **viosecure** в VIOS может потребоваться некоторое время, поскольку они проверяют и настраивают всю систему целиком, внося в ее конфигурацию необходимые изменения. Вывод выглядит следующим образом:

```
Обработано правил=38       Выполнено правил=38  Не выполнено правил=0   Уровень=Все правила
```

Однако некоторые правила могут быть не выполнены в зависимости от среды AIX, набора установки и предыдущей конфигурации.

Например, правило предварительных требований может быть не выполнено из-за того, что система не имеет требуемого набора файлов установки. Необходимо выяснить причины каждого невыполнения правил и устранить их, прежде чем развертывать профайлы соответствия в центре обработки данных.

Понятия, связанные с данным:

“Управление автоматизацией защиты и согласования” на стр. 103
В этом разделе описывается процесс планирования и развертывания профайлов автоматизации защиты и соответствия PowerSC в группе систем согласно принятым процедурам соответствия требования законодательства и управления в ИТ-отрасли.

Настройка соответствия требованиям PowerSC с помощью AIX Profile Manager

Описание процедуры настройки профайлов защиты и соответствия PowerSC и развертывания конфигурации в управляемой системе AIX с помощью AIX Profile Manager.

Для настройки профайлов защиты и соответствия PowerSC с помощью AIX Profile Manager выполните следующие действия:

1. Войдите в IBM Systems Director и выберите AIX Profile Manager.
2. Создайте шаблон на основе одного из профайлов защиты и соответствия PowerSC, выполнив следующие действия:
   a. Выберите **Просмотр шаблонов и управление ими** на правой панели страницы приветствия AIX Profile Manager.
   b. Нажмите **Создать**.
   c. Выберите **Операционная система** в списке **Тип шаблона**.
   d. Введите имя шаблона в поле **Имя шаблона конфигурации**.
   e. Выберите **Продолжить > Сохранить**.
3. Выберите профайл для использования с шаблоном. Для этого щелкните на **Обзор** под опцией **Выберите, какой профайл будет использоваться для этого шаблона**. Профайлы состоят из следующих элементов:
   - `ice_DLS.xml` - уровень защиты по умолчанию операционной системы AIX.
   - `ice_DoD.xml` - руководство по реализации и защите Министерства обороны США для параметров UNIX.
   - `ice_HLS.xml` - общий высокий уровень защиты для параметров AIX.
   - `ice_LLS.xml` - низкий уровень защиты для параметров AIX.
   - `ice_MLS.xml` - средний уровень защиты для параметров AIX.
   - `ice_PCI.xml` - параметры PCI (сфера платежных карт) для операционной системы AIX.
   - `ice_SOX.xml` - параметры SOX или COBIT для операционной системы AIX.
4. Удалите все профайлы из списка выбранных.
5. Выберите **Добавить**, чтобы добавить требуемый профайл в список выбранных.
6. Нажмите **Сохранить**.

Для развертывания конфигурации в управляемой системе AIX выполните следующие действия:

1. Выберите **Просмотр шаблонов и управление ими** на правой панели страницы приветствия AIX Profile Manager.
2. Выберите требуемый шаблон для развертывания.
3. Нажмите **Развернуть**.

4. Выберите системы для развертывания профайла и щелкните на **Добавить**, чтобы добавить требуемый профайл в список выбранных.
5. Нажмите **OK**, чтобы развернуть шаблон конфигурации. Система будет настроена в соответствии с выбранным шаблоном профайла.

Для успешного развертывания для Министерства обороны США, PCI или SOX в конечной точке системы AIX должен быть установлен PowerSC Standard Edition. Если в развертываемой системе не установлен PowerSC, выполнить развертывание не удастся. IBM Systems Director развертывает шаблон конфигурации в выбранные конечные точки системы AIX и настраивает их в соответствии с нормативными требованиями.

Информация, связанная с данной:

Администратор профайлов AIX

IBM Systems Director

PowerSC Real Time Compliance

Компонент PowerSC Real Time Compliance постоянно отслеживает включенные системы AIX для гарантии их согласованной и защищенной настройки.

Компонент PowerSC Real Time Compliance работает со стратегиями PowerSC Compliance Automation и AIX Security Expert для создания уведомлений о возникших нарушениях соответствия или об изменении отслеживаемого файла. При нарушении стратегии конфигурации защиты системы компонент PowerSC Real Time Compliance отправляет сообщение электронной почты или текстовое сообщение для предупреждения системного администратора.

Компонент PowerSC Real Time Compliance - это пассивный компонент защиты, поддерживающий заранее определенные или измененные профайлы соответствия, включающие указания по технической реализации защиты данных министерства обороны, стандарт защиты данных в сфере платежных карт, закон Сарбейна-Оксли и COBIT. Он предоставляет список файлов для отслеживания на наличие изменений, но в список можно добавить и другие файлы.

Установка PowerSC Real Time Compliance

Компонент PowerSC Real Time Compliance устанавливается с PowerSC Standard Edition версии 1.1.4 или более поздней и не входит в состав базовой операционной системы AIX.

Для установки PowerSC Standard Edition выполните следующие действия:

1. Убедитесь, что компонент PowerSC Standard Edition будет устанавливаться в одну из следующих операционных систем AIX:
   - IBM AIX 6 с технологическим пакетом обслуживания 7 или выше с AIX Event Infrastructure для AIX и AIX Clusters (bos.ahafs 6.1.7.0) или выше
   - IBM AIX 7 с технологическим пакетом обслуживания 1 или выше с AIX Event Infrastructure для AIX и AIX Clusters (bos.ahafs 7.1.1.0) или выше
   - AIX версии 7.2 или выше с AIX Event Infrastructure для AIX и AIX Clusters (bos.ahafs 7.2.0.0) или выше
2. Для обновления или установки набора файлов компонента PowerSC Standard Edition установите набор файлов `powerscStd.rtc` из пакета установки для PowerSC Standard Edition версии 1.1.4 или выше.

Настройка PowerSC Real Time Compliance

Компонент PowerSC Real Time Compliance можно настроить для отправки предупреждений при нарушениях профайла соответствия или при изменениях в отслеживаемом файле. Некоторые примеры профайлов включают указания по технической реализации защиты данных министерства обороны, стандарт защиты данных в сфере платежных карт, закон Сарбейнса-Оксли и COBIT.

Компонент PowerSC Real Time Compliance можно настроить одним из следующих способов:

- Выполнить команду **mkrtc**.
- Запустить утилиту SMIT с помощью следующей команды:

  ```
  smit RTC
  ```

Идентификация файлов, отслеживаемых функцией PowerSC Real Time Compliance

Функция PowerSC Real Time Compliance отслеживает список файлов по умолчанию на наличие изменений параметров высокоуровневой защиты. Этот список можно настроить, добавив файл в список или удалив из него в файле `/etc/security/rtc/rtcd_policy.conf`.

Существует два способа определения шаблона соответствия , применяемого в системе. Первый - это использование команды **pscxpert**, второй - использование AIX Profile Manager с IBM Systems Director.

После идентификации профайла соответствия можно добавить дополнительные файлы в список отслеживаемых файлов в файле `/etc/security/rtc/rtcd_policy.conf`. После сохранения файла новый список будет сразу использоваться в качестве контрольной версии без необходимости перезапуска системы.

Настройка предупреждений для PowerSC Real Time Compliance

Для настройки уведомлений компонента PowerSC Real Time Compliance необходимо указать тип и получателей предупреждений.

Демон rtcd, который является основным компонентом функции PowerSC Real Time Compliance, получает информацию о типах и получателях предупреждений из файла конфигурации `/etc/security/rtc/rtcd.conf`. Изменить сведения в этом файле можно с помощью текстового редактора.

Информация, связанная с данной:

Формат файла /etc/security/rtc/rtcd.conf для соответствия среде выполнения

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 Profile Manager 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. 115
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 сбор протоколов контроля, отключение системы от сети, выключение системы и предупреждение пользователей).
- Случалось ли это на других системах, которые необходимо проверить?

Понятия, связанные с данным:

“Устранение неполадок функции Надежная загрузка” на стр. 115
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 VIOS (Сервер виртуального ввода-вывода), 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” на стр. 7
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 защищенной загрузкой AIX`.

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 **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 **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 защищенной загрузки.
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 выполнение незащищенной 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 12. 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.
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. 112

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. 111
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 VIOS (Сервер виртуального ввода-вывода) 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 на стр. 120 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.

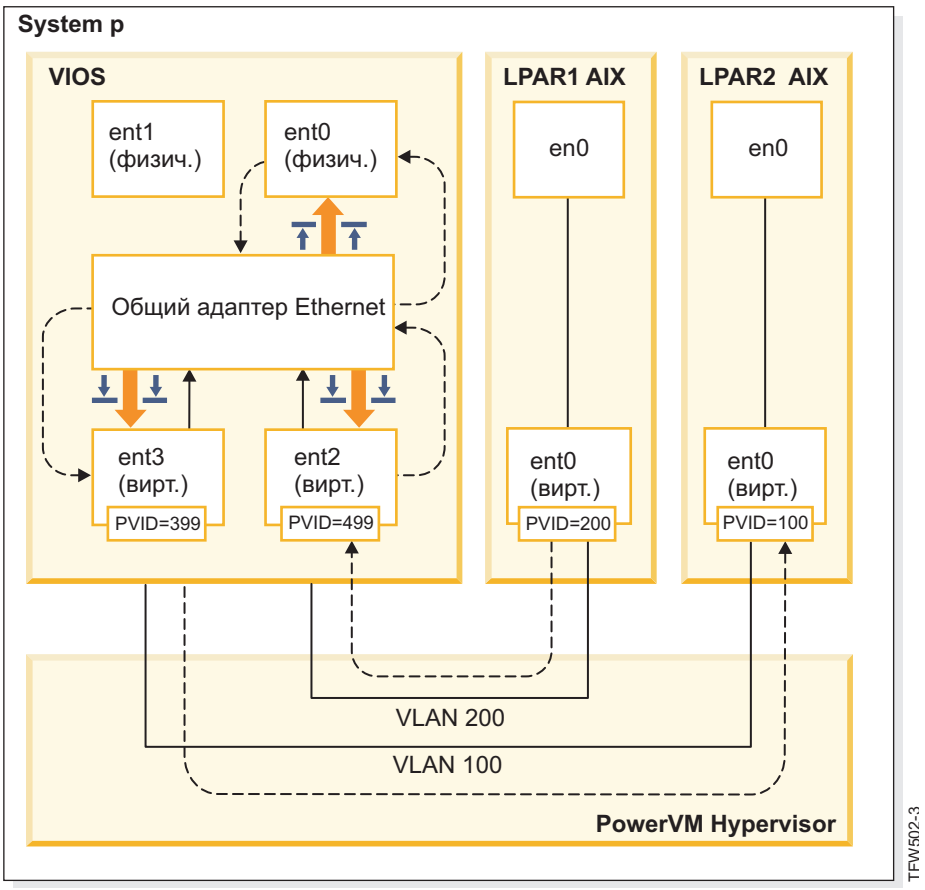

Рисунок 1. Пример передачи информации между VLAN без Надежного брандмауэра

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. 121.

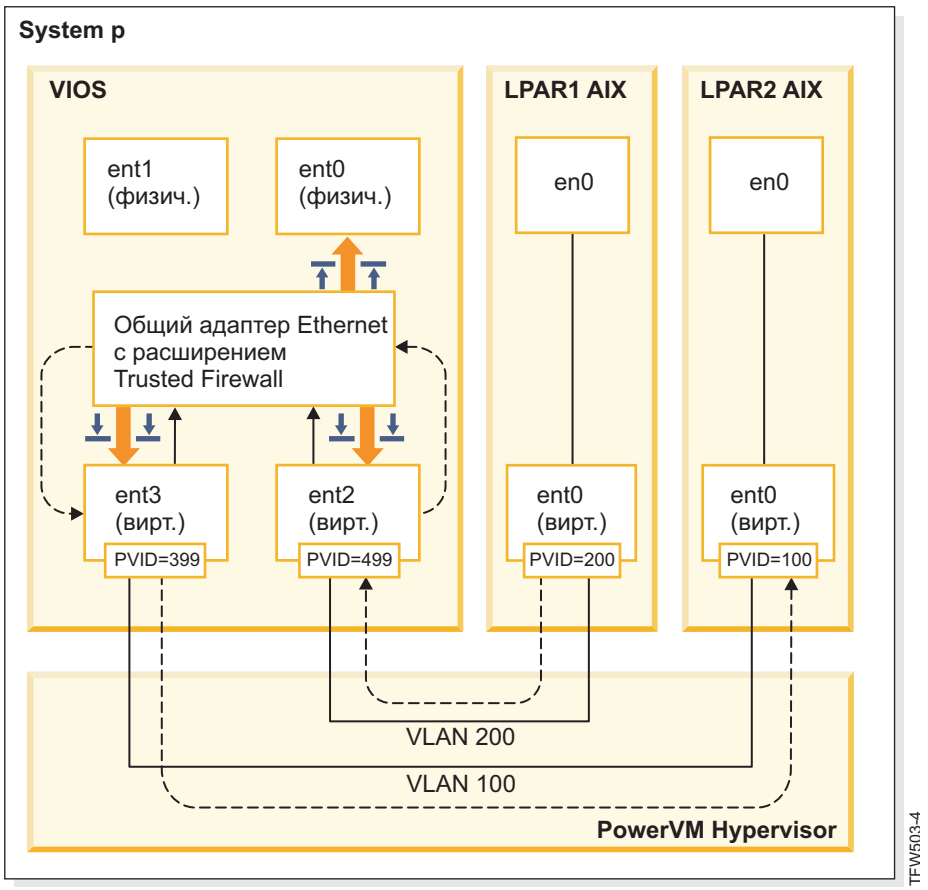

Рисунок 2. Пример передачи информации между VLAN с помощью Надежного брандмауэра

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 VIOS (Сервер виртуального ввода-вывода).

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” на стр. 7
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.

Советник по вопросам надежного брандмауэра

Советник по вопросам надежного брандмауэра анализирует поток данных системы от разных логических разделов (LPAR) для определения, может ли работающий надежный брандмауэр повысить быстродействие системы.

Если функция советника по воспросам 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 включения советника по вопросам надежного брандмауэра выполните следующую команду:

```
vlantfw -m
```

Для отображения результатов советника по вопросам надежного брандмауэра выполните следующую команду:

```
vlantfw -D
```

Для отключения советника по вопросам 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 Советник по вопросам 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`.

Примечание: Можно выполнять команды для запуска и останова ведения протокола доверенного брандмауэра только при входе в систему с именем пользователя root.

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 VIOS (Сервер виртуального ввода-вывода). 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.

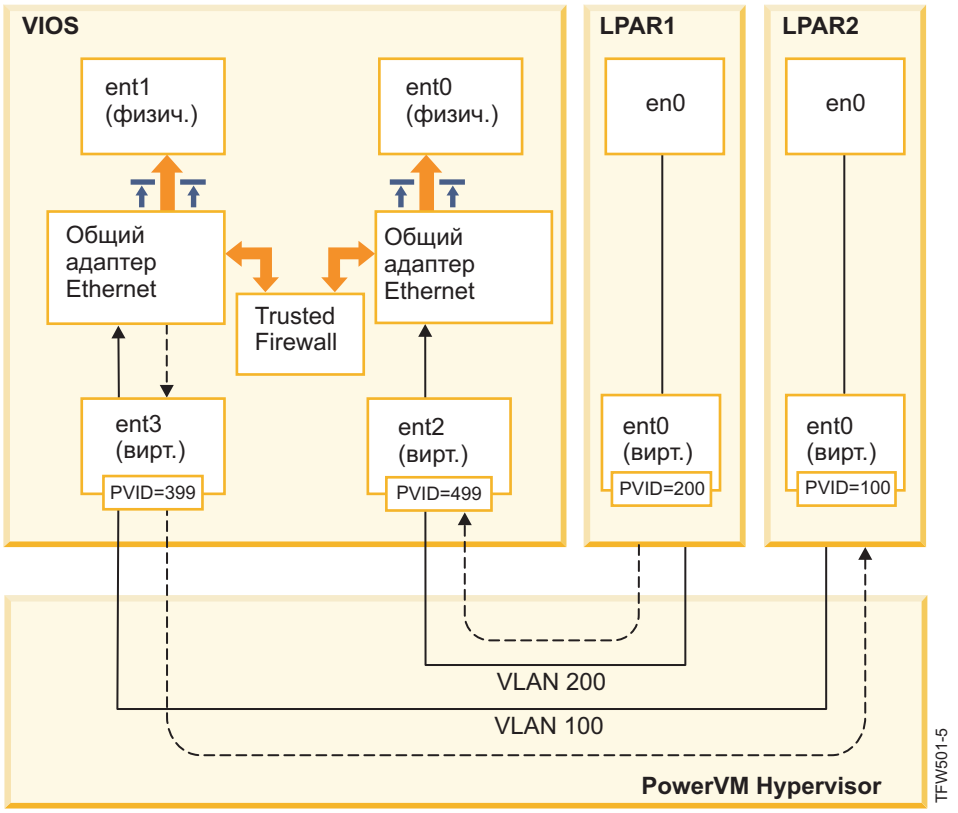

Рисунок 3. Конфигурация с несколькими Общими адаптерами Ethernet в одном VIOS

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 VIOS (Сервер виртуального ввода-вывода), 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 (команды следует вводить в одной строке):
   ```
   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. 168

“Команда mkvfilt” на стр. 170

“Команда vlantfw” на стр. 189

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 VIOS (Сервер виртуального ввода-вывода), 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. 124
Можно создать правила маршрутизации между VLAN с помощью Надежного брандмауэра.

Ссылки, связанные с данной:

“Команда lsvfilt” на стр. 169

“Команда rmvfilt” на стр. 188

Защищенные протоколы

Защищенные протоколы PowerVM позволяют логическим разделам AIX (LPAR) вести записб в в файлы протоколов в присоединенной VIOS (Сервер виртуального ввода-вывода). Данные передаются в VIOS непосредственно через гипервизор, и сетевая связь не требуется между LPAR клиента и VIOS.

Виртуальные протоколы

Администратор VIOS (Сервер виртуального ввода-вывода) 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 от 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

В качестве имен двух компонентов администратор VIOS может указать любые значения, но имя клиента обычно одинаковое для всех виртуальных протоколов в заданной 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” на стр. 7
Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Настройка защищенного ведения протокола

Настройка защищенного ведения протокола в подсистеме контроля AIX 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. 127.

Для настройки подсистемы контроля AIX выполните следующие действия:

1. Настройте подсистему контроля AIX для ведения протокола данных в двоичном режиме (`auditbin`).
2. Активируйте функцию защищенного ведения 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 VIOS (Сервер виртуального ввода-вывода) 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. 127.

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 (TNC)

Надежное сетевое соединение (TNC) - это компонент группы надежных вычислений (TCG), который предоставляет спецификации для проверки целостности конечных точек. TNC определяет открытую архитектуру решения, которая помогает администраторам применять стратегии для эффективного управления доступом к сетевой инфраструктуре.

Надежное сетевое соединение (TNC) состоит из четырех компонентов:

- Сервер TNC
- Управление исправлениями TNC
- Сервер TNC
- Определитель IP TNC

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 Надежное сетевое соединение (TNC)

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 TNC

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

Администратор исправлений загружает последние пакеты обновлений и исправления службы защиты с веб-сайтов IBM ECC и Fix Central. Демон управления исправлениями TNC передает последнюю обновленную информацию на сервер TNC, который играет роль набора файлов контрольной версии для проверки клиентов.

Демон **tncpmd** должен быть настроен для управления загрузками 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.

Управлять исправлениями можно:

- С помощью интерфейса командной строки (pmconf)
- С помощью демона (tncpmd2)

Управление исправлениями с помощью интерфейса командной строки (pmconf):

При загрузке уровня пакета обновлений (уровня SP) с помощью команды **pmconf add** вызываются SUMA и cURL.

При загрузке уровня пакета обновлений (уровня SP) с помощью команды **pmconf add** вызывается SUMA, чтобы загрузить и зарегистрировать уровень SP в TNC. Кроме того, вызывается cURL, чтобы загрузить все новые и недостающие исправления службы защиты.

Следующие аргументы команды **pmconf get** предоставляют дополнительные возможности по управлению исправлениями службы защиты:

- **display-only** позволяет пользователю изучить описания уязвимостей, для которых предназначены исправления службы защиты, применимые к уровню SP. Исправления службы защиты этой командой не загружаются.
- **download-only** позволяет пользователю загрузить исправления службы защиты в пользовательский каталог, но не применять их. Исправления не применяются.

Управление исправлениями с помощью демона (tncpmd2):

Компонент планировщика демона можно настроить на автоматическую проверку наличия обновлений, влияющих на защищенность клиентов TNC.

Частота, с которой планировщик проверяет наличие новых уровней пакетов обновлений, определяется интервалом загрузки. Если для текущего технологического уровня (TL), зарегистрированного в TNC, обнаруживается новый уровень пакета обновлений, то и этот уровень, и все недостающие и новые исправления службы защиты загружаются и добавляются в хранилище. Интервал загрузки задается командой **pmconf init**. Рекомендуемое значение интервала соответствует ежемесячной проверке (43200 минут).

Частота, с которой планировщик проверяет наличие новых временных исправлений службы защиты, который могут быть опубликованы, определяется интервалом загрузки временных исправлений. Все новые исправления службы защиты загружаются и добавляются в хранилище. Рекомендуемое значение интервала загрузки временных исправлений соответствует ежедневной проверке (1440 минут).

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 VIOS (Сервер виртуального ввода-вывода), 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. 175

Требования к TNC

Для полноценного использования всех возможностей каждого компонента TNC необходимо убедиться в соблюдении минимальных требований в среде.

Управление исправлениями TNC

AIX	SUMA	OpenSSL	Примечания
7.2 TL1	7.2.1.0	1.0.2	Поставляется с операционной системой
7.2 TL0	7.2.1.0	1.0.2	Может потребоваться отдельная установка SUMA/Java.
7.1 TL4	7.2.1.0	1.0.2	Может потребоваться отдельная установка SUMA/Java.
7.1 TL1, TL2, TL3			Загрузка уровней пакетов обновлений AIX 7.2 не поддерживается
7.1 TL0			Минимальный поддерживаемый уровень выпусков для TNCPM

Настройка компонентов TNC

Каждый из компонентов TNC требует некоторой настройки для работы в конкретной среде.

Все шаги следующей процедуры обязательны для настройки компонентов TCN. Дополнительные необязательные шаги описаны в разделе

1. Определите IP-адреса систем, в которых предстоит настраивать сервер TNC, сервер TNCPM и указатель IP TNC для Сервер виртуального ввода-вывода (VIOS).
2. Настройте сервер управления сетевой установкой (NIM). Сервером NIM должна служить система, настроенная в качестве сервера TNCPM. В ней нужно установить набор файлов `sets:bos.sysmgt.nim.master`.
3. Для автоматического уведомления сервера TNC о новых пакетах исправлений и исправлениях службы защиты необходимо включить Autonomic Health Advisor (AHA). Если AHA не включен, то планировщик TNC будет обновлять сервер TNC через заданный интервал. Для включения AHA для автоматического уведомления введите следующую команду:

   ```
   mkdir /aha
    /usr/sbin/mount -v ahafs  /aha /aha
   ```

4. Для инициализации хранилищ исправлений, обеспечивающих управление исправлениями TNC, введите следующую команду (в одной строке):

   ```
   pmconf init -i <интервал загрузки> -l <список TL> [-A] [-P <путь для 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**.

5. Настройте сервер TNCPM. Сервер TNCPM можно настроить в системе NIM. Для загрузки исправлений с веб-сайтов IBM Fix Central и ECC сервер TNCPM использует SUMA. Для загрузки временных исправлений с сайта IBM Security Site сервер TNCPM использует cURL. Для загрузки обновлений необходимо подключить систему 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
   ```

6. Настройте стратегии на сервере TNC. Создание стратегий проверки клиентов описано в разделе “Создание стратегий для клиента TNC” на стр. 139.
7. 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
   ```

8. Закончите настройку компонентов TNC, выполнив необязательные шаги для каждого компонента.

Ссылки, связанные с данной:

“Команда psconf” на стр. 175

Информация, связанная с данной:

“Установка PowerSC Standard Edition” на стр. 7
Набор файлов необходимо установить для каждой конкретной функции PowerSC Standard Edition.

Установка с NIM

IBM Fix Central

Электронный справочный центр Passport Advantage

Настройка опций компонентов TNC

Для каждого компонента TNC можно настроить одну или несколько опций.

Настройка опций сервера TNC

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, а для порта `pmserver` - 38240.

Ссылки, связанные с данной:

“Команда psconf” на стр. 175

Настройка дополнительных опций клиента TNC

В статье описаны этапы настройки клиента 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. 175

Настройка опций сервера управления исправлениями TNC

Для создания комплексного решения, предназначенного для управления исправлениями, сервер TNCPM интегрируется с SUMA и cURL.

Сервер TNCPM необходимо настроить на сервере NIM, чтобы можно было обновлять клиенты TNC.

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

Для управления хранилищами открытых пакетов TNCPM можно использовать следующие команды:

```
pmconf add -o <имя пакета> -V
<версия> -T [installp|rqm] -D
<пользовательский путь>
pmconf delete -o <имя пакета> -V <версия>
pmconf list -o <имя пакета> -V <версия>
pmconf list -O [-c] [-q]
```

Открытые пакеты добавляются в этот каталог по умолчанию:

`/var/tnc/tncpm/fix_repository/packages`.

Пользовательский путь = расположение пакета в системе

Если вы хотите просмотреть описания, для которых предназначены исправления службы защиты из пакета исправлений конкретного уровня, не применяя сами исправления к хранилищу, то введите следующую команду:

```
 pmconf get -L -p <SP>
```

Например:

```
pmconf get -L -p 7200-01-01
```

Если вы хотите загрузить исправления службы защиты из пакета исправлений конкретного уровня, не применяя сами исправления к хранилищу, то введите следующую команду:

```
pmconf get -p <SP> -D
<загрузочный_каталог>
```

Примечание: Для выполнения этой команды *каталог загрузки* должен уже существовать.

Например:

```
pmconf get -p 7200-01-01 -D /tmp/ifixes_7200-01-01
```

Сервер управления исправлениями TNC поддерживает применение команды **syslog** для загрузки пакета исправлений, технологического уровня и обновлений клиентов. Утилита - `user`, приоритет - `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. 175

Информация, связанная с данной:

Защита IBM AIX

Настройка почтовых уведомлений сервера Надежное сетевое соединение

В статье описана процедура настройки уведомлений по электронной почте для сервера Надежное сетевое соединение (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. 175

Настройка указателя IP в VIOS

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

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.

Ссылки, связанные с данной:

“Команда psconf” на стр. 175

Управление компонентами TNC

В статье описано управление TNC для выполнения таких задач, как добавление клиентов, стратегий, протоколов и результатов проверки и 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. 175

Создание стратегий для клиента TNC

В статье описана настройка стратегий, относящихся к клиенту 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`

| Для добавления стратегии OpenPackage введите следующую команду:

| `pconf add -O <группа-открытых-пакетов> <имя-открытого-пакета:версия>`

| Ниже приведен пример добавления стратегии OpenPackage:

| `psconf add -O opengrp2 openssl:1.0.1.516`

| Для присвоения стратегии OpenPackage стратегии Fspolicy введите следующую команду:

| `psconf add -O opengrp2 fspolicy=fspolicy1`

| **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. 175

| 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 VIOS (Сервер виртуального ввода-вывода) 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:

  ```
  pconf 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. 175

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. 175

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.

Для обновления клиента с помощью открытых пакетов выполните следующую команду:

```
psconf update -i <ip> -O opengrp2
```

Ссылки, связанные с данной:

“Команда psconf” на стр. 175

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. 171

Импорт сертификатов TNC

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

Демоны 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. 175

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}
```

Для просмотра списка зарегистрированных пакетов с открытым исходным кодом выполните следующую команду:

```
psconf report -O ALL -o TEXT
```

Ссылки, связанные с данной:

“Команда psconf” на стр. 175

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 13. 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.

Таблица 13. Устранение неполадок параметров конфигурации для TNC и системы управления исправлениями (продолжение)

Неполадка	Исправление
Ссылающаяся на IP TNC программа не запущена в VIOS (Сервер виртуального ввода-вывода)	• 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.

GUI (графический пользовательский интерфейс) PowerSC

В этом разделе приведено описание IBM GUI (графический пользовательский интерфейс) PowerSC, включая инструкции по установке обслуживанию и использованию интерфейса.

IBM GUI PowerSC повышает удобство использования продукта PowerSC Standard Edition, предлагая альтернативу командной строке и помогая работать с файлами протоколов. GUI PowerSC предлагает централизованную консоль управления для визуализации конечных точек и их состояния, применения, отмены и проверки уровней соответствия, группировки систем для управления уровнем соответствия, а также просмотра и настройки профайлов соответствия.

GUI PowerSC также включает функцию File Integrity Monitoring (FIM). FIM содержит Real Time Compliance (RTC) и Trusted Execution (TE). С помощью GUI PowerSC можно настроить RTC и TE и просматривать события в режиме реального времени. GUI PowerSC также предоставляет широкие возможности по редактированию профайлов и созданию отчетов.

Концепции GUI PowerSC

Перед тем как приступить к работе с GUI PowerSC, рекомендуется ознакомиться с основными концепциями, которые относятся к защите и обнаружению конечных точек.

Защита GUI PowerSC

GUI PowerSC обеспечивает защиту за счет применения двунаправленных соединений HTTPS между сервером GUI PowerSC и агентами GUI PowerSC в каждой конечной точке AIX.

В процессе согласования TLS применяются сертификаты, доступные на сервере GUI PowerSC и агентах GUI PowerSC. Процесс TLS поддерживает идентификацию в обоих направлениях, поскольку начать взаимодействие может как агент GUI PowerSC, так и сервер GUI PowerSC. Агент создает одноразовую строку (случайное число), которое отправляется серверу GUI PowerSC при первом обращении. Впоследствии сервер GUI PowerSC добавляет эту одноразовую строку во все команды, отправляемые агенту. Одноразовая строка позволяет дополнительно подтвердить, что агент конечной точки получил команду от подлинного сервера GUI PowerSC. Конечная точка должна подтвердить надежность источника вызова веб-службы. Для этой цели применяются начальное согласование и одноразовая строка.

Протоколы и комплекты шифров, применяемые для защиты данных, передаваемых между агентами GUI PowerSC и сервером GUI PowerSC, соответствуют требованиям к безопасности защищенных систем. В настоящее время применяется протокол TLS 1.2. Сервер GUI PowerSC взаимодействует со всеми агентами GUI PowerSC и всеми пользователями GUI PowerSC. Таким образом, сервер GUI PowerSC должен содержать сертификат, который считается надежным всеми соединениями из веб-браузеров пользователя. В качестве примера можно привести сертификаты, выпущенные сертификатными компаниями, такими как Verisign, или внутренними надежными сертификатными компаниями.

В ходе установки сервер GUI PowerSC создает собственный сертификат для собственного использования. Срок действия этого сертификата не ограничен, однако он предназначен для временного использования и его можно заменить на сертификат, выпущенный надежной сертификатной компанией. Кроме того, в ходе установки сервера GUI PowerSC создается подписывающий сертификат, применяемый для подписания всех сертификатов конечных точек.

Процесс установки автоматически создает файл хранилища доверенных сертификатов для каждого конечной точки. Все конечные точки используют один и тот же файл хранилища доверенных сертификатов, который необходимо скопировать с сервера GUI PowerSC в каждую конечную точку. Такая комбинация сертификатов на сервере GUI PowerSC и в конечных точках обеспечивает высокий уровень защиты передаваемых данных.

Группы UNIX предлагают дополнительные средства управления защитой. Для входа в GUI PowerSC любой пользователь, будь то пользователь LDAP или локальный пользователь, определенный операционной системой, должен входить в состав соответствующей группы UNIX. Администратор может задать или изменить состав участников этой группы с помощью команды **pscuiserverctl**.

После входа в систему пользователь может остаться в режиме только просмотра. Функция управления правами доступа пользователей позволяет выполнять действия над конечными точками, управляемыми с помощью групп UNIX. Для выполнения любых действий необходимо входить в состав группы UNIX, обладающей правами на управление конечной точкой. Дополнительная информация приведена в разделе Указание групп, обладающих доступом.

По умолчанию любой пользователь, входящий в состав группы защиты, может управлять всеми конечными точками, отображаемыми в GUI PowerSC. Администратор PowerSC может ограничить доступ пользователей на уровне отдельных конечных точек с помощью команды **setGroups.sh**.

Некоторые команды настройки может выполнять только администратор. Например, это относится к изменению глобальных параметров электронной почты или созданию профайлов. Права администратора задаются через группы UNIX и настраиваются с помощью команды **pscuiserverctl**.

Заполнение данных о конечной точке на странице Соответствие требованиям

Сервер GUI PowerSC и агент GUI PowerSC взаимодействуют с конечной точкой для определения уровня соответствия.

При запуске агент пытается обратиться к серверу GUI PowerSC. После того как соединение будет установлено, выполняется однократное согласование параметров защиты соединения между агентом и сервером. После успешного согласования параметров защиты сервер создает элемент домена с уникальным идентификатором (UID) для внутреннего представления конечной точки и передает UID конечной точке. UID используется во всех операциях взаимодействия между агентом и сервером. Это действие завершает процесс обнаружения. Защищенное взаимодействие сервера GUI PowerSC и конечной точки обеспечивается в обоих направлениях.

После начального согласования или перезапуска агент GUI PowerSC выполняет попытку определить текущее состояние соответствия конечной точки и обновляет сервер GUI PowerSC. С учетом текущей информации о конечных точках и уровне соответствия заполняется страница состояния соответствия в GUI PowerSC. Если информация о состоянии соответствия отсутствует, то эта запись будет отсутствовать на странице состояния соответствия.

Сервер GUI PowerSC содержит представление всех известных конечных точек, которые создаются в автоматическом режиме в результате начального взаимодействия агентов и сервера. Агенты конечных точек отслеживают изменения состояния соответствия конечных точек и передают их серверу. Пользователь может взаимодействовать из GUI PowerSC с конечной точкой только через сервер GUI PowerSC. Пользовательский интерфейс не может обращаться напрямую к конечным точкам и их агентам.

Установка GUI PowerSC

Агенты GUI PowerSC и компоненты сервера GUI PowerSC устанавливаются вместе с PowerSC Standard Edition. Каждый из них устанавливается из наборов файлов `installp`.

Агент GUI PowerSC

Агент GUI PowerSC устанавливается в каждой конечной точке AIX. Агент GUI PowerSC отслеживает операции в конечной точке и передает эту информацию серверу GUI PowerSC.

Кроме того, на агенте GUI PowerSC выполняются команды, запускаемые из GUI PowerSC. Все данные между агентами GUI PowerSC и сервером GUI PowerSC передаются в зашифрованном виде.

Команда `installp` устанавливает базовый продукт PowerSC Standard Edition и агент GUI PowerSC. Набор файлов `powerscStd.uiAgent.rte`**installp** применяется для установки агента GUI PowerSC. В следующем примере показана команда `installp`, которая выполняется в каждой конечной точке:

Примечание: В следующем примере установочные образы распаковываются в каталог `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgent.rte
```

Сервер GUI PowerSC

Сервер GUI PowerSC можно запустить только в системе AIX. Для установки сервера GUI PowerSC рекомендуется создать выделенный логический раздел AIX.

Команда **installp** устанавливает базовый продукт PowerSC Standard Edition и сервер GUI PowerSC. Набор файлов `powerscStd.uiServer.rte` **installp** применяется для установки сервера GUI PowerSC. В следующем примере показана команда **installp**, которая выполняется в конечной точке:

Примечание: В следующем примере установочные образы распаковываются в каталог `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiServer.rte
```

Требования GUI PowerSC

Рассмотрены требования к программному и аппаратному обеспечению для GUI PowerSC.

Аппаратное обеспечение

- Компоненты сервера GUI PowerSC следует устанавливать в отдельном логическом разделе или виртуальной машине, работающей под управлением AIX 7.1 или более поздней версии.
- Компоненты агента GUI PowerSC должны быть установлены в каждой конечной точке AIX.

Программное обеспечение

- Для работы сервера GUI PowerSC требуется AIX 7.1 или более поздней версии.
- Для работы сервера GUI PowerSC необходимо запустить демон sendmail.
- Для правильного отображения описаний правил профайлов на языках, отличных от английского, необходимо установить набор файлов `bos.loc.utf.<ЯЗЫК>` для GUI PowerSC.

Рассылка сертификата защиты хранилища доверенных сертификатов в конечные точки

Системные администраторы должны развернуть сертификат защиты хранилища доверенных сертификатов во всех конечных точках.

Файл хранилища доверенных сертификатов создается во время установки и может использоваться всеми конечными точками. Он называется `endpointTruststore.jks`. Файл помещается в каталог `/etc/security/powersc/uiServer/`.

После установки вы должны поместить файл `endpointtruststore.jks` в каждую конечную точку для агента GUI PowerSC в этой точке, чтобы установить связь с сервером GUI PowerSC и начать процесс, в результате которого в конечной точке будет создано хранилище ключей.

Разослать файл хранилища доверенных сертификатов можно одним из следующих способов:

- Вручную скопировать файл `endpointTruststore.jks` в каждую конечную точку.
- Если в среде применяется PowerVC (или другой Администратор виртуализации), то файл `endpointTruststore.jks` можно поместить в образ PowerVC. При развертывании образа PowerVC в конечной точке будут развернуты и агент GUI PowerSC, и файл хранилища доверенных сертификатов.

После того, как endpointTruststore.jks развернут одним из указанных способов, при запуске конечной точки агент GUI PowerSC воспользуется файлом хранилища доверенных сертификатов для определения расположения сервера GUI PowerSC. Затем агент GUI PowerSC отправит сообщение серверу GUI PowerSC с запросом на объединение списков доступных и отслеживаемых конечных точек.

Копирование файла хранилища доверенных сертификатов в конечные точки вручную

Системные администраторы должны вручную скопировать файл хранилища доверенных сертификатов в каждую конечную точку, существующую в их среде.

Файл хранилища доверенных сертификатов необходимо также скопировать в каждую новую конечную точку, добавляемую в среду.

Примечание: При наличии Администратора виртуализации данных, такого как PowerVC, можно скопировать файл хранилища доверенных сертификатов в новую конечную точку, создав образ, содержащий и агент GUI PowerSC, и этот файл. См. раздел “Копирование файла хранилища доверенных сертификатов в конечные точки с помощью Администратора виртуализации”.

1. Для того чтобы скопировать файл /etc/security/powersc/uiServer/endpointTruststore.jks хранилища доверенных сертификатов конечной точки в файл /etc/security/powersc/uiAgent/endpointTruststore.jks в каждой конечной точке, выполните следующую команду **scp**:

   ```
   # scp endpointTruststore.jks user@endpoint-host-name:
                          /etc/security/powersc/uiAgent
   ```

2. Для того чтобы перезапустить агенты конечных точек после установки сертификата защиты, выполните следующие команды в конечной точке:

   ```
   stopsrc -s pscuiagent
   startsrc -s pscuiagent
   ```

3. Повторите шаги 1 и 2 для всех существующих конечных точек, а также всех новых конечных точек (если у вас нет Администратора виртуализации данных).

Копирование файла хранилища доверенных сертификатов в конечные точки с помощью Администратора виртуализации

С помощью Администратора виртуализации, такого как PowerVC, системные администраторы могут скопировать файл хранилища доверенных сертификатов в конечные точки, используя образ, содержащий агент PowerSC и этот файл.

1. Скопируйте файл хранилища доверенных сертификатов конечных точек, /etc/security/powersc/uiServer/endpointTruststore.jks, в образ PowerVC.
2. Разверните образ PowerVC в каждой новой конечной точке, добавленной в систему.

Настройка учетных записей пользователей

По умолчанию все пользователи, включая пользователей LDAP и локальных пользователей, должны входить в состав группы защиты для входа в GUI PowerSC.

Администратор может изменить состав участников этой группы с помощью команды **pscuiserverctl**. После входа в GUI PowerSC пользователь может просматривать состояние конечных точек, только если он входит в состав группы UNIX, которой разрешено управлять конечной точкой. Администратор может изменить параметры учетной записи пользователя на уровне отдельной конечной точки с помощью команды **setGroups.sh**.

Обратите внимание на следующие рекомендации:

- Между конечными точками и группами AIX существуют взаимосвязи многие-ко-многим:
  - Одну группу AIX можно связать с несколькими конечными точками.

  - Одну конечную точку можно связать с несколькими группами AIX.
- После входа пользователя в GUI PowerSC с учетом связанных групп определяется, может ли пользователь выполнять команды в конкретных конечных точках или может только просматривать состояние конечной точки.
  - Для выполнения команд в конкретной конечной точке с помощью GUI PowerSC пользователь должен входить в состав одной из групп, связанных с конечной точкой.
  - Группы пользователя сравниваются с набором групп, связанных с конечной точкой. Если среди групп пользователя есть хотя бы одна, связанная с этой конечной точкой, то пользователю разрешено выполнять в этой конечной точке такие команды, как **Применить профайлы**, **Отменить** и **Проверить**. Если среди групп пользователя нет ни одной, связанной с этой конечной точкой, то пользователь может лишь просматривать состояние этой конечной точки.

В каталоге `/opt/powersc/uiServer/bin/` сервера GUI PowerSC доступны следующие сценарии оболочки.

Таблица 14. Сценарии оболочки для работы с группами

Сценарий оболочки	Описание
`pscuiserverctl`	Задает группу входа в систему AIX (UNIX), в состав которой должен входить пользователь для входа в GUI PowerSC. Пользователю достаточно входить в состав одной такой группы.
`setGroups.sh`	Задает одну или несколько групп AIX, в состав которых должен входить пользователь для выполнения команд в конкретных конечных точках.

Выполнение команд и сценариев настройки групп

Системный администратор должен выполнить команду **pscuiserverctl** и сценарий **setGroups**, чтобы указать группы операционной системы, которым будет разрешен вход в GUI PowerSC, выполнение администраторских функций и выполнение команд в конкретных конечных точках.

1. На сервере GUI PowerSC перейдите в каталог `/opt/powersc/uiServer/bin/`.
2. Выполните следующую команду, чтобы указать группу AIX, участникам которой будет разрешено входить в GUI PowerSC. Указанная группа записывается в файл `/etc/security/powersc/uiServer/uiServer.conf`.

   ```
   pscuiserverctl set logonGroupList abp,security
   ```

   Совет: Перед выполнением этой команды можно просмотреть список групп, в состав которых входит пользователь, с помощью команды **groups** *имя_пользователя*.
3. Выполните следующую команду, чтобы указать группы UNIX, которым будет разрешено выполнять администраторские функции с помощью GUI PowerSC.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```
4. Выполните следующий сценарий, чтобы указать группы AIX, участникам которых будет разрешено выполнять команды в конкретных конечных точках. Укажите полные имена хостов конечных точек. Указанные группы записываются в файл `/etc/security/powersc/uiServer/groups.txt`.

   ```
   ./setGroups.sh имя_группы "список имен хостов конечных точек через запятую"
   ```

   Примечание: При поиске конечных точек предоставляется ограниченная поддержка символов подстановки. Например, следующие спецификации позволяют запросить все конечные точки, имена которых начинаются со строки "Boston_" или заканчиваются строкой ".rs.com":
   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Совет: Эта команда поддерживает единственный символ подстановки - звездочку (*). Его можно указывать только в начале или конце строки.

Работа с GUI PowerSC

С помощью GUI PowerSC можно просмотреть конечные точки, обнаруженные в системе, создать настроенные группы, создать настроенные профайлы, скопируйте пользовательские профайлы в конечные точки и применить профайлы. Кроме того, можно проверить и прервать связь между конечными точками и сервером GUI PowerSC.

Главная страница GUI PowerSC содержит следующие разделы:

- Раздел **Группы**: содержит список групп, созданных в среде. Группа - это набор конечных точек, сгруппированных по общему признаку. Группа **Все системы** создается автоматически в процессе обнаружения конечных точек в среде. Можно создать настроенные группы. Например, можно создать группу конечных точек с поддержкой HIPPA.
- Страница **Соответствие требованиям** состоит из трех разделов:
  - На верхней панели отображается статистическая информация для группы, выбранной в разделе **Группы**, включая последние уровни соответствия, примененные к конечным точкам из выбранной группы. Для выбранной группы можно просмотреть процент успешных и неудачных проверок, общее число проверенных правил и список правил, в которых возникли ошибки.
  - Центральная панель предназначена для выполнения действий над одной или несколькими конечными точками. Можно применить, отменить или проверить уровень соответствия.
  - Нижняя панель содержит таблицу со всеми конечными точками или с группой конечных точек, доступных в среде. В таблице указана следующая информация о каждой конечной точке:
    - Имя системы
    - Тип правила соответствия
    - Время и дата применения уровня соответствия к конечной точке
    - Время и дата проверки уровня соответствия в конечной точке
    - Состояние уровня соответствия
    - Число непройденных правил в конечной точке
    - Число успешно пройденных правил в ходе проверки уровня соответствия конечной точки
- Страница **Защита** состоит из двух разделов:
  - На верхней панели отображается информация о защите в режиме реального времени для группы конечных точек, выбранной в разделе **Группы**. Для выбранной группы можно просмотреть общее количество событий Real time Compliance (RTC), общее количество событий Trusted Execution (TE), процентную долю конечных точек с актуальными исправлениями TNC, процентную долю конечных точек с установленным Trusted Boot, количество конечных точек с установленным Trusted Firewall и процентную долю конечных точек с установленным Trusted Logging.
  - На нижней панели показана таблица системных конечных точек группы. В таблице указана следующая информация о каждой конечной точке:
    - Имя системной конечной точки
    - Индикаторы событий целостности файлов
    - Состояние активации RTC
    - Состояние активации TE
    - Состояние актуальности исправлений TNC
- На странице **Отчеты** содержатся отчеты о соответствии требованиям и о целостности файлов. Даны и обзорные, и подробные отчеты.
- Страница **Редактор профайлов** состоит из трех разделов:
  - Верхняя панель содержит выпадающее меню с перечнем имеющихся встроенных и пользовательских профайлов
  - Центральная панель - это строка задач, позволяющая удалять и создавать профайлы, а также копировать их в конечные точки, входящие в группу.

– Нижняя панель содержит таблицу всех правил выбранного профайла. Для каждого правила показана следующая информация:
  - Имя правила соответствия
  - Тип правила соответствия
  - Описание правила

Выбор языка GUI PowerSC

GUI PowerSC может работать на разных языках.

Для выбора языка для GUI PowerSC щелкните на значке **Языки и параметры** в строке меню главной страницы. В меню будет показан текущий рабочий язык интерфейса. Для смены языка щелкните на соответствующем значке. Выберите язык для сеанса из списка имеющихся языков.

Навигация в GUI PowerSC

С помощью GUI PowerSC можно настраивать и администрировать соединения между конечными точками и сервером; организовывать и группировать конечные точки; отслеживать и применять встроенные и пользовательские уровни и профайлы соответствия; отслеживать и настраивать защиту конечных точек; генерировать и планово рассылать отчеты.

1. Откройте GUI PowerSC. Откроется домашняя страница GUI PowerSC.
2. Для администрирования соединений между конечными точками и сервером щелкните на значке **Языки и параметры** в строке меню главной страницы. Щелкните на значке **Администратор конечной точки**, чтобы проверить или прервать соединения между конечными точками и сервером GUI PowerSC. Дополнительная информация приведена в разделе “Администрирование соединения между конечной точкой и сервером”.
3. Для того чтобы открыть Редактор групп, щелкните на многоточии горизонтальной линии в окне навигации страницы Соответствие требованиям или Защита. С помощью Редактора групп можно создавать пользовательские группы конечных точек. Дополнительная информация приведена в разделе “Создание пользовательских групп” на стр. 153.
4. Для того чтобы создать пользовательские профайлы соответствия и скопировать их в конечные точки, щелкните на вкладке **Редактор профайлов**. Дополнительная информация приведена в разделе “Работа с профайлами соответствия” на стр. 154.
5. Для отслеживания и применения встроенных и пользовательских уровней и профайлов соответствия щелкните на вкладке **Соответствие требованиям**. Дополнительная информация приведена в разделе Применение уровней и профайлов соответствия.
6. Для отслеживания и настройки защиты конечных точек щелкните на вкладке **Защита**. Дополнительная информация приведена в разделе Отслеживание защиты конечных точек.
7. Для создания и рассылки отчетов по требованию или согласно плану щелкните на вкладке **Отчеты**. Дополнительная информация приведена в разделе Работа с отчетами.

Администрирование соединения между конечной точкой и сервером

На странице **Администратор конечной точки** можно проверить или прервать соединения между конечными точками и сервером GUI PowerSC. Можно также проверить и сгенерировать запросы на создание хранилища ключей.

Проверка связи между конечной точкой и сервером

Можно проверить связь между обнаруженными конечными точками и сервером GUI PowerSC.

1. Щелкните на значке **Языки и параметры** в строке меню главной страницы. Выберите **Администратор конечных точек**. Откроется страница администрирования конечных точек.

2. В разделе **Группы** выберите группу, содержащую конечные точки, которые требуется проверить. В таблице отображаются конечные точки, входящие в состав группы.
3. В таблице соответствия отображаются все системные конечные точки из выбранной группы. С помощью поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст фильтра в поле и нажмите Enter. В списке конечных точек останутся только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**.
5. Отметьте переключатель каждой конечной точки, которую требуется проверить.
6. Щелкните на значке **Проверить**.
7. В столбцах **Проверено** и **Диагностика связи** отображается подтверждение.

Удаление конечных точек из числа отслеживаемых в GUI PowerSC

Все обнаруженные конечные точки постоянно отслеживаются. В случае удаления из среды конечную точку также необходимо удалить из конфигурации сервера GUI PowerSC.

Для удаления конечных точек из числа отслеживаемых в GUI PowerSC выполните следующие действия:

1. Щелкните на значке **Языки и параметры** в строке меню главной страницы. Выберите **Администратор конечных точек**. Откроется страница администрирования конечных точек.
2. В разделе **Группы** выберите группу, содержащую конечные точки, которые требуется удалить. В таблице отображаются конечные точки, входящие в состав группы.
3. В таблице соответствия отображаются все системные конечные точки из выбранной группы. С помощью поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст фильтра в поле и нажмите Enter. В списке конечных точек останутся только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**.
5. Отметьте переключатель каждой конечной точки, которую требуется прекратить отслеживать.
6. Щелкните на значке **Удалить**.
7. В столбцах **Проверенное системное время** и **Диагностика связи** отображается подтверждение об удалении конечной точки.

Проверка и генерация запросов на создание хранилищ ключей

Для каждой конечной точки необходимо проверить допустимость запроса на создание хранилища ключей; если запрос допустим, то можно создать хранилище.

При первом запуске конечной точки агент GUI PowerSC с помощью файла хранилища доверенных сертификатов определяет расположение сервера GUI PowerSC. Затем агент GUI PowerSC отправит сообщение серверу GUI PowerSC с запросом на объединение списков доступных, отслеживаемых конечных точек.

На странице **Администратор конечных точек Запросы на создание хранилищ ключей** можно проверить допустимость запроса на создание хранилища ключей; если запрос допустим, то можно создать хранилище.

1. Щелкните на значке **Языки и параметры** в строке меню главной страницы. Выберите **Администратор конечных точек**. Откроется страница администрирования **Конечная точка - все системы**.
2. Все известные конечные точки перечислены в столбце **Имя системы**. Нажмите **Запросы на создание хранилищ ключей**, чтобы проверить, нет ли ожидающих запросов. Откроется страница **Администратор конечных точек Запросы на создание хранилищ ключей**.
3. Запросы на создание хранилищ ключей для всех новых или добавленных серверов перечислены в столбце **Имя хоста**. Подтвердив, что вы хотите расширить хранилище ключей до данной конечной точки, отметьте ее переключатель и нажмите **Проверить**.

4. Проверку выполняет PowerVC. Укажите ИД пользователя и пароль в окне **Необходимы идентификационные данные PowerVC**. Нажмите **OK**. Если у вас нет PowerVC, пропустите этот и следующий шаги.

   Примечание: Проверка - это процесс, в ходе которого с помощью API Openstack выясняется, известно ли PowerVC о только что объявленной конечной точке. Если PowerVC отсутствует в пользовательской среде или если powervcKeystoneUrl не настроен (с помощью pscuiserverctl), то PowerSC не сможет проверить конечную точку.
5. После проверки выдается сообщение в виде всплывающего текста в столбце **Имя хоста**. Сообщение указывает, удалось ли PowerVC распознать новую конечную точку. В зависимости от содержимого этого сообщения, вы можете принять решение о создании хранилища ключей.
6. Для создания хранилища ключей нажмите **Создать хранилище ключей**. Во время создания хранилища ключей строка конечной точки в таблице будет мигать. По окончании значение в столбце **Создано хранилище ключей** изменится с **нет** на **да**.

   Примечание: Если вы не проверили конечную точку с помощью PowerVC, то появится сообщение с вопросом, следует ли продолжать проверку. Нажмите **Продолжить**, если вы распознали конечную точку и хотите создать хранилище ключей.

   На обнаружение вновь созданного хранилища ключей у агента PowerSC может уйти несколько минут. После того, как агент установит хранилище ключей, новая конечная точка будет указана как полностью управляемая конечная точка на страницах **Администратор конечных точек - все системы**, **Соответствие требованиям**, **Защита** и **Отчеты** GUI PowerSC.
7. Если вы не хотите создавать хранилище ключей для конечной точки, удалите запрос. Отметьте переключатель конечной точки, которую вы хотите удалить, и щелкните на значке **Удалить**.
8. В таблице конечных точек отображаются все конечные точки, ожидающие проверки хранилищ ключей. С помощью поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст фильтра в поле и нажмите **Enter**. В списке конечных точек останутся только те конечные точки, которые содержат указанный текст.
9. Для обновления содержимого таблицы конечных точек нажмите **Обновить таблицу**.

Организация и группировка конечных точек

Системный администратор может организовать и сгруппировать конечные точки с учетом какого-либо общего свойства. Пользовательские группы могут содержать выбранные конечные точки, управляемые с помощью GUI PowerSC.

Например, в конфигурации с 3 - 4 средами может потребоваться создать группы, содержащие рабочие конечные точки, тестовые конечные точки и конечные точки обеспечения качества.

В ходе установки создается группа по умолчанию с именем **Все системы**. Эта группа содержит все конечные точки, обнаруженные в среде.

Создание пользовательских групп

Можно создать пользовательскую группу с нумерованным списком, содержащим выбранные конечные точки.

1. В разделе **Группы** выберите **Создать группу**. Откроется раздел **Создание группы**. Если раздел **Группы** не развернут, щелкните на многоточии горизонтальной линии в левом окне главной страницы интерфейса.
2. Введите уникальное имя для новой группы и нажмите Enter. Новая группа будет добавлена в раздел **Группы**.
3. Добавьте системы в группу. В списке **Все системы** имеющихся систем конечных точек выберите те, которые нужно включить в группу. Щелкните на стрелке вправо, чтобы переместить все выбранные системы в новую группу. Для удаления систем конечных точек из группы выделите конечную точку в списке новых групп и нажмите стрелку влево.

4. Добавив или удалив элементы группы, сохраните изменения, щелкнув на значке **Сохранить** в строке меню окна содержимого.
5. Щелкните на многоточии горизонтальной линии, чтобы вернуться в раздел **Группы**. В списке появится новая группа.

Добавление или удаление систем, назначенных существующей группе

Можно добавлять и удалять конечные точки, назначенные существующей группе.

1. В разделе **Группы** щелкните на многоточии справа от той группы, в которую вы хотите добавить или из которой вы хотите удалить систему конечной точки. Если раздел **Группы** не развернут, то щелкните на многоточии горизонтальной строки в левом окне главной страницы интерфейса.
2. Нажмите **Изменить группу**.
3. Для добавления системы конечной точки в группу выберите систему в списке **Все системы** и щелкните на стрелке вправо. Система будет добавлена в список ***Имя группы***.
4. Для удаления конечной точки из группы выберите систему в списке **Системы группы** и щелкните на стрелке влево. Система будет удалена из списка ***Имя группы***.
5. Щелкните на значке **Сохранить изменения в группе** для сохранения изменений.
6. Для удаления системы из группы выберите систему и щелкните на стрелке влево.
7. Для отмены изменений в группе нажмите **Отменить изменения в группе**.
8. Щелкните на многоточии **Группы**, чтобы вернуться в раздел **Группы**.

Удаление группы

Ненужные группы можно удалить.

1. В разделе **Группы** щелкните на многоточии справа от той группы, которую вы хотите удалить. Если раздел **Группы** не развернут, то щелкните на многоточии горизонтальной строки в окне навигации главной страницы интерфейса.
2. Нажмите **Удалить группу**. Группа будет удалена и исчезнет из списка групп в разделе **Группы**.

Переименование группы

Можно переименовать группу конечных точек.

1. В разделе **Группы** щелкните на многоточии справа от той группы, которую вы хотите переименовать. Если раздел **Группы** не развернут, то щелкните на многоточии горизонтальной линии в окне навигации главной страницы интерфейса.
2. Нажмите **Переименовать группу**. В поле **Имя группы** введите новое имя группы.

Дублирование группы

Дублирование группы позволяет создать ее копию с теми же конечными точками и новым именем.

1. В разделе **Группы** щелкните на многоточии справа от группы, которую нужно удалить. Если раздел **Группы** не развернут, щелкните на многоточии горизонтальной линии в окне навигации главной страницы интерфейса.
2. Нажмите **Дублировать группу**. Группа будет скопирована под новым именем.

Работа с профайлами соответствия

В редакторе профайлов GUI PowerSC можно просматривать встроенные профайлы соответствия, создавать пользовательские профайлы и копировать профайлы в конечные точки.

В состав продукта PowerSC Standard Edition входит набор встроенных профайлов, предназначенных для настройки конечных точек с учетом требований следующих стандартов обеспечения безопасности:

- Отрасль платежных карт - соответствие стандартам защиты данных (PCI)

- Закон Сарбейна-Оксли и согласование с COBIT (SOX-COBIT)
- Соответствие требованиям STIG Министерства обороны США (DoD)
- Акт о преемственности и подотчетности медицинского страхования (HIPAA)
- Соответствие требованиям NERC

Дополнительная информация о встроенных профайлах приведена в разделе “Понятия автоматизации обеспечения соответствия и защиты” на стр. 9.

Каждый встроенный профайл содержит правила, которые необходимо применить к конечной точке для выполнения требований защиты. Если требуется применить только подмножество или другой набор этих правил или настроить уровни соответствия, то можно создать пользовательский профайл.

В большинстве сред администраторы часто изменяют файлы соответствия с целью удаления правил, вызывающих неполадки. После завершения проверок совместимости файлы правил соответствия определяются как стабильные и развертываются на рабочих серверах.

GUI PowerSC позволяет создавать пользовательские профайлы путем комбинирования правил из встроенных профайлов (или других пользовательских профайлов).

Просмотр профайлов соответствия

Можно просмотреть правила, входящие в состав встроенных и пользовательских профайлов.

1. На главной странице выберите вкладку **Редактор профайлов**. Откроется страница **Редактор профайлов**.
2. Щелкните на стрелке вниз, чтобы открыть список профайлов. В выпадающем меню будут показаны имеющиеся **Встроенные профайлы** и **Пользовательские профайлы**.
3. Выберите профайл для просмотра. Для каждого правила в профайле показаны его имя, тип и описание. Дополнительная информация о правилах приведена в разделе “Понятия автоматизации обеспечения соответствия и защиты” на стр. 9.
4. Все правила для выбранного профайла отображаются в таблице профайлов. С помощью поля **Фильтрация по тексту** можно отфильтровать список профайлов. Введите текст для фильтрации в текстовом поле. Список правил в выбранном профайле будет обновлен.

Создание пользовательского профайла

Новый профайл можно создать на основе существующего, а затем настроить его, включив в него лишь нужные правила.

1. На главной странице выберите вкладку **Редактор профайлов**. Откроется страница **Редактор профайлов**.
2. Щелкните на стрелке вниз, чтобы открыть список профайлов. В выпадающем меню будут перечислены имеющиеся **Встроенные профайлы** и **Пользовательские профайлы**.
3. Выберите профайл, который послужит основой для нового профайла.
4. Щелкните на значке **Создать профайл**. Откроется окно Имя и тип нового профайла.
5. Введите имя нового профайла в поле **Имя профайла**.
6. Введите тип в поле **Тип профайла**. Это значение обычно указывает тип встроенной стратегии, на которой основан новый профайл, плюс уникальный идентификатор. Например, PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz или NERCabc.
7. Нажмите **Подтвердить**.
8. Для добавления правила к пользовательскому профайлу выберите правило в исходном профайле, на основе которого вы создаете профайл, и нажмите стрелку вправо. Правило будет добавлено в новый пользовательский профайл. Повторите это действие для каждого правила, которое нужно добавить.
9. Для удаления правила из пользовательского профайла выберите правило в профайле и нажмите стрелку влево. Правило будет удалено из нового пользовательского профайла. Повторите это действие для каждого правила, которое нужно удалить.
10. По окончании добавления правил нажмите **Сохранить**.

Копирование профайлов в элементы группы

Пользовательские профайлы можно скопировать в группу конечных точек. Профайл, скопированный в конечную точку, доступен для применения в ней. Кроме того, можно проверить возможность применения профайла к конечной точке без ошибок.

1. На главной странице выберите вкладку **Редактор профайлов**. Откроется страница **Редактор профайлов**.
2. Щелкните на стрелке вниз, чтобы открыть список профайлов. В выпадающем меню будут показаны имеющиеся **Встроенные профайлы** и **Пользовательские профайлы**.
3. Выберите профайл, который вы хотите скопировать в элементы группы.
4. Щелкните на значке **Скопировать профайл в элементы группы**. Откроется окно **Скопировать *имя_профайла* в**.
5. Группы, созданные для организации, снабжены переключателями. Отметьте переключатель каждой группы, в которую требуется скопировать выбранный профайл.
6. Нажмите **Скопировать**.
7. Для применения или проверки профайла вернитесь на страницу **Соответствие требованиям**, выбрав вкладку **Соответствие требованиям**.

Удаление пользовательского профайла

Можно удалить пользовательские профайлы.

1. На главной странице выберите вкладку **Редактор профайлов**. Откроется страница **Редактор профайлов**.
2. Щелкните на стрелке вниз, чтобы открыть список профайлов. В выпадающем меню будут показаны имеющиеся **Встроенные профайлы** и **Пользовательские профайлы**.
3. Разверните список **Пользовательские профайлы**.
4. Выберите профайл, который требуется удалить.
5. Щелкните на значке **Удалить профайл**. Выбранный пользовательский профайл удален.

Администрирование уровней и профайлов соответствия

Системный администратор может применить, проверить или отменить встроенные и пользовательские уровни и профайлы соответствия в нескольких конечных точках.

В следующей таблице перечислены стандартные уровни и профайлы соответствия, поддерживаемые PowerSC Standard Edition.

Таблица 15. Стандартные уровни и профайлы соответствия, поддерживаемые PowerSC Standard Edition

Профили	**Уровни**
База данных	низкий
DoD	средний
DoD_to_AIXDefault	высокий
DoDv2	по умолчанию
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	

Таблица 15. Стандартные уровни и профайлы соответствия, поддерживаемые PowerSC Standard Edition (продолжение)

Профили	Уровни
SOX-COBIT	

На странице **Соответствие требованиям** в GUI PowerSC можно выполнить следующие задачи:

- Выберите и примените профайл или уровень к одной или нескольким конечным точкам.
- Запустите операцию отмены в одной или нескольких конечных точках.
- Проверьте профайл или уровень с учетом текущего состояния для одной или нескольких конечных точек. Операция проверки не вносит изменения в конечную точку, однако параметр **Системное время проверки** обновляется с учетом времени последней проверки.

Применение уровней и профайлов соответствия

Уровень или профайл соответствия можно применить к одной или нескольким конечным точкам из выбранной группы.

1. На главной странице выберите вкладку **Соответствие требованиям**. Откроется страница **Соответствие требованиям**.
2. В разделе **Группы** выберите группу, содержащую конечные точки, к которым требуется разрешить уровни и профайлы соответствия.
3. В таблице соответствия отображаются все системные конечные точки из выбранной группы. С помощью текстового поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст для фильтрации в текстовом поле и нажмите клавишу Enter. В списке конечных точек остаются только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**. Для того чтобы указать частоту автоматического обновления, выберите **Интервал обновления**.
5. В списке **Тип правила соответствия требованиям** можно просмотреть уровни и профайлы, скопированные в связанную конечную точку. Выберите уровень или профайл для применения к конечной точке. Включите связанный переключатель.
6. Повторите шаг 5 для каждой конечной точки в группе, к которой требуется применить уровни и профайлы соответствия.
7. Щелкните на значке **Применить профайлы**.
8. Выбранные уровни и профайлы соответствия применяются ко всем выбранным конечным точкам. Если отдельные правила не удалось применить, то конечная точка выделяется красной полосой; в столбце **Число невыполненных правил** отображается текст **Не выполнено**.
9. В столбце **Число невыполненных правил** для каждой выделенной конечной точки показана причина сбоя правила. Набор применяемых правил можно настроить путем создания или редактирования пользовательского профайла.

Отмена уровней соответствия

Можно отменить последний уровень или профайл соответствия, который был применен к одной или нескольким конечным точкам из выбранной группы.

Для отмены уровней соответствия выполните следующие действия:

1. На главной странице выберите вкладку **Соответствие требованиям**. Откроется страница **Соответствие требованиям**.
2. В разделе **Группы** выберите группу, содержащую конечные точки, для которых требуется отменить уровни соответствия и профайлы.

3. В таблице соответствия отображаются все конечные точки из выбранной группы. С помощью текстового поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст для фильтрации в текстовом поле и нажмите клавишу Enter. В списке конечных точек остаются только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**. Для того чтобы указать частоту автоматического обновления, выберите **Интервал обновления**.
5. Для отмены уровня или профайла, примененного к конечной точке, выполните следующие действия:
   a. Включите переключатель, связанный с конечной точкой.
   b. Щелкните на значке **Отменить**.

Проверка последнего примененного уровня или профайла соответствия

Можно проверить уровень или профайл соответствия, примененный последним к одной или нескольким конечным точкам из выбранной группы.

1. На главной странице выберите вкладку **Соответствие требованиям**. Откроется страница **Соответствие требованиям**.
2. В разделе **Группы** выберите группу, содержащую конечные точки, для которых требуется проверить уровни и профайлы соответствия.
3. В таблице соответствия отображаются все конечные точки из выбранной группы. С помощью текстового поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст для фильтрации в текстовом поле и нажмите клавишу Enter. В списке конечных точек остаются только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**. Для того чтобы указать частоту автоматического обновления, выберите **Интервал обновления**.
5. Отметьте переключатель конечной точки, которую требуется проверить.
6. Повторите шаг 5 на стр. 157 для каждой конечной точки в группе, которую требуется проверить.
7. Щелкните на значке **Проверить**.
8. Для конечной точки выполняется проверка возможности применения правил из уровня или профайла соответствия. Конечные точки не обновляются. Если отдельные правила не удалось применить, то конечная точка выделяется красной полосой; в столбце **Число невыполненных правил** отображается текст **Не выполнено**.
9. В списке **Число невыполненных правил** для каждой выделенной конечной точки можно просмотреть сообщение с причиной сбоя правила. Набор применяемых правил можно настроить путем создания пользовательского профайла.

Проверка неприменного уровня соответствия или профайла

Можно проверить уровень соответствия или профайл, который не был применен к одной или нескольким конечным точкам из выбранной группы.

1. На главной странице выберите вкладку **Соответствие требованиям**. Откроется страница **Соответствие требованиям**.
2. В разделе **Группы** выберите группу, содержащую конечные точки, для которых требуется проверить эффект уровня соответствия или профайла.
3. В таблице соответствия отображаются все конечные точки из выбранной группы. С помощью текстового поля **Фильтрация по тексту** можно отфильтровать список конечных точек. Введите текст для фильтрации в текстовом поле и нажмите клавишу Enter. В списке конечных точек остаются только те конечные точки, которые содержат указанный текст.
4. Для обновления информации о состоянии выберите **Обновить таблицу**. Для того чтобы указать частоту автоматического обновления, выберите **Интервал обновления**.
5. Отметьте переключатель конечной точки, которую требуется проверить. Можно выбрать несколько конечных точек.

6. Откройте выпадающий список **Тип последней проверки**. Выберите одну из следующих опций:
   - **Все доступные уровни** Выдает список всех доступных уровней, которые можно проверить относительно конечной точки.
   - **Все доступные профайлы** Выдает список всех профайлов, которые можно проверить относительно конечной точки.
7. Выберите уровень или профайл, который вы хотите проверить относительно конечной точки.
8. Щелкните на значке **Проверить**. Результаты проверки будут возвращены в виде списка под конечной точкой.

Отправка по электронной почте уведомления о событии соответствия

На странице Соответствие требованиям можно настроить отправку по электронной почте уведомлений о событиях соответствия одному или нескольким получателям.

1. На главной странице выберите вкладку **Соответствие требованиям**. Откроется страница **Соответствие требованиям**.
2. Щелкните на значке **Параметры электронной почты** в правом верхнем углу строки меню. Откроется окно **Параметры электронной почты**.
3. Отметьте переключатель **Отправлять мне**.
4. Введите через запятую адреса электронной почты всех получателей в поле **Адреса (через запятую)**.

Отслеживание защиты конечных точек

На странице **Защита** можно отслеживать защиту конечных точек в режиме реального времени.

На странице Защита показано состояние конечных точек, отслеживаемых функциями Real Time Compliance (RTC) и Trusted Execution (TE).

И RTC, компонент PowerSC, и TE, компонент AIX, представляют средство File Integrity Monitoring (FIM). FIM отслеживает изменения в важнейших файлах, чтобы гарантировать правомочность событий, влияющих на файлы. К событиям, потенциально угрожающим безопасности, относятся: непредвиденное изменение прав доступа к файлу, обновление содержимого файла и внеплановая установка приложения. Такие события необходимо распознавать, чтобы обеспечить безопасность важнейших файлов и приложений.

На странице **Защита** выполняется отслеживание в режиме реального времени в GUI PowerSC. На ней отображаются события, генерируемые при изменении файлов, отслеживаемых RTC и TE. Сведения о событиях указывают, когда изменилось содержимое файла, произошло обращение к конечной точке или изменилась конфигурация.

На странице **Защита** можно выполнять следующие задачи:

- Просматривать информацию об отслеживании в режиме реального времени, выполняемом RTC и TE
- Настраивать RTC и TE для всех конечных точек
- Просматривать состояние других продуктов PowerSC в конечных точках
- Включать и выключать TE

Настройка Real Time Compliance (RTC)

На странице **Защита** можно настроить продукт Real Time (RTC) для конкретной точки или их группы.

1. Щелкните на многоточии справа от конечной точки, для которой вы хотите отредактировать конфигурацию RTC.
2. Нажмите **Настроить RTC**. Откроется окно Конфигурация стратегий RTC.

3. Все доступные опции конфигурации RTC перечислены с пояснениями. Для изменения каких-либо опций конфигурации RTC отметьте или сотрите отметку с их переключателей слева от опций. В некоторых случаях изменения в опциях вступят в силу только после перезапуска сервера.
4. Нажмите **Сохранить**.

Восстановление опций конфигурации Real Time Compliance (RTC) к предыдущей версии по дате и времени

Конфигурацию RTC можно вернуть к предыдущей версии по дате и времени.

1. Щелкните на многоточии справа от конечной точки, для которой вы хотите вернуть опции конфигурации RTC к предыдущей версии.
2. Нажмите **Вернуть RTC**. Будут показаны значения системного времени для каждой версии конфигурации RTC.
3. Щелкните на системном времени нужной версии конфигурации. Будут восстановлены опции конфигурации RTC, существовавшие на эту дату и время.

Копирование опций конфигурации Real Time Compliance (RTC) в другие группы

Опции конфигурации RTC можно скопировать в другую группу или набор конечных точек.

1. Щелкните на многоточии справа от конечной точки, опции конфигурации которой вы хотите скопировать в другую группу или набор конечных точек.
2. Нажмите **Скопировать конфигурацию RTC**. Будут перечислены все группы конечных точек, в том числе группа **Все системы**.
3. Выберите группу или конкретные конечные точки одним из следующих способов:
   - Отметьте переключатель группы конечных точек в списке доступных групп. Опции конфигурации будут скопированы в каждую конечную точку группы.
   - С помощью стрелки вправо разверните группу, чтобы просмотреть список всех ее конечных точек. Отметьте переключатели всех конечных точек, в которые вы хотите скопировать опции конфигурации.
   - Разверните список конечных точек в группе **Все системы**. Отметьте переключатели всех конечных точек группы, в которые вы хотите скопировать опции конфигурации.
4. Нажмите **OK**. Опции конфигурации будут скопированы в выбранную группу или конечные точки.

Редактирование списка файлов Real Time Compliance (RTC)

Для каждого файла конечной точки можно просмотреть и отредактировать его опции отслеживания RTC.

1. Щелкните на многоточии справа от конечной точки, в которой размещены файлы, опции отслеживания RTC которых нужно просмотреть или отредактировать.
2. Нажмите **Изменить список файлов RTC**. Откроется страница **Конфигурация списка файлов RTC** с перечнем всех каталогов и файлов конечной точки. Отметка на значке папки каталога указывает, что один или несколько файлов в этом каталоге отслеживаются.
3. Если файл, опции которого вы хотите отредактировать, находится в каталоге, дважды щелкните на этом каталоге, чтобы открыть список файлов. Появится список всех файлов каталога.
4. Для каждого файла конечной точки его опции отслеживания указаны в столбцах **Содержимое** и **Атрибуты**. Отмеченный переключатель в столбце **Содержимое** означает, что отслеживаются изменения в содержимом файла. Отмеченный переключатель в столбце **Атрибуты** - что отслеживаются изменения в атрибутах файла. Для изменения опций отслеживания отметьте или сотрите отметки с переключателей файлов конечной точки.
5. Нажмите **Сохранить**.

Восстановление опций отслеживания файлов Real Time Compliance (RTC) к предыдущей конфигурации

Файлы, отслеживаемые RTC, можно вернуть к предыдущей версии.

1. Щелкните на многоточии справа от конечной точки, для которой вы хотите вернуть опции отслеживания файлов RTC к предыдущей версии.
2. Нажмите **Вернуть список файлов RTC**. Будут показаны значения системного времени для каждой версии конфигурации отслеживаемых файлов.
3. Щелкните на системном времени нужной версии конфигурации опций отслеживания. Будут восстановлены опции конфигурации, существовавшие на эту дату и время.

Копирование опций отслеживания списка файлов Real Time Compliance (RTC) в другие группы

Опции отслеживания файлов RTC можно скопировать в другую группу или набор конечных точек.

1. Щелкните на многоточии справа от конечной точки, опции отслеживания файлов которой вы хотите скопировать в другую группу или набор конечных точек.
2. Нажмите **Скопировать список файлов RTC**. Будут перечислены все группы конечных точек, в том числе группа **Все системы**.
3. Выберите группу или конкретные конечные точки одним из следующих способов:
   - Отметьте переключатель группы конечных точек в списке доступных групп. Опции отслеживания списка файлов будут скопированы в каждую конечную точку группы.
   - С помощью стрелки вправо разверните группу, чтобы просмотреть список всех ее конечных точек. Отметьте переключатели всех конечных точек, в которые вы хотите скопировать опции отслеживания списка файлов.
   - Разверните список конечных точек в группе **Все системы**. Отметьте переключатели всех конечных точек группы, в которые вы хотите скопировать опции конфигурации.
4. Нажмите **OK**. Опции отслеживания файлов будут скопированы в выбранную группу или конечные точки.

Выполнение проверки Real Time Compliance (RTC)

На странице **Защита** можно выполнить проверку RTC, чтобы выяснить, соответствует ли по-прежнему конечная точка требованиям.

1. Щелкните на многоточии справа от конечной точки, для которой вы хотите выполнить проверку Real Time Compliance (RTC).
2. Нажмите **Выполнить проверку соответствия**. Откроется страница **Соответствие требованиям** с мигающей последней строкой, что означает, что проверка выполняется.
3. Если какие-либо правила пройти не удалось, то в столбце **#Непройденные правила** появится сообщение о сбое. Щелкните на стрелке вниз слева от конечной точки, чтобы просмотреть непройденное правило.

Настройка Trusted Execution (TE)

На странице **Защита** можно настроить продукт Trusted Execution (TE) для конкретной точки или их группы.

1. Щелкните на многоточии справа от конечной точки, для которой вы хотите отредактировать опции конфигурации TE.
2. Нажмите **Настроить TE**. Откроется окно Конфигурация стратегий TE.
3. Все опции конфигурации TE перечислены с пояснениями. Для изменения каких-либо опций конфигурации TE отметьте или сотрите отметку с их переключателей. В некоторых случаях изменения в опциях вступят в силу только после перезапуска сервера.
4. Нажмите **Сохранить**.

Копирование опций Trusted Execution (TE) в другие группы

Опции конфигурации TE можно скопировать в другую группу или набор конечных точек.

1. Щелкните на многоточии справа от конечной точки, опции конфигурации которой вы хотите скопировать в другую группу или набор конечных точек.
2. Нажмите **Скопировать конфигурацию TE**. Будут перечислены все группы конечных точек, в том числе группа **Все системы**.
3. Выберите группу или конкретные конечные точки одним из следующих способов:
   - Отметьте переключатель группы конечных точек в списке доступных групп. Опции конфигурации будут скопированы в каждую конечную точку группы.
   - Разверните группу, чтобы просмотреть список всех ее конечных точек. Отметьте переключатели всех конечных точек, в которые вы хотите скопировать опции конфигурации.
   - Разверните список конечных точек в группе **Все системы**. Отметьте переключатели всех конечных точек группы, в которые вы хотите скопировать опции конфигурации.
4. Нажмите **OK**. Опции конфигурации будут скопированы в выбранную группу или конечные точки.

Редактирование списка файлов Trusted Execution (TE)

Для каждого файла конечной точки можно просмотреть и отредактировать его опции отслеживания TE.

1. Щелкните на многоточии справа от конечной точки, в которой размещены файлы, опции отслеживания TE которых нужно просмотреть или отредактировать.
2. Нажмите **Изменить список файлов TE**. Откроется страница **Конфигурация списка файлов TE** с перечнем всех каталогов и файлов конечной точки. Отметка на значке папки каталога указывает, что один или несколько файлов в этом каталоге отслеживаются.
3. Если файл, опции которого вы хотите просмотреть или отредактировать, находится в каталоге, дважды щелкните на этом каталоге, чтобы открыть список файлов. Появится список всех файлов каталога.
4. Для каждого файла конечной точки его опции отслеживания указаны в столбцах **TE** и **Волатильный**. Отмеченный переключатель в столбце **TE** означает, что отслеживаются изменения в содержимом файла. Отмеченный переключатель в столбце **Волатильный** - что отслеживаются изменения лишь прав доступа к файлу. Для изменения опций отслеживания отметьте или сотрите отметки с переключателей файлов конечной точки.
5. Нажмите **Сохранить**.

Копирование опций отслеживания списка файлов Trusted Execution (TE) в другие группы

Опции отслеживания файлов TE можно скопировать в другую группу или набор конечных точек.

1. Щелкните на многоточии справа от конечной точки, опции отслеживания файлов которой вы хотите скопировать в другую группу или набор конечных точек.
2. Нажмите **Скопировать список файлов TE**. Будут перечислены все группы конечных точек, в том числе группа **Все системы**.
3. Выберите группу или конкретные конечные точки одним из следующих способов:
   - Отметьте переключатель группы конечных точек в списке доступных групп. Опции отслеживания списка файлов будут скопированы в каждую конечную точку группы.
   - Разверните группу, чтобы просмотреть список всех ее конечных точек. Отметьте переключатели всех конечных точек, в которые вы хотите скопировать опции отслеживания списка файлов.
   - Разверните список конечных точек в группе **Все системы**. Отметьте переключатели всех конечных точек группы, в которые вы хотите скопировать опции конфигурации.
4. Нажмите **OK**. Опции отслеживания файлов будут скопированы в выбранную группу или конечные точки.

Просмотр состояния других функций PowerSC

На странице Защита можно просмотреть состояние следующих функций PowerSC: Trusted Boot, Trusted Firewall и Trusted Logging. Можно также просмотреть состояние обновлений TNC в конечной точке.

1. На главной странице выберите вкладку **Защита**. Откроется страница **Защита**.

2. Компонент TNC PowerSC служит для проверки и обновления исправлений службы защиты в каждой конечной точке. Столбец **Актуальная для TNC** в таблице конечных точек указывает, актуальна ли конечная точка с точки зрения сервера TNC. В разделе **Актуальные для TNC** баннера сводной панели показана процентная доля актуальных конечных точек в группе. Для того чтобы убрать отображение информации об обновлениях TNC со страницы **Защита**, выполните следующие действия:
   a. Щелкните на значке **Языки и параметры** в строке меню главной страницы.
   b. Выберите **Использование промежуточных продуктов**.
   c. Отключите опцию **Актуальная для TNC**.
   d. Для восстановления отображения этой информации передвиньте переключатель **Актуальная для TNC** в положение Вкл.
3. Столбец **TB** в таблице конечных точек указывает, доступен ли Trusted Boot PowerSC в конечной точке. В разделе **Trusted Boot** баннера сводной панели показана процентная доля конечных точек в текущей выбранной группе, в которых активирован Trusted Boot PowerSC. Для того чтобы убрать отображение информации Trusted Boot PowerSC со страницы **Защита**, выполните следующие действия:
   a. Щелкните на значке **Языки и параметры** в строке меню главной страницы.
   b. Выберите **Использование промежуточных продуктов**.
   c. Передвиньте переключатель **Trusted Boot** в положение Выкл.
   d. Для восстановления отображения этой информации передвиньте переключатель в положение Вкл.
4. Столбец **TF** в таблице конечных точек указывает, доступен ли Trusted Firewall PowerSC в конечной точке. В разделе **Trusted Firewall** баннера сводной панели показана процентная доля конечных точек в текущей выбранной группе, в которых активирован Trusted Firewall PowerSC. Для того чтобы убрать отображение информации Trusted Firewall со страницы **Защита**, выполните следующие действия:
   a. Щелкните на значке **Языки и параметры** в строке меню главной страницы.
   b. Выберите **Использование промежуточных продуктов**.
   c. Передвиньте переключатель **Trusted Firewall** в положение Выкл.
   d. Для восстановления отображения этой информации передвиньте переключатель в положение Вкл.
5. Столбец **TL** в таблице конечных точек указывает, доступен ли Trusted Logging PowerSC в конечной точке. В разделе **Trusted Logging** баннера сводной панели показана процентная доля конечных точек в текущей выбранной группе, в которых активирован Trusted Logging PowerSC. Для того чтобы убрать отображение информации Trusted Logging со страницы **Защита**, выполните следующие действия:
   a. Щелкните на значке **Языки и параметры** в строке меню главной страницы.
   b. Выберите **Использование промежуточных продуктов**.
   c. Передвиньте переключатель **Turusted Logging** в положение Выкл.
   d. Для восстановления отображения этой информации передвиньте переключатель в положение Вкл.

Переключение отслеживания Trusted Execution

Отслеживание Trusted Execution (TE) можно включать и выключать. Можно также выключить отслеживание TE и запланировать его включение через заданный интервал.

1. Щелкните на значке **Переключение Trusted Execution**.
2. В выпадающем разделе выберите одну из следующих опций:
   - **Включить во всех конечных точках** - чтобы включить отслеживание TE в каждой конечной точке.
   - **Выключить во всех конечных точках** - чтобы выключить отслеживание TE в каждой конечной точке.
3. Если отслеживание TE выключено, то становятся доступными опции, позволяющие задать время его повторного включения. Можно выбрать один из следующих интервалов повторного включения:
   - **1 час**
   - **5 часов**
   - **1 день**
   - **1 неделя**

- **Никогда**

4. Нажмите **Сохранить**.

Отправка по электронной почте уведомления о событии защиты

На странице Защита можно настроить отправку по электронной почте уведомлений о событиях защиты одному или нескольким получателям.

1. На главной странице выберите вкладку **Защита**. Откроется страница **Защита**.
2. Щелкните на значке **Параметры электронной почты** в правом углу строки меню. Откроется окно **Параметры электронной почты**.
3. Отметьте переключатель **Отправлять мне**.
4. Введите через запятую адреса электронной почты всех получателей в поле **Адреса (через запятую)**.

Работа с отчетами

Работать с отчетами можно на странице Отчеты GUI PowerSC.

Доступны следующие отчеты:

- Отчет **Обзор соответствия требованиям** - это моментальная копия высокоуровневой информации со страницы **Соответствие требованиям** интерфейса.
- Отчет **Сведения о соответствии требованиям** - это моментальная копия высокоуровневой и подробной информации со страницы **Соответствие требованиям**.
- Отчет **Обзор целостности файлов** - это моментальная копия высокоуровневой информации со страницы **Защита** интерфейса.
- Отчет **Сведения о целостности файлов** - это моментальная копия высокоуровневой и подробной информации со страницы **Защита**.
- **Объединенная информация о соответствии требованиям и целостности файлов**

По умолчанию на странице **Отчеты** показаны отчеты **Обзор соответствия требованиям** и **Обзор целостности файлов** для группы **Все системы**. Для отчетов **Сведения о соответствии требованиям**, **Сведения о целостности файлов** и **Объединенная информация о соответствии требованиям и целостности файлов** групп по умолчанию нет.

Вы можете создать отчет каждого типа для группы **Все системы** и любой группы, которую вы определили. Отчет можно создать для всех конечных точек группы или их подмножества. Создав отчет, вы можете запланировать его рассылку по электронной почте в виде файла CSV, вложенного в сообщение в формате HTML, одному или нескольким получателям - по требованию или ежедневно.

Перечень отчетов, показанных на странице **Отчеты**, зависит от идентификатора, под которым вы вошли в систему. Вы можете создавать отчеты только для тех конечных точек, которыми вы управляете в соответствии со своим идентификатором. Все отчеты, созданные вами в данном сеансе, будут показаны и в следующем сеансе.

Выбор группы отчета

Вы можете создать отчет каждого типа для группы **Все системы** и любой группы, которую вы определили. Отчет можно создать для всех конечных точек группы или их подмножества.

1. На главной странице выберите вкладку **Отчеты**. Откроется страница **Отчеты**.
2. Щелкните на многоточии справа от типа требуемого отчета.
3. Нажмите **Изменить группу**.
4. Откроется окно выбора с перечнем всех имеющихся групп. Отметьте переключатель группы, для которой нужно создать отчет. Нажмите **Подтвердить**. Отчет будет запущен, и на главной странице появится информация о выбранной группе.

5. Для создания отчета для подмножества конечных точек разверните группу **Все системы**. Будет показан список всех имеющихся конечных точек. Отметьте переключатель каждой конечной точки, которую нужно включить в отчет. Нажмите **Подтвердить** для создания отчета.

   Примечание: Если вы хотите создать отчет для конкретного набора конечных точек, то можете создать группу, содержащую эти точки. Создание группы позволяет сэкономить время; группа может применяться всеми пользователями, поскольку группы глобальны (видны всем пользователям интерфейса).
6. Для того чтобы найти конечную точку, введите ее имя в текстовом поле поиска. Нажмите **Подтвердить** для создания отчета для этой конечной точки.

Рассылка отчетов по электронной почте

Настроив группу для создания отчетов, вы можете запланировать их рассылку по электронной почте в виде файлов CSV, вложенных в сообщения в формате HTML. Можно запланировать немедленную или ежедневную рассылку отчетов.

Рассылка отчетов в виде файлов CSV позволяет получателям загружать данные отчетов в электронную таблицу или импортировать их в другие приложения, поддерживающие формат CSV. Файлы CSV не поддерживают графику и сводные панели. В файле CSV, созданном на основе обзорного отчета, заголовки столбцов разделены запятыми и находятся в первой строке. Последующие строки содержат конечные точки и значения всех столбцов.

На основе подробного отчета создается несколько файлов CSV. Первый файл CSV форматируется аналогично обзорному отчету. Далее, для каждого уровня сведений из отчета создается отдельный файл CSV. Например, в подробном отчете о целостности файла каждый из перечисленных ниже уровней сведений породит отдельный файл CSV:

- **Конфигурация TE**
- **Конфигурация RTC**
- **Состояние промежуточного продукта**

1. На главной странице выберите вкладку **Отчеты**. Откроется страница **Отчеты**.
2. В списке имеющихся отчетов выберите отчет для рассылки. Отчет будет запущен, и содержимое главной страницы обновится.
3. Щелкните на многоточии справа от рассылаемого отчета.
4. Нажмите **Опции электронной почты**. Откроется окно **Отправить отчет по электронной почте**.
5. Укажите электронный адрес каждого получателя в поле **Адреса**. Адреса получателей разделяются точкой с запятой (;).
6. Укажите описание электронной почты в поле **Тема**.
7. Выберите одну из следующих опций:
   - Отметьте переключатель **Отправлять ежедневно в**, чтобы отправлять отчет получателям ежедневно. Укажите местное время в часах и минутах для отправки отчета. Нажмите **Сохранить и закрыть**. Отчет будет отправляться ежедневно в указанное время.
   - Нажмите **ОТПРАВИТЬ НЕМЕДЛЕННО**, чтобы отправить отчет немедленно. Отчет будет отправлен и окно закроется.

Команды PowerSC Standard Edition

PowerSC Standard Edition предоставляет команды, позволяющие установить связь с компонентом Trusted Firewall и компонентом TNC 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” на стр. 170

“Команда vlantfw” на стр. 189

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. 125
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. 168

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 того чтобы можно было загружать метаданные пакета исправлений, сервер TNCPM необходимо запускать только в AIX версии 7.2 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** <*загрузочный каталог*>] [**-x** <*интервал ifix*>] [**-K** <*ключ ifix*>]

pmconf add -l *Список-TL*

pmconf add -o <*имя пакета*> -V <*версия*> -T [installp|rqm] -D <*пользовательский путь*>

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**

pmconf chtncpm attribute = *значение*

pmconf delete -l <*Список TL*>

pmconf delete -o <*имя пакета*> -V <*версия*>

pmconf delete -p <*Список SP*>

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

pmconf export -f *имя-файла*

pmconf get -o <пакет> -V <версия> -T <installp | rpm> -D <загрузочный каталог>

pmconf get -L -o <пакет> -V <версия | all> -T <installp | rpm>

pmconf get -L -p <SP>

pmconf get -p <SP> -D <загрузочный_каталог>

pmconf hist -d

pmconf hist -u

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

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*имя пакета*> -V <*версия*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

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 proxy display

pmconf proxy [enable=yes | no] [host=<хост>] [port=<порт>]

pmconf restart

pmconf status

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.
get	Показывает или загружает информацию об имеющихся исправлениях службы защиты и пакетах с открытым исходным текстом.
history	Отображает хронологию обновления и загрузки.
list	Отображает информацию о TNCPM.
log	Задает уровень протокола для компонентов TNC.
mktncpm	Создает сервер TNCPM.
modify	Изменяет атрибуты tncpm.conf.
proxy	Управляет конфигурацией параметров прокси-сервера.
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.
-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).
-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 указывается целым числом минут или в следующем формате: **d** (число дней): **h** (часы): **m** (минуты). Поддерживаемый диапазон значений для *интервала-загрузки*: 30 - 525600 минут.
-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**.
-L	Задает режим Список или Только поиск.
o *имя пакета*	Имя пакета с открытым исходным текстом для поиска в нем или загрузки.
-P *путь-к-хранилищу-исправлений*	Задает каталог загрузки для хранилищ исправлений, которые будут загружены TNCPM. Каталог по умолчанию: **/var/tnc/tncpm/fix_repository**.
-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.
T *тип пакета*	Тип пакета с открытым исходным текстом для поиска в нем или загрузки.
-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.
V *версия*	Версия пакета с открытым исходным текстом для поиска в нем или загрузки. В режиме поиска (-L) можно задать значение “all”, чтобы искать все имеющиеся версии указанного пакета.
-d	Создает отчет о хронологии загрузки пакетов обновлений.
-C	Создает отчет для сертификата сервера.
-f *имя-файла*	Указывает имя файла сертификата.
-k	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.

Элемент	Описание
-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. Поддерживаемый диапазон значений для <*интервала ifix*>: 30 - 525600 минут.

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
```

18. Для просмотра всех имеющихся версий пакета ‘emacs’ с открытым исходным текстом в формате rpm введите следующую команду:

```
pmconf get -L -o emacs -V all -T rpm
```

19. Для загрузки версии 4.5.1 пакета ‘lsof’ с открытым исходным текстом в формате rpm в каталог /tmp/new_lsof введите следующую команду:

```
mkdir /tmp/new_lsof
pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
```

20. Для просмотра всех имеющихся версий OpenSSH в формате installp введите следующую команду:

```
pmconf get -o openssh -T installp -L -V all
```

21. Для просмотра текущих параметров конфигурации прокси-сервера, которые будет применять cURL при загрузке пакетов с открытым исходным текстом или исправлений службы защиты, введите следующую команду:

```
pmconf proxy display
```

22. Для отключения конфигурации прокси-сервера введите следующую команду:

```
pmconf proxy enable=no
```

23. Для включения прокси-сервера и настройки хоста ‘myProxyServer’ на порту 9876 введите следующую команду:

```
pmconf proxy enable=yes host=myProxyServer port=9876
```

24. Для смены применяемого порта прокси-сервера введите следующую команду:

```
pmconf proxy port=1234
```

25. Для просмотра известных уязвимостей, для которых предназначены исправления службы защиты из пакета исправлений уровня 7100-03-02, введите следующую команду:

```
 pmconf get -L -p 7100-03-02
```

26. Для того чтобы загрузить исправления службы защиты из пакета исправлений уровня 7200-00-01 в каталог /tmp/ifixes_for_7.2.0.1, но не применять их, введите следующую команду:

```
mkdir /tmp/ifixes_for_7.2.0.1
pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
```

Команда psconf

Назначение

Создание отчетов и управление сервером 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*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*время_в_минутах*> | **d** (дни) : **h** (часы) : **m** (минуты)] [**clientDataPath=**<*полный путь*>]

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

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

psconf chserver attribute = *значение*

psconf clientData -i *хост* **[-l | -g]**

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

psconf add { **-G** <*имя_ipgroup*> **ip=**[**±**]<*хост_1, хост_2...*> | {**-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** <*группа_ip*>[**-r** <*информация_компоновки*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1, ifix2,...*> | **-O** <*openpkggrp1, openkggrp2,...*>}

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*> | -O <*openpkggrp*|*ALL*>} [**-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>

psconf clientData {-l | -g} -i <*ip-адрес*|*хост*>

psconf add -O <*группа-открытых-пакетов*> <*имя-открытого-пакета:версия*>

psconf delete -O <*группа-открытых-пакетов*> <*имя-открытого-пакета:версия*>

psconf delete -O <*группа-открытых-пакетов*>

psconf delete -O ALL

psconf add -O <*группа-открытых-пакетов*> fspolicy=<*имя-стратегии-FS*>

psconf report -O ALL -o TEXT

psconf add -V <*группа_ifix*> autoupdate=<yes|no>

psconf reboot -i <*хост*> last one

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**.
clientData	Создает моментальную копию информации (уровень операционной системы и установленный наборы файлов) о клиенте TNC. Путь *clientDataPath* определяет расположение сведений о наборе моментальных копий. Расположение по умолчанию - каталог `/var/tnc/clientData/` клиента TNC. Путь *clientDataPath* можно изменить или задать с помощью команд **chserver** или **mkserver**. Набор моментальных копий клиента TNC можно проинициализировать из командной строки с помощью команды **clientData** в клиенте TNC. Команда **clientData**, выполняемая из командной строки, не зависит от интервала **clientData_interval**.
clientData_interval	Команды **chserver** и **mkserver** применяются для настройки сбора набора моментальных копий через равные интервалы, заданные в значении интервала **clientData_interval**. Сбор моментальных копий запускается автоматически, если значение интервала **clientData_interval** отличается от 0. По умолчанию сбор моментальных копий отключен в планировщике. Для включения планировщика укажите для параметра **clientData_interval** целочисленное значение, не превышающее 30. Для отключения планировщика укажите для параметра **clientData_interval** значение 0. Поддерживаемый диапазон значений параметра **clientData_interval**: 30 - 525600 минут.
dbpath	Задает расположение базы данных TNC. Значение по умолчанию: `/var/tnc`.

Элемент	Описание
default_policy	Включает или отключает автоматическую проверку клиента TNC на наличие промежуточных исправлений (ifix) и APAR на уровне, совпадающем с уровнем клиента. Для включения проверки укажите значение *yes*. Для отключения автоматической проверки укажите значение *no*. Дополнительная информация о команде **default_policy** приведены в таблице default_policy.
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.
list	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.
Openpkggrp	Задает имя группы открытых пакетов из стратегии набора файлов, применяемой для проверки клиентов.
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.
reboot	Перезагружает клиент TNC, определяемый IP-адресом в переменной <*хост*>.
recheck_interval	Задает для сервера TNC интервал (в минутах или в формате d (дни) : h (часы) : m (минуты)) между проверками клиентов TNC. Поддерживаемый диапазон значений **recheck_interval**: 30 - 525600 минут. **Примечание:** Значение **recheck_interval=0** означает, что планировщик не запускает проверку клиентов через равные промежутки времени, а зарегистрированные клиенты автоматически проверяются 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.

В следующей таблице отображаются результаты настройки команды **default_policy** в зависимости от значений *yes* или *no*:

Таблица 16. Результаты команды default_policy

FSpolicy (стратегия Fileset)	**default policy=***yes*	**default policy=***no*
Клиент TNC относится к стратегии набора файлов с определенными промежуточным исправлением (iFix) и группами APAR	Стратегия по умолчанию заменяется iFix и APAR, заданными в стратегии набора файлов.	Стратегия по умолчанию не используется. Во время процесса проверки клиента TNC применяются iFix и APAR, заданные в стратегии набора файлов.
Клиент TNC относится к стратегии набора файлов без определенных iFix и групп APAR	Во время процесса проверка клиента TNC применяется стратегия по умолчанию с iFix и APAR. Во время проверки применяются только iFix и APAR, соответствующие уровню клиента TNC.	Стратегия по умолчанию не используется.

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, за которым следует разделенный запятыми список имен групп IP-адресов.
-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 - COMPLIANT. 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	Выполнить команду **clientData** на заданном клиенте TNC. Этот флаг доступен только с командой **clientData**.
-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.
-l	Выводит сведения о моментальной копии на сервере TNC для указанного клиента TNC. Этот флаг доступен только с командой **clientData**.
-O <группа-открытых-пакетов>	Задает имя группы открытых пакетов для стратегии.
-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.

Элемент	Описание
-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<*CVEid|ALL*>	Показывает все уязвимости и открытости для зарегистрированных пакетов обновления. **CVEid** **All** Показывает все уязвимости и открытости для зарегистрированных пакетов обновления.
-v<*ifix1, ifix2,...*>	Указывает разделенный запятыми список промежуточных исправлений.
-V<*группа_ifix*>	Задает имя группы промежуточных исправлений.
-V <*группа_ifix*> autoupdate=<yes|no>	Указывает, обновляются ли автоматически промежуточные исправления из заданной группы промежуточных исправлений. **Yes** Стратегия, заданная в fspolicy, автоматически обновляется при поступлении новых промежуточных исправлений на сервер TNC. **No** Новые промежуточные исправления назначаются стратегии вручную после поступления на сервер TNC. Значение по умолчанию отсутствует.

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 **COMPLIANT** 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
    ```
18. Для отображения сведений о моментальной копии, собранных с помощью команды **clientData**, введите следующую команду:
    ```
    psconf clientData -l [ip|host]
    ```
19. Для отображения хронологии для клиента TNC введите следующую команду:
    ```
    psconf list -H -i [ip|ALL]
    ```

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 pscuiserverctl

Назначение

Служит для настройки опций сервера GUI PowerSC.

Синтаксис

pscuiserverctl -r set [arg1 [arg2 [arg3]]]

pscuiserverctl set [httpPort]

pscuiserverctl set [httpsPort]

pscuiserverctl set [administratorGroupList]

pscuiserverctl set [logonGroupList]

pscuiserverctl set [powervcKeystoneUrl]

pscuiserverctl set [QRadarSyslogResponseEnabled]

pscuiserverctl set [tncServer]

Флаги

-r Перезапускает сервер GUI PowerSC после применения значения параметра.

set
Задает или извлекает значение опции сервера GUI PowerSC.

Параметры

httpPort ***httpPortno***
Просмотреть или задать порт по умолчанию, применяемый GUI PowerSC.

httpsPort ***httpsPortno***
Просмотреть или задать защищенный порт по умолчанию, применяемый GUI PowerSC.

administratorGroupList ***unixgrp1,unixgrp2,...***
Просмотреть или задать группы UNIX, которым будет разрешено выполнять администраторские функции с помощью GUI PowerSC.

logonGroupList ***unixgrp1,unixgrp2,...***
Просмотреть или задать группы UNIX, которым будет разрешено входить в систему GUI PowerSC.

powervcKeystoneUrl ***powervcKeystoneurl***
Просмотреть или задать URL сервера хранилища ключей PowerVC.

QRadarSyslogResponseEnabled on | off
Просмотреть текущее значение опции ведения системного протокола из GUI PowerSC или задать (включить или выключить) эту опцию.

tncServer ***tncserver.abc.com***
Просмотреть или задать имя хоста сервера TNC. При изменении имени хоста сервера TNC необходимо перезапустить сервер GUI PowerSC.

Код завершения

Эта команда возвращает следующие коды завершения:

0 Успешное выполнение.

>0 Произошла ошибка.

Примеры

1. Узнать, какой порт используется GUI PowerSC по умолчанию:
   ```
   pscuiserverctl set httpPort
   ```
2. Задать порт по умолчанию GUI PowerSC:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Узнать, какой защищенный порт используется GUI PowerSC по умолчанию:
   ```
   pscuiserverctl set httpsPort
   ```

4. Задать защищенный порт по умолчанию GUI PowerSC:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Узнать, каким группам UNIX разрешено выполнять администраторские функции с помощью GUI PowerSC:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Задать группы UNIX, которым будет разрешено выполнять администраторские функции с помощью GUI PowerSC:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Узнать, каким группам UNIX разрешено входить в систему GUI PowerSC:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Задать группы UNIX, которым будет разрешено входить в систему GUI PowerSC:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Узнать URL сервера хранилища ключей PowerVC:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Задать URL сервера хранилища ключей PowerVC:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```
11. Узнать, ведется ли системный протокол в GUI PowerSC:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled
    ```
12. Включить или выключить ведение системного протокола в GUI PowerSC:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled on
    pscuiserverctl set QRadarSyslogResponseEnabled off
    ```
13. Узнать имя хоста сервера TNC:
    ```
    pscuiserverctl set tncServer
    ```
14. Задать имя хоста сервера TNC:
    ```
    pscuiserverctl set tncServer tncserver.abc.com
    ```
15. Для того чтобы задать имя хоста сервера TNC, необходимо перезапустить сервер GUI PowerSC. Перезапустить сервер GUI PowerSC:
    ```
    pscuiserverctl -r set tncServer tncs1.rs.com
    ```

Команда pscxpert

Назначение

Помощь системному администратору в настройке конфигурации защиты.

Синтаксис

pscxpert -l {high|medium|low|default|sox-cobit} [**-p**]

pscxpert -l {h|m|l|d|s} [**-p**]

pscxpert -f Profile [**-p**] [**-r**|**-R**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r**|**-R**] [**-P** Профайл] [**-l** Уровень]

pscxpert -t

pscxpert -l <Level> [**-p**] **<-a** *файл1* | **-n** *файл2* | **-a** *файл3* **-n** *файл4***>**

pscxpert -f Профайл **-a** Файл [**-p**]

pscxpert -d

Описание

Команда **pscxpert** включает указанный уровень защиты для различных параметров конфигурации системы.

Выполнение **pscxpert** только с флагом **-l** устанавливает соответствующие параметры защиты без запроса значений у пользователя. Например **pscxpert -l high** автоматически применяет все параметры защиты высокого уровня в системе. Однако при запуске команды **pscxpert -l** с флагами **-n** и **-a** параметры защиты будут сохранены в файле, заданном в параметре *Файл*. Затем флаг **-f** применит новую конфигурацию.

После начального выбора в меню отображаются все опции конфигурации защиты, связанные с выбранным уровнем защиты. Эти опции можно выбрать как все сразу, так и каждую в отдельности, включая или выключая. После вторичного выбора команда **pscxpert** продолжит применение параметров защиты в компьютерной системе.

Запустите команду **pscxpert** от имени пользователя root на целевом сервере виртуального ввода-вывода. Если вы не обладаете правами пользователя root целевого сервера виртуального ввода-вывода, выполните команду **oem_setup_env** перед запуском команды.

Если команда **pscxpert** запускается при уже запущенном другом экземпляре команды **pscxpert**, то команда **pscxpert** завершит выполнение с выводом сообщения об ошибке.

Примечание: Запускайте повторно команду **pscxpert** после любого крупного изменения системы, например после установки или обновления программного обеспечения. Если при повторном запуске команды **pscxpert** какой-либо элемент конфигурации не выбран, то он будет пропущен.

Флаги

Права доступа	Описание
-a	Параметры со связанными опциями уровня защиты записываются в указанный файл в сокращенном формате.
-c	Проверяет параметры защиты по сравнению с примененным ранее набором правил. Если проверка выполняется с ошибками, то будет выполнена проверка предыдущих версий правила. Этот процесс будет продолжен до успешной проверки либо до проверки всех экземпляров правила с ошибкой в файле `/etc/security/aixpert/core/appliedaixpert.xml`. Эту проверку можно запустить для любого профайла по умолчанию или для пользовательского профайла.
-d	Отображает определение типа документа (DTD).

Права доступа	Описание
-f	Применяет параметры защиты, заданные в файле *Профайл*. Профайлы расположены в каталоге `/etc/security/aixpert/custom`. В список доступных профайлов включены следующие стандартные профайлы: **DataBase.xml** Этот файл содержит требования для параметров базы данных по умолчанию. **DoD.xml** Этот файл содержит требования для параметров Department of Defense Security Technical Implementation Guide (STIG). **DoD_to_AIXDefault.xml** Этот файл восстанавливает параметры AIX по умолчанию. **DoDv2.xml** Этот файл содержит требования для параметров Department of Defense Security Technical Implementation Guide (STIG) версии 2. **DoDv2_to_AIXDefault.xml** Этот файл восстанавливает параметры AIX по умолчанию. **Hipaa.xml** Этот файл содержит требования для параметров HIPAA (акт о передаче и защите данных учреждений здравоохранения). **NERC.xml** Этот файл содержит требования для параметров NERC. **NERC_to_AIXDefault.xml** Этот файл изменяет параметры NERC и восстанавливает параметры AIX по умолчанию. **PCI.xml** Этот файл содержит требования для параметров стандарта защиты данных PCI. **PCIv3.xml** Этот файл содержит требования для параметров стандарта защиты данных PCI версии 3. **PCI_to_AIXDefault.xml** Этот файл восстанавливает параметры AIX по умолчанию. **PCIv3_to_AIXDefault.xml** Этот файл восстанавливает параметры AIX по умолчанию. **SOX-COBIT.xml** Этот файл содержит требования для параметров закона Сарбейнса-Оксли и COBIT. В этом же каталоге можно создать пользовательские профайлы и применять их к своим параметрам путем переименования и редактирования существующих файлов XML. Например, для применения профайла HIPAA в системе выполните следующую команду: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Если указан флаг **-f**, параметры защиты последовательно передаются от системы к системе путем передачи и применения файла **appliedaixpert.xml** профайла. Все успешно примененные правила записываются в файл `/etc/security/aixpert/core/appliedaixpert.xml`, а правила действия `undo`, соответственно, в файл `/etc/security/aixpert/core/undo.xml`.

Права доступа	Описание
-l	Позволяет задать требуемый уровень параметров защиты системы. Поддерживает следующие опции: **h|high** Задает опции высокого уровня защиты. **m|medium** Задает опции среднего уровня защиты. **l|low** Задает опции низкого уровня защиты. **d|default** Задает опции стандартного уровня защиты AIX. **s|sox-cobit** Задает опции защиты согласно закону Сарбейнса-Оксли и COBIT. При одновременном указании флагов **-l** и **-n** параметры защиты не будут применены в системе, а будут только записаны в указанный файл. Все успешно примененные правила записываются в файл `/etc/security/aixpert/core/appliedaixpert.xml`, а, соответственно, правила отмены действий - в файл `/etc/security/aixpert/core/undo.xml`. **Внимание:** При использовании флага **d|default** могут быть переопределены настроенные параметры защиты, заданные ранее с помощью команды **pscxpert** или самостоятельно, и восстановлены стандартные открытые параметры системы.
-n	Записывает параметры со связанными опциями уровня защиты в указанный файл.
-p	Указывает, что при выводе правил защиты отображается подробная информация. Флаг **-p** записывает обработанные правила в подсистему контроля, если включена опция **auditing**. Эту опцию можно использовать совместно с любой из **-l**, **-u**, **-c** или **-f**. Флаг **-p** включает подробный вывод на терминал и в файл aixpert.log.
-P	Принятие имени профайла в качестве входных данных. Эта опция используется совместно с флагом **-c**. Одновременно указанные флаги **-c** и **-P** применяются для проверки совместимости системы с успешно примененным профайлом.
-r	Записывает существующие параметры системы в файл `/etc/security/aixpert/check_report.txt`. Вывод можно использовать в отчетах аудита соответствия или защиты. В отчете описываются все параметры, их привязка к соблюдению требованиям законодательства и результат проверки (успешно или с ошибками). **Примечание:** • Флаг -r поддерживает операцию применения только для профайлов. Он не поддерживает операцию применения для уровней. • Опция -r выдает все сообщение (одну или несколько строк) для правила.
-R	Создает тот же вывод, что и флаг **-r**. Кроме того, этот флаг добавляет описание сценария или программы правила, применяемых для реализации параметра конфигурации. **Примечание:** • Флаг -R поддерживает операцию применения только для профайлов. Он не поддерживает операцию применения для уровней.
-t	Отображает тип профайла, примененного в системе.
-u	Отменяет примененные параметры защиты. **Примечание:** • С помощью флага **-u** нельзя отменить применение профайлов DoD, DoDv2, NERC, PCI или PCIv3. Для удаления этих профайлов после добавления следует использовать профайл, оканчивающийся на `_AIXDefault.xml`. Например, для удаления профайла NERC.xml необходимо применить профайл NERC_to_AIXDefault.xml. • Операция отмены аннулирует изменения в системе, вызванные операцией применения. Параметры возвращаются к значениям, существовавшим перед выполнением операции применения.

Параметры

Права доступа	Описание
Файл	Выходной файл, в котором хранятся параметры защиты. Для доступа к этому файлу требуются права доступа Root.
Уровень	Пользовательский уровень для проверки примененных ранее параметров.
Profile	Имя файла профайла, предоставляющего согласованные правила для системы. Для доступа к этому файлу требуются права доступа Root.

Security

Для запуска команды **pscxpert** требуются права доступа root.

Примеры

1. Для записи в выходной файл всех опций высокого уровня защиты выполните следующую команду:

   ```
   pscxpert -l high -n /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   После выполнения этой команды выходной файл можно изменять. Для преобразования конкретных правил защиты в комментарий их требуется заключить в стандартные строки комментария XML (<-- для начала комментария и -\> для его завершения).
2. Для применения параметров защиты из файла конфигурации STIG DoD введите следующую команду:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Для применения параметров защиты из файла конфигурации HIPAA введите следующую команду:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Для проверки параметров защиты системы и вывода протокола о непримененных правилах в подсистему контроля выполните следующую команду:

   ```
   pscxpert -c -p
   ```
5. Для проверки пользовательского уровня параметров защиты для профайла NERC в системе и вывода протокола о непримененных правилах в подсистему контроля введите следующую команду:

   ```
   pscxpert -c -p -l NERC
   ```
6. Для создания отчетов и их записи в файл `/etc/security/aixpert/check_report.txt` введите следующую команду:

   ```
   pscxpert -c -r
   ```

Расположение

Права доступа	Описание
/usr/sbin/pscxpert	Содержит команду **pscxpert**.

файлы

Права доступа	Описание
/etc/security/aixpert/log/aixpert.log	Содержит протокол трассировки применяемых настроек безопасности. Этот файл не использует стандарт syslog. Команда **pscxpert** выполняет запись непосредственно в файл, для которого установлены права доступа для чтения/записи и владелец root.
/etc/security/aixpert/log/firstboot.log	Содержит протокол трассировки параметров защиты, примененных при первой загрузке установки Защиты по умолчанию (SbD).
/etc/security/aixpert/core/undo.xml	Содержит список (в формате XML) параметров защиты, которые можно отменить.

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. 125
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. 168

Примечания

Данная 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 лицензии на эти патенты. Запросы на получение лицензии можно отправлять в письменном виде по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

За получением лицензий, имеющих отношение к двухбайтовому набору символов (DBCS), обращайтесь в местное отделение компании IBM по интеллектуальной собственности или направьте запрос в письменной форме по следующему адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

КОМПАНИЯ IBM 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 юрисдикциях 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. IBM может вносить обновления или изменения в этот документ без предварительного уведомления.

Любые ссылки на веб-сайты других компаний приведены в данной публикации исключительно для удобства пользователей и не должны рассматриваться как рекомендация этих веб-сайтов. Материалы, размещенные на этих веб-сайтах, не являются частью информации по данному продукту IBM, и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять предоставленную вами информацию любым способом без каких-либо обязательств перед вами.

Лицам, обладающим лицензией на данную программу и желающим получить информацию о ней с целью: (i) настройки обмена данными между независимо разработанными программами и другими программами (включая данную) и (ii) использования информации, полученной в результате обмена, этими программами, следует обращаться по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM или любого другого эквивалентного соглашения.

Данные о производительности и примеры клиентов приведены исключительно в иллюстративных целях. Фактические результаты производительности зависят от конкретных конфигураций и рабочих сред.

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.

Заявления относительно будущих намерений IBM могут быть изменены или отозваны без дополнительного уведомления и отражают только текущие цели и задачи.

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 только для планирования. Она может быть изменена до выпуска описанных в данном документе продуктов.

Настоящая документация содержит примеры данных и отчетов, применяемых в повседневной деятельности компаний. Для большего сходства с реальностью примеры содержат имена людей, названия компаний, товарных знаков и продуктов. Все эти имена и названия вымышленные. Любые совпадения с реально существующими физическими или юридическими лицами совершенно 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. IBM не несет ответственности за ущерб, который может возникнуть в результате использования эти образцов программ.

Во все копии или фрагменты этих примеров программ, а также программы созданные на их основе, следует добавлять следующее замечание об авторских правах:

© (название компании) (год).

Некоторые фрагменты исходного кода получены из примеров программ фирмы IBM Corp.

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 адресу www.ibm.com/legal/copytrade.shtml.

Linux - это зарегистрированный товарный знак Линуса Торвальдса в США и других странах.

Java и все товарные знаки и эмблемы на основе Java являются товарными знаками или зарегистрированными товарными знаками компании Oracle и/или ее дочерних компаний.

Индекс

И

К

М

Н

О

П

Р

С

Т

У

Напечатано в Дании